

OFFICE OF MANAGEMENT AND BUDGET**Legislative Reference Division
Labor-Welfare-Personnel Branch****TO:**Devorah

_____**URGENT****FROM: Robert J. Pellicci****Phone # :** (202) 395-4871**Fax # :** (202) 395-6148**E-Mail:** Robert_J._Pellicci@omb.eop.gov**Number of Pages (including cover page):**13**Date:**5/1**Time:**3 PM**Comments:**FINAL Internet drugs bill -

[GCL DRAFT 4/13/00]

The Honorable J. Dennis Hastert
Speaker of the House of Representatives
Washington, DC 20515

Dear Mr. Speaker:

Enclosed for the consideration of the Congress is the Administration's draft bill, the "Internet Prescription Drug Sales Act of 2000". The bill would amend the Federal Food, Drug, and Cosmetic Act (the "Act") to enhance the health and safety of consumers purchasing prescription drugs over the Internet and to provide them the same level of protections enjoyed by customers of traditional "brick and mortar" pharmacies.

The Administration's objective in developing this legislation is to provide sufficient safeguards to protect the public health effectively without hindering the enormous potential benefit of the Internet. In addition, the bill is designed to enhance the effectiveness of the Federal-State partnership in the regulation of prescription drugs and recognize the importance of the States' traditional role in regulating the practice of medicine and pharmacy. Accordingly, the bill would support and strengthen the States' authority to enforce applicable law within their borders, while providing enhanced Federal authority to monitor the multistate and interstate aspects of Internet prescription drug sales. By filling gaps in Federal and State authority, the bill seeks to curb illegal sales of prescription drugs and to ensure that consumers are receiving safe and effective drugs prescribed by health care professionals, and dispensed by pharmacies that are properly licensed, and in compliance with, all applicable State and Federal law.

Specifically, the bill would require online pharmacies to be licensed in each State in which they operate or to which they deliver prescription drugs. They would have to comply with all applicable Federal and State laws governing the practice of pharmacy which include, among others, requirements for proper storage and handling of prescription drugs, record keeping, and other consumer protections including safeguards on patient privacy and confidentiality of medical records.

The online pharmacy would be required to provide to the Secretary and concerned State boards of pharmacy, prior to launching an online site (or, if later, by 30 days after enactment), a notification containing the information required to be posted on the site and assurances of compliance with the requirements of the bill; it would be required to post on its website a declaration that this notification has been made. If the online pharmacy failed to comply with any requirement, the Secretary, after providing notice and opportunity for a hearing, could prohibit the pharmacy from displaying the declaration and from selling drugs online, subject to substantial civil money penalties. Finally, States would be authorized to bring civil actions

The Honorable J. Dennis Hastert—page 2

against online pharmacies for violations of these requirements.

The growth of the Internet in recent years has vastly expanded patients' options for access to health-related information, products, and services. The Internet can afford purchasers of pharmaceuticals convenience and privacy, as well as expanded access to products and the ability easily to compare prices. The Internet, however, also has provided a new marketplace for sales that are already illegal (whether on- or off-line), such as sales of unapproved new drugs (including counterfeit drugs), prescription drugs sold without a prescription, drugs imported (or re-imported) illegally, and products marketed with fraudulent claims. Patients who buy prescription drugs from websites that engage in such illegal activities are at risk for adverse effects from inappropriately prescribed medications, dangerous drug interactions, and contaminated drugs.

As you know, long before the Internet was created, Congress and the State legislatures enacted a comprehensive system of pre-market approval, prescription drug designation, practitioner evaluation and pharmacy dispensing to protect patients from injuries resulting from unsafe or counterfeit drugs and from the illicit practice of medicine and pharmacy. This system has worked well over the years.

Because the current laws were not enacted with the Internet in mind, however, they do not provide regulatory and law enforcement agencies with fully effective tools to protect consumers from operators of online pharmacies that engage in illegal activities. For example, both consumers and law enforcement officials may have difficulty identifying the name, location, and State licensure of physicians, pharmacists, and online pharmacy operators. Even if the parties can be identified, because the Internet is largely unconstrained by State and national boundaries, States—traditionally the primary regulators of the practice of pharmacy and the practice of medicine—are undercut in their efforts to regulate online pharmacies. Finally, both State and Federal agencies are limited in the causes of action that may be brought against illegal on-line sellers of prescription drugs.

This bill would fill gaps in current consumer protection and enforcement authority. The compliance and disclosure requirements for online pharmacies would afford substantial public health benefits and provide enhanced tools for law enforcement. Legitimate online pharmacies could be much more easily distinguished from illegal online pharmacies. Enactment of this bill would enhance consumer safety and confidence in the Internet, and level the playing field for legitimate online pharmacies by reducing their illegal competition.

We therefore urge the Congress to give the draft bill its prompt and favorable consideration. The Office of Management and Budget has advised that there is no objection to the submission of this

The Honorable J. Dennis Hastert—page 3

legislative proposal to the Congress, and that its enactment would be in accord with the President's program.

Sincerely,

Donna E. Shalala

Enclosures

[GCL DRAFT 4/19/00]

A BILL

To amend the Federal Food, Drug, and Cosmetic Act to provide for regulation of sales of prescription drugs on the Internet, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Internet Prescription Drug Sales Act of 2000".

SEC. 2. REGULATION OF INTERNET PRESCRIPTION DRUG SALES.

(a) IN GENERAL.—Chapter V of the Federal Food, Drug, and Cosmetic Act is amended by adding after section 503A the following new section:

"SEC. 503B. INTERNET PRESCRIPTION DRUG SALES.

"(a) DEFINITIONS.—

"(1) INTERNET.— The term 'Internet' means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

"(2) CONSUMER.—The term 'consumer' means a person (other than a pharmacy or other entity licensed under state or federal law to purchase prescription drugs for resale) that purchases or seeks to purchase prescription drugs through the Internet.

"(3) ONLINE PHARMACY.— The term 'online pharmacy' means a person, whether in the United States or abroad, that engages in, offers to engage in, or causes the delivery or sale of a prescription drug to a consumer through the Internet in the United States.

"(4) PRESCRIPTION DRUG.— The term 'prescription drug' has the meaning given the term in section 503(b)(1).

"(b) REQUIREMENTS FOR ONLINE PHARMACIES.—

"(1) IN GENERAL.—Each online pharmacy shall demonstrate that it complies with the requirements of this subsection with respect to the delivery or sale of prescription drugs through the Internet and shall at all times display on the homepage of its Internet website a declaration of compliance in accordance with subsection (c).

"(2) LICENSURE.—The online pharmacy shall be licensed to practice pharmacy in each State in which it operates, and in each State to which it delivers or offers to deliver prescription drugs ordered on the Internet.

"(3) COMPLIANCE WITH FEDERAL AND STATE LAWS.—The online pharmacy shall comply with all applicable requirements of Federal and State law governing the practice of pharmacy.

"(4) WEBSITE DISCLOSURE INFORMATION.—The online pharmacy shall post in a visible and clear manner (as determined by the Secretary) on the homepage of its Internet website or on a page directly linked to its homepage the following:

"(A) the name (or names) of the online pharmacy or pharmacies identified on its license (or licenses) in each State in which it is licensed to engage in the practice of pharmacy;

"(B) the street address of the online pharmacy's principal place of business;

"(C) the name, professional degree, and licensure of the pharmacist in charge;

"(D) a telephone number or numbers at which a licensed pharmacist may be contacted;

"(E) a list of the States in which the online pharmacy is licensed to dispense prescription drugs and the applicable license numbers;

"(F) a statement that the online pharmacy will dispense prescription drugs only upon a valid prescription by a licensed practitioner and only to an individual

located in a State in which the online pharmacy is licensed to dispense such drugs;
and

"(G) a declaration of compliance in accordance with subsection (c).

"(5) NOTIFICATION.—The online pharmacy shall notify the Secretary and the applicable State boards of pharmacy 30 days prior to launching any website. Such notification shall include the information required to be posted on the online pharmacy's website pursuant to paragraph (4) of this subsection and shall notify the Secretary and the applicable State boards of pharmacy, under penalty of perjury, that the online pharmacy complies in all respects to the requirements set forth in paragraphs (1) through (4) of this subsection and that the information disclosed on its website pursuant to paragraph (4) is truthful. An online pharmacy that is already operational as of the effective date of this section, shall notify the Secretary and applicable State boards of pharmacy in accordance with this paragraph within 30 days after the effective date of this section.

"(c) DECLARATION OF COMPLIANCE.— On and after the date of the notification pursuant to subsection (b)(5), the online pharmacy shall display on the homepage of its Internet website, in such form as the Secretary may require, a declaration that it has made the required notification to the Secretary.

"(d) SECRETARIAL REVIEW; WITHDRAWAL OF DECLARATION.—

"(1) Within 90 days after receiving a notification pursuant to subsection (b)(5), the Secretary shall review the accuracy of such notification and shall notify the online pharmacy if the Secretary concludes that it is not in compliance with the requirements of subsection (b).

"(2) The Secretary may order an online pharmacy to cease displaying a declaration on its website, at any time, if the Secretary determines that an online pharmacy fails to meet any of the requirements set forth in subsection (b). Such an order may be issued only after the Secretary has provided notice to the online pharmacy of the intent of the Secretary to issue the order and has provided an opportunity for a hearing

with respect to such intent. If the failure of an online pharmacy constitutes a minor violation of this section, the Secretary shall delay issuing the order and provide the online pharmacy an opportunity to correct the violation. If the Secretary has prohibited an online pharmacy from displaying a declaration, it shall be unlawful for the online pharmacy to engage in, offer to engage in, or cause the delivery or sale of prescription drugs to a consumer. Nothing in this subsection shall preclude the Attorney General from bringing an action to enforce any other law, including any other provision of this section.

"(e) DESIGNATION OF EXAMINING ENTITY.—The Secretary may designate one or more private nonprofit organizations or State agencies to verify licensing information included in a notification submitted pursuant to subsection (b)(5) and to examine and inspect the records and facilities of an online pharmacy that has submitted a notification pursuant to subsection (b)(5) to verify the information submitted in such notification. Any state agency so designated may accept or reject such designation to conduct these examinations and inspections.

"(f) SUBPOENAS.—

"(1) AUTHORIZATION.—

"(A) For the purpose of any civil or criminal investigation with respect to this statute, the Attorney General or the Attorney General's designee may issue in writing and cause to be served a subpoena—

"(i) requiring the production of any records (including any books, papers, documents, electronic media, or other objects or tangible things), which may be relevant to an authorized law enforcement inquiry, that a person or legal entity may possess or have care, custody, or control over, or

"(ii) requiring a custodian of records to give testimony concerning the production and authentication of such records.

"(B) A subpoena under this subsection shall describe the objects required to be produced and prescribe a return date within a reasonable period of time

within which the objects can be assembled and made available.

"(C) The production of records shall not be required under this section at any place more than 500 miles distance from the place where the subpoena for the production of such records is served.

"(D) Witnesses summoned under this section shall be paid the same fees and mileage that are paid witnesses in the courts of the United States.

"(2) SERVICE.—A subpoena issued under this section may be served by any person who is at least 18 years of age and is designated in the subpoena to serve it. Service upon a natural person may be made by personal delivery of the subpoena to him. Service may be made upon a domestic or foreign corporation or upon a partnership or other unincorporated association which is subject to suit under a common name, by delivering the subpoena to an officer, to a managing or general agent, or to any other agent authorized by appointment or by law to receive service of process. The affidavit of the person serving the subpoena entered on a true copy thereof by the person serving it shall be proof of the service.

"(3) ENFORCEMENT.—In the case of contumacy by or refusal to obey a subpoena issued to any person, the Attorney General may invoke the aid of any court of the United States within the jurisdiction of which the investigation is carried on or of which the subpoenaed person is an inhabitant, or in which he carries on business or may be found, to compel compliance with the subpoena. The court may issue an order requiring the subpoenaed person to appear before the Attorney General to produce records, if so ordered, or to give testimony concerning the production and authentication of such records. Any failure to obey the order of the court may be punished by the court as a contempt thereof. All process in any such case may be served in any judicial district in which such person may be found.

"(4) IMMUNITY FROM CIVIL LIABILITY.—Notwithstanding any Federal, State, or local law, any person, including officers, agents, and employees, receiving a

summons under this section, who complies in good faith with the summons and thus produces the materials sought, shall not be liable in any court of any State or the United States to any customer or other person for such production or for non-disclosure of that production to the customer.

"(5) LIMITATION ON USE.—

"(A) Health information about an individual that is disclosed under this section may not be used in, or disclosed to any person for use in, any administrative, civil, or criminal action or investigation directed against the individual who is the subject of the information unless the action or investigation arises out of and is directly related to receipt of health care or payment for health care or action involving a fraudulent claim related to health; or if authorized by an appropriate order of a court of competent jurisdiction, granted after application showing good cause therefor.

"(B) In assessing good cause, the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services.

"(C) Upon the granting of such order, the court, in determining the extent to which any disclosure of all or any part of any record is necessary, shall impose appropriate safeguards against unauthorized disclosure.

"(6) REGULATIONS.—The Secretary is authorized to promulgate such regulations as necessary to carry out the provisions of this section.

"(h) STATE CAUSE OF ACTION.—

"(1) AUTHORITY OF STATES.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is being threatened or adversely affected by the action of a person that violates the provisions of this section, the attorney general may bring a civil action on behalf of such residents in a district court of the United States with appropriate jurisdiction—

"(A) to enjoin such action,

"(B) to enforce compliance with this section,

"(C) to obtain damages, restitution, or other compensation, including civil money penalties under section 303(h), or

"(D) to obtain such other legal or equitable relief as the court may find appropriate.

"(2) RIGHTS OF THE ATTORNEY GENERAL.—

"(A) NOTICE TO THE ATTORNEY GENERAL.—The State shall serve prior written notice of any civil action under paragraph (1) upon the Attorney General and provide the Attorney General with a copy of its complaint, except in any case where such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action.

"(B) The Attorney General shall have the right—

"(i) to intervene in such action,

"(ii) upon so intervening, to be heard in all matters arising therein,

and

"(iii) to file petitions for appeal.

"(3) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act shall prevent an attorney general from exercising the powers conferred on the attorney general by the laws of such State to conduct investigations or to administer oaths or affirmations or to compel the attendance of witnesses or the production of documentary or other evidence.

"(4) VENUE; SERVICE OF PROCESS.—Any civil action brought under paragraph (1) in a district court of the United States may be brought in the district in which the defendant is found, is an inhabitant, or transacts business or wherever venue is proper under section 1391 of Title 28, United States Code. Process in such action may be served in any district in which the defendant is an inhabitant

or in which the defendant may be found.

"(i) INTERSTATE COMMERCE.—The Internet is an instrumentality of interstate

commerce, and the use of the Internet by an online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug, affects interstate commerce."

(b) PROHIBITED ACTS.—Section 301 of the Federal Food, Drug, and Cosmetic Act is amended by adding at the end the following new subsection:

"(aa) The violation of section 503B by operating an online pharmacy without providing the notification and all other information required under subsection (b)(1) through (b)(5), or making a materially false statement in making or displaying the required declaration or information or operating an online pharmacy without the required evidence of such declaration or otherwise in violation of the requirements of 503B."

(c) PENALTIES.—Section 303 is amended by adding at the end the following new subsection:

"(h) Any person who violates the requirements of section 503B, as specified in section 301(aa), shall be subject to civil money penalties of at least \$2,500, but not more than \$15,000, per violation, not to exceed \$500,000 for any of such violations that took place during the same week, measured from Sunday through Saturday. In determining the amount of such a civil money penalty, the court may take into account the degree of culpability, the risk of non-monetary harm to the public, any actual non-monetary harm to the public, benefit to the offender, any history of prior such conduct, ability to pay, and such other matters as justice may require."

(d) CONFORMING AMENDMENT.—Section 503(b)(2) of the Federal Food, Drug, and Cosmetic Act is amended by inserting after "or by Internet communication that is based on an online questionnaire" after "mail".

(e) RULE OF CONSTRUCTION.—The civil and criminal remedies provided in this

Act are in addition to, and do not displace or modify, any statutes, regulations, or remedies under existing Federal, state, or local law.

(f) EFFECTIVE DATE.—The amendments made by this Act shall become effective one year after the date of enactment.



U.S. DEPARTMENT OF HEALTH AND HUMAN
SERVICES

ROOM 405H, HUMPHREY BUILDING
200 INDEPENDENCE AVE, SW
WASHINGTON, D.C. 20201

DATE:

8/15/00

PHONE: (202)690-7450

FAX: (202)690-8425

FROM:

☒ JANE HORVATH

☐ SHARON CLARKIN

☐ BOB GUIDOS

☐ JOANNE JEE

☐ GREG JONES

☐ ANDREA LEVARIO

☐ ROGER MCCLUNG

☐ JACK MITCHELL

☐ TANISHA PARKER

☐ PAUL SELTMAN

☐ STEPHANIE WILSON

☐

TO:

Chris J

OFFICE:

ROOM:

PHONE:

FAX:

456-5557

Bibley letter
on Internet

(INCLUDING COVER):

?

1

REMARKS:

TIM BALEY, VICE CHAIRMAN

W.J. "BILLY" LELAND, LOUISIANA
 MICHAEL G. ORLEY, OHIO
 MICHAEL BILMAREK, FLORIDA
 JOE BARTON, TEXAS
 FRED UPTON, MISSOURI
 CLYDE STEARNS, ALABAMA
 PAUL E. CLARKE, OHIO
 JAMES C. CAPPANNO, PENNSYLVANIA
 LINDSEY HARRIS, CALIFORNIA
 MARIAN BICAL, GEORGIA
 STEVE LARGENT, DELAWARE
 RICHARD BURN, NORTH CAROLINA
 BRIAN P. DE BRYN, CALIFORNIA
 MIKE FIELD, KENTUCKY
 LARRY MARRIS, ILLINOIS
 CHARLES BROWDER, ALABAMA
 TOM COLUMA, DELAWARE
 RICK LARO, NEW YORK
 WANDA CUBB, WYOMING
 JAMES S. NOGAM, CALIFORNIA
 JOHN SHARPLE, ILLINOIS
 MATTHEW WALSON, NEW MEXICO
 JOHN S. SHAFER, ARIZONA
 CHARLES W. "CHUCK" MCKEITHEN, MISSISSIPPI
 VITO FORSALLA, NEW YORK
 RAY BLUNT, MISSOURI
 ED BRYANT, TENNESSEE
 ROBERT L. ENGLISH, JR., MARYLAND

JOHN D. BENDALL, MISSOURI
 BRUCE A. WATSON, CALIFORNIA
 EDWARD J. BARNETT, MASSACHUSETTS
 GARY H. BALL, TEXAS
 MIKE DONAHUE, VIRGINIA
 EDUARDO TORRES, NEW YORK
 FRANK PALLONE, JR., NEW JERSEY
 STEPHEN BROWN, OHIO
 DALE GEORGIN, TENNESSEE
 FRANK DEWIS, FLORIDA
 GERRY L. BUCK, ILLINOIS
 ANITA G. BROWN, CALIFORNIA
 DON BLUM, PENNSYLVANIA
 MIKE SHARP, MISSOURI
 MARY L. BARKER, NEW YORK
 THOMAS C. BARTER, OHIO
 MIKE B. WYNN, MARYLAND
 GARY CRANE, TEXAS
 LARRY MCKINLEY, MISSOURI
 TERRY STEWART, OHIO
 GARY BOWEN, OHIO
 THOMAS H. BARNETT, WISCONSIN
 BILL LUTHER, MINNESOTA
 LON CAPPEL, CALIFORNIA

JAMES F. SPIDENMAN, CHIEF OF STAFF

U.S. House of Representatives Committee on Commerce

Room 2125, Rayburn House Office Building
 Washington, DC 20515-6115

January 24, 2000

The Honorable William Jefferson Clinton
 President of the United States of America
 The White House
 Washington, D.C. 20502

Dear President Clinton:

As you may know, for the past year the Committee on Commerce has been investigating a number of issues relating to the sale of pharmaceutical products over the Internet. On Friday, July 30, 1999, the Subcommittee on Oversight and Investigations held a hearing on this important issue, during which I called on the Administration to establish a joint Federal-State task force to coordinate current law enforcement efforts and to assess whether they are adequate to protect consumers.

Following the hearing, on August 5, 1999, you ordered, via Executive Order 13133, the establishment of a Federal Working Group on unlawful conduct on the Internet, including prescription drugs. The Working Group was asked to prepare a report and recommendations for you and the Vice President within 120 days of the order, or December 5, 1999. According to the Executive Order, the Working Group was ordered to undertake this review in the context of current Administration Internet policy, which includes, "support for industry self-regulation where possible, technology-neutral laws and regulations, and an appreciation of the Internet as an important medium both domestically and internationally for commerce and free speech."

I supported the creation of this Working Group and the underlying principles that you stated would guide its work. But because the practice of pharmacy and medicine traditionally has been regulated at the state level, I again requested, on September 16, 1999, that you include state regulatory and enforcement agencies in this effort. Recent enforcement actions against on-line pharmacies in several States -- including Kansas, Washington, California, Ohio, Maryland, Illinois, Nevada, Colorado, Missouri, Wyoming and Arizona -- are indicative of increased scrutiny at the state level. Unfortunately, the Working Group was never expanded to include these key state enforcement and regulatory agencies.

The Honorable William Jefferson Clinton
Page 2

On December 28, 1999, you announced a new initiative that would grant the Food and Drug Administration (FDA) broad new authority over Internet pharmacies. This proposal would, in part, nationalize state-level pharmacy regulations by requiring pharmacies to obtain certification from the FDA before they can sell pharmaceuticals on-line. I presume that this new initiative would have been based, at least in some part, on the final report and recommendations from the Federal Working Group that you established in August. However, your public pronouncements on this topic did not reference any such report or recommendations, and you did not release these documents publicly when you announced this sweeping new initiative. Indeed, I was surprised to learn that you had not yet even received specific recommendations or a final report from the Working Group prior to making your December 28, 1999 proposal to regulate electronic commerce and federalize the traditional state function of pharmacy regulation. I also understand that a final report from the Working Group is not scheduled to be completed until the end of January, a month after you made your proposal and nearly two months past the deadline given in the Executive Order.

As I have stated previously, I am committed to working with the Administration to ensure that American consumers can reap the obvious benefits of Internet pharmacies, while being protected from the unscrupulous or illegal vendors peddling drugs on-line -- many of which reside in foreign countries and are beyond the reach of your recent initiative. But I am concerned that your current proposal conflicts with the guiding principles you set forth in creating the Federal Working Group -- namely, that the Federal government should act carefully and thoughtfully before making to regulate this important and efficient new medium. Further, given the facts outlined above, I must ask whether you even relied on any preliminary findings, analysis, or recommendations of the Working Group in crafting your December 28 initiative -- and, if not, what other analysis or review motivated the Administration to propose such a sweeping reform without awaiting or relying upon the work product of its own, self-appointed task force. I also believe that, in order to ensure full and fair consideration of your legislative proposals, it is imperative that you release to this Committee and to the American public all draft reports or recommendations of the Working Group regarding prescription drug sales, as well as the final product of that task force once it is completed.

I look forward to hearing from you on this important issue. Should you have any questions about this matter, please contact me or have your staff contact Lori Wall, Committee Counsel, at (202) 226-2424.

Sincerely,



Tom Bliley
Chairman

The Honorable William Jefferson Clinton
Page 3

cc: The Honorable John D. Dingell, Ranking Member
The Honorable Fred Upton, Chairman
Subcommittee on Oversight and Investigations
The Honorable Ron Klink, Ranking Member
Subcommittee on Oversight and Investigations
The Honorable Janet Reno, Attorney General
United States Department of Justice
The Honorable Jane E. Henney, M.D., Commissioner
Food and Drug Administration
The Honorable Robert Pitofsky, Chairman
Federal Trade Commission

DRAFT

The Honorable Tom Bliley
Committee on Commerce
U.S. House of Representatives
Washington, D.C. 20515-6115

Dear Mr. Chairman:

Thank you for your continued interest in the sale of prescription drugs over the Internet. I have been asked to reply to your January 24 letter to President Clinton, which expressed concern that the President's December 28 announcement of an initiative to control illegal drug sales via the Internet had been made without consideration of the states' role in regulating pharmacies and without coordination by the Federal Working Group on Unlawful Conduct on the Internet.

As you know, the Food and Drug Administration's (FDA) responsibility over pharmaceuticals is primarily one of ensuring that only safe and effective drugs are marketed to American consumers. The principal responsibility for ensuring that pharmacies properly receive, handle, and dispense drugs lies with the individual states in which pharmacies operate. However, the rapid rise of the Internet as an avenue to sell prescription drugs and the subsequent increase in fraudulent activities, demonstrates that traditional state regulation can be undercut, thus putting patients at potentially great risk of receiving unapproved or improperly prescribed drugs.

With this concern in mind, the Administration has announced a proposal that seeks to curb illegal sales by primarily strengthening the states' ability to ensure that all online pharmacies that are selling or dispensing pharmaceuticals to their citizens are properly licensed and operating within the confines of existing law. If enacted, the proposal would authorize FDA to establish a process by which online pharmacies can be certified as meeting the state requirements that they are already required to meet. The underlying basis for this proposal is that online pharmacies should be licensed and operated under the same regulatory scheme that Congress and the states put in place for traditional "brick and mortar" pharmacies. Online pharmacies operating without the licensure required by states would be subject to both state and Federal penalties, with the primary enforcement agency being the state. The proposal also includes disclosure requirements and the use of an idicia or "seal" on legitimate pharmacy websites attesting that they meet the state licensing requirements that all pharmacies must meet. Consumers would then be better able to avoid sites that are not properly licensed.

Under the Administration's proposal, the traditional role of the states in regulating the practice of medicine and pharmacy would be maintained. Moreover, states would have additional legal tools to ensure that their citizens are receiving safe and effective drugs from properly licensed prescribers and pharmacies. Consequently, legitimate online pharmacies would be allowed to flourish without unnecessary new regulation.

We have discussed the concepts underlying the proposal with a variety of state officials, including the National Association of Attorneys General and the National Association of

Boards of Pharmacy. They have expressed initial support for the proposal's reliance on the traditional state regulation of the practice of medicine and pharmacy. We believe that these groups are very interested in working with the Administration and Congress on enacting appropriate legislation to strengthen their ability to monitor the evolving impact of the Internet on the practice of medicine and pharmacy.

Finally, Administration officials have reviewed this proposal and believe that it is consistent with the upcoming report of the President's Working Group on Unlawful Conduct on the Internet in that it ensures that regulation of the Internet is limited to only those instances where it is essential to protect the public health.

I hope that this letter is responsive to your concerns, and we look forward to working with your committee on this important public health initiative.

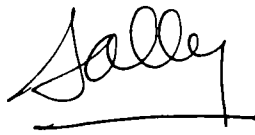
Sincerely,

Jane E. Henney, M.D.
Commissioner of Food and Drugs

R/D:WHubbard
Cleared:JDupont, TMcGinnis, MDotzel:2/9/00
Cleared:MPlaisier:2/10/00

G:\WP\BROADBEN\00-857.doc

3/21



GCL DRAFT 2/23/00

A BILL

To amend the Federal Food, Drug, and Cosmetic Act to provide for regulation of sales of prescription drugs on the Internet, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Internet Prescription Drug Sales Act of 2000".

SEC. 2. REGULATION OF INTERNET PRESCRIPTION DRUG SALES.

(a) IN GENERAL.—Chapter V of the Federal Food, Drug, and Cosmetic Act is amended by adding after section 503A the following new section:

"SEC. 503B. INTERNET PRESCRIPTION DRUG SALES.

“(a) DEFINITIONS.—

"(1) INTERNET.— The term 'Internet' means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

"(2) CONSUMER.—The term 'consumer' means a person (other than a pharmacy or other entity licensed under state or federal law to purchase prescription drugs for resale) that purchases or seeks to purchase prescription drugs through the Internet.

"(3) ONLINE PHARMACY.— The term 'online pharmacy' means a person that engages in, offers to engage in, or causes the delivery or sale of a prescription drug to a

consumer through the Internet.

"(4) PRESCRIPTION DRUG.— The term 'prescription drug' has the meaning given the term in section 503(b)(1).

"(b) REQUIREMENTS FOR ONLINE PHARMACIES.—

"(1) IN GENERAL.—Each online pharmacy shall demonstrate ~~to the Secretary's satisfaction~~ that it complies and will continue to comply with the requirements of this

subsection with respect to the delivery or sale of prescription drugs through the Internet,

and shall at all times display on the homepage of its Internet website a ~~declaration~~ ^{demonstration} of the ~~Secretary's determination of compliance~~ ^{of compliance,} in such form as the Secretary may require, ~~(and~~

~~including such seal, symbol, or other evidence of such determination of compliance as the Secretary may specify).~~

"(2) LICENSURE.—The online pharmacy must be licensed to practice pharmacy in each State in which it operates, and in each State to which it delivers or offers to deliver prescription drugs ordered on the Internet.

"(3) COMPLIANCE WITH FEDERAL AND STATE LAWS.—The online pharmacy must comply with all applicable requirements of Federal and State law governing the practice of pharmacy.

"(4) REQUIREMENT OF VALID PRESCRIPTION.—The online pharmacy must ensure that each prescription drug dispensed to an individual is based on a prescription—

"(A) that is valid under the laws of the State in which the individual is located; and

separate hook

specifying prominently on web

"(B) that is pursuant to a relationship between the individual and prescribing health care practitioner that is not based primarily on an online questionnaire or a similar document concerning the patient's current condition or medical history.

(4) **NOTIFICATION TO FDA**

(grandfather) clause in

"(5) **WEBSITE DISCLOSURE INFORMATION.**—The online pharmacy must

post on the homepage of its Internet website, or on a page directly linked to its homepage the following:

standard format that sec determines

"(A) the name (or names) of the online pharmacy or pharmacies identified on its license (or licenses) in each State in which it is licensed to engage in the practice of pharmacy;

"(B) the street address of the online pharmacy's principal place of business;

"(C) the name, professional degree, and licensure of the pharmacist in charge;

"(D) a telephone number or numbers at which a licensed pharmacist may be contacted;

"(E) a list of the States in which the online pharmacy is licensed to dispense prescription drugs and the applicable license numbers; and

"(F) a declaration that the online pharmacy will dispense prescription drugs only upon a valid prescription by a licensed practitioner and only to an individual located in a State in which the online pharmacy is licensed to dispense such drugs.

(P)

Keinas

do you need to be licensed in the state that you mail to?

finding of non compliance.
4
“(c) EFFECTIVE PERIOD OF DETERMINATION.—

~~“(1) IN GENERAL.—Subject to paragraph (2), a determination by the Secretary under subsection (b) shall be effective for a period of two years from the date of the determination.”~~

“(2) ~~WITHDRAWAL OF DETERMINATION.~~—The Secretary may withdraw a determination of compliance under subsection (b) if, at any time, the Secretary finds that an online pharmacy fails to meet any of the requirements set forth in subsection (b). *process*

Upon issuance of such withdrawal of determination, it shall be unlawful for the online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug to a consumer. *State level / FDA / Fed work consistent w state*

FDA
“(d) FEES.—The Secretary is authorized to assess fees for determinations of compliance of online pharmacies under this section, in amounts not to exceed amounts that the Secretary finds to be sufficient in the aggregate to cover the costs (including costs for periodic inspections) of such determinations. A determination of compliance of an online pharmacy shall not be effective until any applicable fee has been paid in full. *hook*

“(e) DESIGNATION OF EXAMINING ENTITY.—The Secretary may designate one or more private nonprofit organizations or State agencies to examine and inspect the records and facilities of applicants for a ~~determination~~ *det* of compliance under this section. Fees assessed under subsection (d) (or, as determined by the Secretary, an appropriate portion thereof) may be used to reimburse a designated entity for its costs related to such responsibilities.

“(f) SUBPOENAS.—

“(1) COMMISSIONER’S AUTHORITY.— For the purpose of any audit,

investigation, examination, analysis, review, evaluation, determination of compliance, or other proceeding with respect to this section, the Commissioner shall have power to sign and issue subpoenas to any person requiring the production of any books, records, or other documentary evidence. Subpoenas so issued by the Commissioner shall be served by anyone authorized by the Commissioner—

"(A) by delivering a copy thereof to the person named therein, or—

"(B) by registered mail or by certified mail addressed to such person at his or her last dwelling place or principal place of business. A verified return by the person so serving the subpoena setting forth the manner of service, or, in the case of service by registered mail or by certified mail, the return post office receipt therefor signed by the person so served, shall be proof of service.

"(2) JUDICIAL ENFORCEMENT.—In case of contumacy by, or refusal to obey or fully comply with a subpoena issued pursuant to paragraph (1) and duly served upon, any person, any district court of the United States for the judicial district in which such person charged with contumacy or refusal to obey is found or resides or transacts business, upon application by the Commissioner, shall have jurisdiction to issue an order requiring such person to produce the books, records, or other documentary evidence sought by the subpoena; and any failure to obey such order of the court may be punished by the court as a contempt thereof.

"(g) REGULATIONS.—The Secretary is authorized to promulgate such regulations as necessary to carry out the provisions of this section.

"(h) STATE CAUSE OF ACTION.—In any case in which the attorney general 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 the action of a person that violates the provisions of this section, the attorney general may bring a civil action on behalf of such residents in a district court of the United States with appropriate jurisdiction—

"(A) to enjoin such action;

"(B) to enforce compliance with this section;

"(C) to obtain damages, restitution, or other compensation; or

"(D) to obtain such other legal or equitable relief as the court may find

appropriate.

~~XX~~ "(i) INTERSTATE COMMERCE.— The use of the Internet by an online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug is deemed to be a transaction in interstate commerce." *internet*

(b) PROHIBITED ACTS.—Section 301 of the Federal Food, Drug, and Cosmetic Act is amended by adding at the end the following new subsection:

'(aa) The violation of section 503B by—

"(1) operating an online pharmacy without a determination by the Secretary of compliance with the requirements of such section, without a seal or other required evidence of such determination, or otherwise in violation of the requirements set forth in section 503B(b);

"(2) dispensing a prescription drug in violation of section 503B; or

"(3) writing a prescription that is invalid under section 503B."

(c) PENALTIES.—Section 303 is amended by adding at the end the following new

subsection:

"(h) Any person who violates the requirements of section 503B, as specified in section 301(aa), shall be subject to civil money penalties of up to \$500,000 per violation."

(d) EFFECTIVE DATE.—The amendments made by this Act shall become effective one year after the date of enactment.

OFFICE OF MANAGEMENT AND BUDGET

**Legislative Reference Division
Labor-Welfare-Personnel Branch**

URGENT

TO: Chris
Deborah
Dan

FROM: Robert Pellicci

Phone #: (202) 395-4871

Fax #: (202) 395-6148

E-mail Address: Robert_J._Pellicci@omb.eop.gov

Number of Pages (Including cover page): 7

Date: 3/15 Time: 1 PM

Comments:

Advance Justice letter on
the internet drugs bill -
For today's meeting.



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

March 15, 2000

The Honorable Jacob J. Lew
Director
Office of Management and Budget
Washington, D.C. 20503

DRAFT

Dear Mr. Lew:

This letter presents the views of the Department of Justice on the draft legislation proposed by the Department of Health and Human Services, the "Internet Prescription Drug Sales Act of 2000." The Department strongly supports much of this bill, particularly to the extent it treats online and offline conduct in a consistent manner. See Report of the President's Working Group on Unlawful Conduct on the Internet at 11-12 (regulation of unlawful conduct should "apply in the same way to conduct in the cyberworld as it does to conduct in the physical world"). However, as we explain in Part I, the Department strongly opposes the administrative subpoena and judicial enforcement provisions of the proposed bill, which would provide the Food and Drug Administration (FDA) with authority that it does not possess with respect to traditional, brick-and-mortar pharmacies. In Part II, we identify other concerns and offer suggestions on how the bill may be improved and clarified.

I. Subpoena Authority and Enforcement

The Department objects to the administrative subpoena authority and enforcement provisions in the proposed bill.

Section 503(B)(f) of the bill would give FDA the power to issue subpoenas for just about any purpose - "for the purpose of any audit, investigation, examination, analysis, review, evaluation, determination of compliance, or other proceeding with respect to this section[.]" The Department strongly opposes giving FDA such authority. As we have informed the FDA, the Department's longstanding policy is that subpoena authority should in nearly every instance reside with the prosecuting enforcement authority, not the investigative agency. In our long experience, when subpoena authority

DRAFT

resides outside the control of the enforcement authority, agencies often proceed without the involvement, expertise, guidance, and judgment of the prosecutor. Failure to place subpoena authority with the enforcement authority can also lead to inconsistent, overly aggressive, and potentially improper investigations and prosecutions. So far as we can determine, the FDA does not have subpoena authority with respect to other criminal enforcement matters.

It would be unwise, in our view, to depart from this traditional practice and grant the FDA subpoena authority as to online pharmacies, a new technology governed by a complex statute, the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 301 *et seq.* With all the new, cutting-edge legal and policy issues raised by the proposed legislation, subpoena authority should remain with the Department. To the extent that the Administration seeks to create subpoena authority to assist in the investigation of online pharmacies, that can be accomplished by placing such authority within the Department. Moreover, to the extent the FDA seeks additional tools with which to audit and inspect the books and records of online pharmacy operators -- which we wholeheartedly support -- that can be achieved short of providing subpoena authority.

There is also a related issue with respect to the enforcement of the subpoenas that are to be issued. Section 503B(f)(2), entitled "Judicial Enforcement," refers to enforcement in federal court "upon application by the Commissioner." It is unclear whether this provision seeks to divest the Attorney General of her well-established authority to represent the United States in federal court. If that is the intent of this provision, we strongly oppose it. In any event, we do not believe such language is sufficient to divest the Department of its litigating authority, but to eliminate any such uncertainty, we recommend making it explicit that the Attorney General has the authority to enforce Department-issued subpoenas.

II. DOJ Suggestions for Improving the Bill

The Department offers the following suggestions for improving the proposed legislation.

1. Offshore Online Pharmacies

The proposed legislation should explicitly include pharmacies located overseas, which currently offer drugs to citizens of the United States. While the definition of "Online Pharmacy" is not restricted to those operating in the United States, we believe an explicit reference to extraterritorial application would avoid any uncertainties. For this reason, we would recommend adding a section at the end of the bill stating

DR

"Extraterritorial jurisdiction shall exist for violations of Section 503B if the online pharmacy operates, in interstate or foreign commerce or within the special maritime and territorial jurisdiction of the United States, or otherwise engages in commerce with an individual located within the United States."

2. Prohibition on Online Questionnaires

Section 503B(b)(4)(B) prohibits dispensing a prescription drug to an individual if the prescription is based "primarily on an online questionnaire or a similar document concerning the patient's current condition or medical history." The Department agrees that a prescription should not be based on an online questionnaire, but we believe this formulation will be easy to evade and is not sufficiently supple to account for advances in technology. For example, by describing what is not a valid prescription in very narrow terms, the proposed language could be evaded by an exchange of e-mails between a doctor and someone seeking a prescription; in that instance, the physician or other prescriber could claim that he or she relied "primarily" on the contents of the email rather than the questionnaire, thus easily defeating the narrow definition in the bill.

We leave alternative formulations to others more expert in this area, although one alternative may be to state that a prescription is valid only if "based on a legitimate practitioner-patient relationship." In our view, such a broadly-worded formulation would encompass changing circumstances and technology better than a narrow definition based on a current problem.

3. Information Regarding Doctors and Other Prescribers

Section 503B(b)(5) would require online pharmacies to post on their websites information regarding where it is located and licensed and the "name, professional degree and licensure of the pharmacist who is in charge." But no similar information must be posted for any prescriber who may be writing prescriptions or assisting in issuing prescriptions for consumers through the website. To the extent that online pharmacies offer consumers the services of a person authorized by law to write prescriptions (such as a doctor, dentist, or nurse-practitioner), the website should be obligated to post information analogous to that required to be posted concerning the pharmacist.

4. Applicable State Law

Section 503B(b)(3) of the draft bill requires pharmacies to comply with all "applicable requirements of federal and state law governing the practice of pharmacy."

DRAFT

The section does not define which states' laws are included – is it the laws of all states where the consumer, website, doctor, and/or pharmacist are located? This should be clarified.

Similarly, section 503B(4)(A) requires an online pharmacy to "ensure" that prescription drugs are dispensed pursuant to prescriptions that are valid under the laws of the state "where the individual is located." The draft bill does not identify who the "individual" is intended to be, though it appears to refer to the individual to whom the drug is dispensed, that is, the consumer. Again, this should be made more explicit.

5. Delegation of Functions to the States

Section 503B(e) authorizes the Secretary to designate state agencies to perform certain functions, including examinations and inspections of records, on behalf of the Secretary. While the language is permissive as to the Secretary's power to designate, we recommend clarifying that State agencies are free to accept or reject any designation to conduct these examinations and inspections. While this appears to be the intent of the draft bill, such clarification would be useful to remove any federalism and Tenth Amendment concerns.

6. Civil Enforcement by States

The proposed legislation should also require that States notify the Department of Justice regarding filing of civil enforcement actions, and the legislation should define the scope of relief available in State-initiated actions.

Section 503B(h) creates a state cause of action by which State attorneys general could bring civil actions to enforce section 503B. It is essential that the Department of Justice have notice of the action before it is filed, and the right to participate in the litigation by intervention and appeal. Such rights are given to the Federal Trade Commission (an independent agency with its own litigating authority) in analogous situations by the Telephone Disclosure and Dispute Resolution Act, 15 U.S.C. § 5712(b), and by the Credit Repair Organizations Act, 15 U.S.C. § 1679h(c)(2). These protections would allow the Department to participate in litigation that may be crucial in the development of case law interpreting the section.

7. Use of the Term "interstate commerce"

Section 503B(i) provides "The use of the Internet by an online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug is

DRAFT

deemed to be a transaction in interstate commerce." Because the term "interstate commerce" is not referred to elsewhere in the draft bill, it is unclear what purpose this subsection serves. To the extent that it is included as a justification for Congress' authority to legislate in this area, we recommend that it be mentioned in the beginning of the bill in a subsection describing Congress' findings. We also recommend that, instead of using the "deemed" construction, the subsection read as follows: "The Internet is an instrumentality of interstate commerce, and the use of the Internet by an online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug affects interstate commerce."

8. Civil Penalties

The draft bill provides for a civil penalty of \$500,000 per violation. This is an exceedingly stiff per-violation civil penalty, particularly for a "new" federal civil offense. We are aware of very few civil penalties in this dollar range. We would recommend a lower per-violation penalty, at least in the context of this regulatory certification process.

In addition, whatever amount is ultimately selected as the per-violation civil penalty, we recommend amending the bill to provide the courts with guidance on what factors they should consider in determining the amount of the penalty to impose. Other statutes imposing far less severe civil penalties list such factors, which aid courts or agencies in determining the appropriate penalty. *E.g.*, 15 U.S.C. § 45(m)(1)(C) (FTC Act - court to consider degree of culpability, history of such conduct, ability to pay, effect on business, and other matters as justice may require); 15 U.S.C. § 2069(b) (CPSC Act - Commission to consider nature of product defect, severity of risk of injury, occurrence of injury, number of defective products, and size of business of person charged). We recommend inserting a similar provision into this bill that could include these and/or other factors, such as economic benefit to the violator.

9. Tolling the Effective Date in the Event of Certification Backlog

The bill provides an effective date one year after enactment. Due process requires some mechanism to ensure that online pharmacies that are operating when the legislation is enacted and that satisfy statutory and regulatory standards are not exposed to liability simply because the Secretary is unable to complete the necessary certifications before the penalties become effective. To address this due process issue, a sentence could be added to section 2(d) such as, "To the extent that the Secretary requires additional time to complete the determinations of compliance for online pharmacies operating at the time of the statute's enactment, the Secretary may postpone the effective date of these amendments." Alternatively, the bill could provide that proof of compliance with the

DRAFT

statutory and regulatory standards is an affirmative defense for online pharmacies operating at the time of the statute's enactment and awaiting a determination of compliance by the Secretary.

10. Harmonization of Penalties Provisions with Existing Law

With respect to the relationship to existing law, a provision should be inserted stating that "the civil and criminal remedies provided in this section are in addition to, and do not displace, any statutes, regulations, or remedies under existing federal, state, or local law." This would make it clear that online pharmacies must continue to comply with all other federal and state laws.

11. False Statements

Any false statements made in the course of the certification process would presumably be subject to sanctions under 18 U.S.C. § 1001. Nevertheless, it would be useful to have a separate criminal provision targeted at false statements made in the certification process. See 18 U.S.C. §§ 1007, 1010, 1011, 1012, and 1014 for examples of statutes prohibiting false statements in particular circumstances.

Thank you for requesting our views. If further assistance on this matter is needed, please do not hesitate to contact this office.

Sincerely,

DRAFT

Robert Raben
Assistant Attorney General



Brad Sherman
Congress of the United States

24th District, California

SERVING THE SAN FERNANDO AND CONEJO VALLEYS,
THE MOUNTAIN COMMUNITIES AND MALIBU

COMMITTEES:

BANKING AND FINANCIAL
SERVICES

INTERNATIONAL RELATIONS

SUBCOMMITTEES:

INTERNATIONAL ECONOMIC
POLICY AND TRADE

WESTERN HEMISPHERE

FAX COVER SHEET

TO: Chris Jennings

FAX NUMBER: 456-5557

FROM: Congressman Sherman

DATE: 3/15/2000

REGARDING: _____

COMMENTS:

Number of pages including cover sheet 7

Please call 202-225-5911 if you have problems receiving this transmission.

WASHINGTON OFFICE:
1524 LONGWORTH BUILDING
WASHINGTON, DC 20515-0524
(202) 225-5911
FAX (202) 225-5879

PRIMARY DISTRICT OFFICE:
21031 VENTURA BOULEVARD, SUITE 1010
WOODLAND HILLS 91364-6400
(818) 999-1990
FAX (818) 999-2287

CONEJO VALLEY OFFICE:
2100 E. THOUSAND OAKS BLVD., SUITE F
THOUSAND OAKS 91362-2903
(805) 449-2372
FAX (805) 449-2376



Brad Sherman
Member of Congress

WASHINGTON OFFICE:
1524 LONGWORTH BUILDING
WASHINGTON, DC 20515-0524
(202) 225-5911
FAX (202) 225-5879

PRIMARY DISTRICT OFFICE:
21031 VENTURA BOULEVARD, SUITE 1010
WOODLAND HILLS 91364-6400
(818) 998-1990
FAX (818) 999-2287

CONEJO VALLEY OFFICE:
2100 E. THOUSAND OAKS BLVD., SUITE F
THOUSAND OAKS 91362-2903
(805) 448-2372
FAX (805) 448-2375

E-Mail: brad.sherman@mail.house.gov

Web site: <http://www.house.gov/sherman>

Information Hotline: (818) 999-1094 or (805) 497-4734



U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20415

OFFICE OF CHIEF COUNSEL FOR ADVOCACY

FEB 29 2000

Hon. Jans E. Henney, MD
Office of the Commissioner
Food and Drug Administration
5600 Fishers Lane
Rockville, MD 20857

Dear Commissioner Henney:

The Office of Advocacy of the U.S. Small Business Administration (SBA) was established by Congress pursuant to Pub. L. No. 94-305 to advocate the views of small business before federal agencies and Congress. Advocacy is also required by section 612(a) of the Regulatory Flexibility Act (RFA)¹ to monitor agency compliance with the RFA. In addition, the Chief Counsel of Advocacy is authorized to appear as *amicus curiae* in regulatory appeals from final agency actions, and is allowed to present views with respect to compliance with the RFA, the adequacy of the rulemaking record with respect to small entities, and the effect of the rule on small entities.² On March 28, 1996, President Clinton signed the Small Business Regulatory Enforcement Fairness Act (SBREFA)³ which made a number of significant changes to the RFA, including the provision to allow judicial review of agencies' compliance with the RFA.⁴

These comments are intended to focus attention on the severe economic impact that will be placed on the drug wholesale industry as a result of the final rule referenced above. Based on this severe impact, and pursuant to the Administrative Procedure Act (APA), the Office of Advocacy hereby petitions the Food and Drug Administration (FDA) to reconsider this final rule, suspend the effective date, and reissue regulations that will effectuate the intent of Congress with respect to the Prescription Drug Marketing Act of 1987 (PDMA).⁵

¹ 5 U.S.C. § 601 et seq.

² *Id.*

³ Pub. L. No. 104-121, 110 Stat. 857 (1996).

⁴ 5 U.S.C. § 611.

⁵ "Each agency shall give an interested person the right to petition for the issuance, amendment, or repeal of a rule." 5 U.S.C. § 553(e).



Background

On March 14, 1994, FDA proposed regulations entitled, "Prescription Drug Marketing Act of 1987; Prescription Drug Amendments of 1992 (PD Amendments); Policies, Requirements, and Administrative Procedures."⁶ The proposed regulations were designed to implement the (then) seven-year-old PDMA and the PD Amendments. The primary intent of the PDMA was to combat abuses involved in the distribution of prescription drugs.⁷ The PDMA contains drug pedigree requirements that impose prior sale documentation obligations on non-authorized distributors. Central to whether or not a business would have to comply with the documentation requirements was whether a business was "an authorized distributor of record" that maintained an "ongoing relationship" to distribute a manufacturer's products.

Subsequent to passage of the PDMA, FDA issued guidance on the meaning of "ongoing relationship" in the context of the manufacturer/wholesale distributor relationship. Clearly, the 1988 guidance demonstrated that "ongoing relationship" was to be interpreted broadly so that "authorized distributors of record" may be interpreted to mean a continuing business relationship in which it is intended that the wholesale distributor engage in wholesale distribution of a manufacturer's product. Among other criteria, the guidance indicated that the existence of two transactions in a two-year period would be presumptive evidence of a continuing relationship.

The PD Amendments of 1992 altered the pedigree requirements to increase the amount of information that had to be provided before each wholesale distribution of a drug. Under section 503(e) of the PDMA, the statement of prior sale now had to include the date of the transaction and the names and addresses of all parties to the transaction.

The most important thing to remember at this point is that Congress, in passing the PD Amendments, indicated no intent to alter either the definition of "authorized distributor of record" or FDA's guidance on the definition of "ongoing relationship."

The 1994 proposed regulations introduced a reversal of policy some six years after a standard for industry compliance had been established by FDA. For the first time, FDA would redefine "ongoing relationship" to mean:

"An association that exists when a manufacturer and a distributor enter into a written agreement under which the distributor is authorized to sell the manufacturer's products for a period of time or for a number of

⁶ 42 Fed. Reg. 11,842.

⁷ The PDMA requires the following: 1) more licensing of wholesale drug distributors; 2) a ban on the re-importation of prescription drugs produced in the U.S. (except when re-imported by the manufacturer or for emergencies); 3) a ban on the sale, trade or purchase of drug samples; 4) a ban on trafficking in or counterfeiting of drug coupons; 5) mandates on storage, handling and record keeping requirements for drug samples; 6) written practitioner requests for drug samples; 7) a prohibition on the resale of prescription drugs purchased by hospitals or other health care facilities; and, 8) criminal and civil penalties for violations.

⁸ Food and Drug Administration, Compliance Policy Guide 7356.022 (August 1, 1988).

shipments . . . and the name of the authorized distributor of record is entered on the manufacturer's list of authorized distributors of record."⁹

Thus, FDA is now requiring a written statement between a manufacturer and each authorized distributor, and that distributors appear on the manufacturer's list of authorized distributors. This may seem like a fairly innocuous change on its face; but in reality, the changes make it much harder to become an authorized distributor and give manufacturers the sole discretion to determine whom to designate as an "authorized distributor."

FDA's new scheme ignores the reality of the drug distribution chain that exist now under the statute. Secondary wholesale distributors will have to provide information about "each prior sale, purchase or trade of such drug . . . , starting with the manufacturer."¹⁰ This means that secondary distributors must provide a full pedigree even if that distributor purchased the drug from an authorized distributor, and even though the authorized distributor is under no legal obligation to provide a pedigree to secondary distributors. How is the secondary distributor to get the pedigree?

The industry raised these serious concerns described above in their 1994 comments to FDA.¹¹ The industry suggested, alternatively, that FDA revise the proposal to require that the pedigree only go back to the last authorized distributor of record—a seemingly reasonable solution. This recommendation was rejected and FDA has chosen to move forward with the final regulation without substantial change.

The Final Rule and Its Impact on Small Business

By FDA's own account, at least 4,000 small businesses (94% of the industry) will be affected by this rulemaking.¹² FDA, however, concluded that the impact would not be significant. In dismissing the industry's arguments to the contrary, FDA stated,

"Section 503(e)(1)(A) of the act [PDMA] requires that, prior to completion of a wholesale distribution of a prescription drug by a person who is not the manufacturer or an authorized distributor of the drug, a statement must be provided to the recipient identifying each prior sale, purchase, or trade of the drug, including the date of the transaction and the names and addresses of all parties to the transaction. There is no indication in PDMA that Congress intended that the statement include only those sales, purchases, or trades since the drug was last handled by an authorized distributor. Thus, an unauthorized distributor is required to provide a full drug origin statement in accordance with PDMA and the final rule whether or not it has purchased a prescription drug from an

⁹ 49 Fed. Reg. at 11,863.

¹⁰ 64 Fed. Reg. at 67,747.

¹¹ See Letter from the American Association of Pharmaceutical Distributors to the Food and Drug Administration (May 31, 1994).

¹² 64 Fed. Reg. at 67,753.

authorized distributor of record. Although the agency encourages authorized distributors to provide a drug origin statement to unauthorized distributors, they are not required to do so under PDMA or the final rule."

FDA apparently has not considered the possibility that Congress did not specifically prohibit the interpretation proposed by the industry. Nor has FDA taken into consideration the impact of abandoning its long standing guidance. In any event, FDA certainly has not provided a rational explanation for its reversal.

With regard to the written agreement whereby the manufacturer authorizes the distributor to distribute some or all of its products, FDA simply stated,

"Given the relative ease with which the agreement required by § 203.3(u) can be created, the agency believes that it is highly unlikely that a manufacturer would refuse to enter into a written agreement with a distributor with whom it wishes to have a continuing business relationship. Moreover, it is clearly not the agency's intent in requiring a written agreement to confer additional discretion on manufacturers, but rather to implement the requirement in the act for an ongoing relationship in a manner in which it can be efficiently enforced."¹³

Again, this response ignores the reality of the relationship between secondary drug wholesalers and manufacturers. The drug wholesalers are entirely at the mercy of manufacturers. The fact that an agreement is easily created is irrelevant if the manufacturer chooses to limit whom it considers authorized dealers. Moreover, the fact that FDA does not intend to confer additional discretion on manufacturers, does nothing to change the fact that the door is open for manufacturers to "cherry pick" and create a situation where secondary marketers are eliminated and consumer prices more easily increased.

FDA's responses to the industry are unacceptable. The final rule was modified to remove the requirement for a completed sale under the written agreement; however, FDA's responses largely ignore obvious impacts on the industry. First, according to industry experts, authorized wholesalers (even large ones) are not now able to and could not, at any reasonable cost, provide pedigrees to those to whom they distribute drugs. Moreover, because they are authorized distributors of record, they are not required to do so. Second, wholesalers buying from full line wholesalers that do not provide a pedigree will not be able to pass along to their customers a pedigree describing transactional information back to the manufacturer. And, third, full line wholesalers who now buy from the secondary market will not be able to do so because the secondary market will not be able to provide them with pedigrees back to the manufacturer.

All of the above will be exacerbated by FDA's final regulation requirement that there be a writing from the manufacturer to the distributor indicating that it is an authorized distributor. In the past, FDA accepted two transactions in two years between a

¹³ 64 Fed. Reg. at 67,728.

wholesaler and a manufacturer as evidence that a distributor is authorized. Now, such transactions will not be sufficient. This will further restrict the secondary market. Even as the market stands now, some manufacturers refuse to do business with wholesaler to prevent them from claiming "authorized" status.

In the end, serious disruption can be expected in the prescription drug distribution system—resulting in less competition, higher prices and lost jobs.

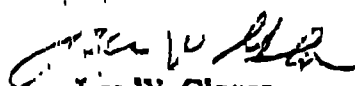
Unanticipated Impact

Not even the industry anticipated all of the adverse impacts that would be associated with implementation of this regulation. Drug products now in the inventory of wholesalers will have to be cleared out and new orders will have to cease or be severely limited in order to comply with the December 4, 2000 effective date. Unless distributors have relief by this summer, disruptions could begin to appear then. The Office of Advocacy has a letter from one Texas manufacturer that underscores this possibility, "we are modifying our procedures for reviewing pedigrees to ensure we are closer to following the new regulations which take effect on December 4th, 2000. Beginning on March 1st, 2000 all invoices received without a complete pedigree will not be paid." The problem, therefore, needs to be addressed immediately.

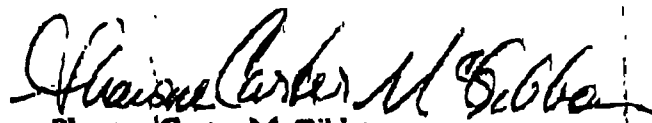
Conclusion

Again, the Office of Advocacy petitions FDA to reconsider its decisions underlying this regulation and to suspend implementation immediately until the impacts are more carefully studied and understood by FDA, and adjustments are made to avoid adverse disruptions. FDA should reissue the regulation after a more thorough review of impacts. Advocacy believes that this approach is consistent with congressional intent and is consistent with the agency's objective to ensure that suspect products do not enter the distribution system. Please do not hesitate to contact my office if you have any questions, 202-205-6533.

Sincerely,



Jere W. Glover
Chief Counsel for Advocacy



Shawn Carter McGibbon
Asst. Chief Counsel for Advocacy

The Honorable Jacob J. Lew
Director
Office of Management and Budget
Washington, D.C. 20503

Dear Mr. Lew:

This letter presents the views of the Department of Justice on the draft legislation proposed by the Department of Health and Human Services, the "Internet Prescription Drug Sales Act of 2000." The Department strongly supports much of this bill, particularly to the extent it treats online and offline conduct in a consistent manner. *See* Report of the President's Working Group on Unlawful Conduct on the Internet at 11-12 (regulation of unlawful conduct should "apply in the same way to conduct in the cyberworld as it does to conduct in the physical world"). However, as we explain in Part I, the Department strongly opposes the administrative subpoena and judicial enforcement provisions of the proposed bill, which would provide the Food and Drug Administration (FDA) with authority that it does not possess with respect to traditional, brick-and-mortar pharmacies. In Part II, we identify other concerns and offer suggestions on how the bill may be improved and clarified.

I. Subpoena Authority and Enforcement

The Department objects to the administrative subpoena authority and enforcement provisions in the proposed bill.

Section 503(B)(f) of the bill would give FDA the power to issue subpoenas for just about any purpose – "for the purpose of any audit, investigation, examination, analysis, review, evaluation, determination of compliance, or other proceeding with respect to this section[.]" The Department strongly opposes giving FDA such authority. As we have informed the FDA, the Department's longstanding policy is that subpoena authority should in nearly every instance reside with the prosecuting enforcement authority, not the

investigative agency. In our long experience, when subpoena authority resides outside the control of the enforcement authority, agencies often proceed without the involvement, expertise, guidance, and judgment of the prosecutor. Failure to place subpoena authority with the enforcement authority can also lead to inconsistent, overly aggressive, and potentially improper investigations and prosecutions. So far as we can determine, the FDA does not have subpoena authority with respect to other criminal enforcement matters.

It would be unwise, in our view, to depart from this traditional practice and grant the FDA subpoena authority as to online pharmacies, a new technology governed by a complex statute, the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 301 *et seq.* With all the new, cutting-edge legal and policy issues raised by the proposed legislation, subpoena authority should remain with the Department. To the extent that the Administration seeks to create subpoena authority to assist in the investigation of online pharmacies, that can be accomplished by placing such authority within the Department. Moreover, to the extent the FDA seeks additional tools with which to audit and inspect the books and records of online pharmacy operators -- which we wholeheartedly support - - that can be achieved short of providing subpoena authority.

There is also a related issue with respect to the enforcement of the subpoenas that are to be issued. Section 503B(f)(2), entitled "Judicial Enforcement," refers to enforcement in federal court "upon application by the Commissioner." It is unclear whether this provision seeks to divest the Attorney General of her well-established authority to represent the United States in federal court. If that is the intent of this provision, we strongly oppose it. In any event, we do not believe such language is sufficient to divest the Department of its litigating authority, but to eliminate any such uncertainty, we recommend making it explicit that the Attorney General has the authority to enforce Department-issued subpoenas.

II. DOJ Suggestions for Improving the Bill

The Department offers the following suggestions for improving the proposed legislation.

1. Offshore Online Pharmacies

The proposed legislation should explicitly include pharmacies located overseas, which currently offer drugs to citizens of the United States. While the definition of "Online Pharmacy" is not restricted to those operating in the United States, we believe an explicit reference to extraterritorial application would avoid any uncertainties. For this

reason, we would recommend adding a section at the end of the bill stating “Extraterritorial jurisdiction shall exist for violations of Section 503B if the online pharmacy operates, in interstate or foreign commerce or within the special maritime and territorial jurisdiction of the United States, or otherwise engages in commerce with an individual located within the United States.”

2. Prohibition on Online Questionnaires

Section 503B(b)(4)(B) prohibits dispensing a prescription drug to an individual if the prescription is based "primarily on an online questionnaire or a similar document concerning the patient's current condition or medical history." The Department agrees that a prescription should not be based on an online questionnaire, but we believe this formulation will be easy to evade and is not sufficiently supple to account for advances in technology. For example, by describing what is not a valid prescription in very narrow terms, the proposed language could be evaded by an exchange of e-mails between a doctor and someone seeking a prescription; in that instance, the physician or other prescriber could claim that he or she relied "primarily" on the contents of the email rather than the questionnaire, thus easily defeating the narrow definition in the bill.

We leave alternative formulations to others more expert in this area, although one alternative may be to state that a prescription is valid only if "based on a legitimate practitioner-patient relationship." In our view, such a broadly-worded formulation would encompass changing circumstances and technology better than a narrow definition based on a current problem.

3. Information Regarding Doctors and Other Prescribers

Section 503B(b)(5) would require online pharmacies to post on their websites information regarding where it is located and licensed and the “name, professional degree and licensure of the pharmacist who is in charge.” But no similar information must be posted for any prescriber who may be writing prescriptions or assisting in issuing prescriptions for consumers through the website. To the extent that online pharmacies offer consumers the services of a person authorized by law to write prescriptions (such as a doctor, dentist, or nurse-practitioner), the website should be obligated to post information analogous to that required to be posted concerning the pharmacist.

4. Applicable State Law

Section 503B(b)(3) of the draft bill requires pharmacies to comply with all “applicable requirements of federal and state law governing the practice of pharmacy.”

The section does not define which states' laws are included – is it the laws of all states where the consumer, website, doctor, and/or pharmacist are located? This should be clarified.

Similarly, section 503B(4)(A) requires an online pharmacy to “ensure” that prescription drugs are dispensed pursuant to prescriptions that are valid under the laws of the state “where the individual is located.” The draft bill does not identify who the “individual” is intended to be, though it appears to refer to the individual to whom the drug is dispensed, that is, the consumer. Again, this should be made more explicit.

5. Delegation of Functions to the States

Section 503B(e) authorizes the Secretary to designate state agencies to perform certain functions, including examinations and inspections of records, on behalf of the Secretary. While the language is permissive as to the Secretary's power to designate, we recommend clarifying that State agencies are free to accept or reject any designation to conduct these examinations and inspections. While this appears to be the intent of the draft bill, such clarification would be useful to remove any federalism and Tenth Amendment concerns.

6. Civil Enforcement by States

The proposed legislation should also require that States notify the Department of Justice regarding filing of civil enforcement actions, and the legislation should define the scope of relief available in State-initiated actions.

Section 503B(h) creates a state cause of action by which State attorneys general could bring civil actions to enforce section 503B. It is essential that the Department of Justice have notice of the action before it is filed, and the right to participate in the litigation by intervention and appeal. Such rights are given to the Federal Trade Commission (an independent agency with its own litigating authority) in analogous situations by the Telephone Disclosure and Dispute Resolution Act, 15 U.S.C. § 5712(b), and by the Credit Repair Organizations Act, 15 U.S.C. § 1679h(c)(2). These protections would allow the Department to participate in litigation that may be crucial in the development of case law interpreting the section.

7. Use of the Term “interstate commerce”

Section 503B(i) provides “The use of the Internet by an online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug is deemed to be

a transaction in interstate commerce.” Because the term “interstate commerce” is not referred to elsewhere in the draft bill, it is unclear what purpose this subsection serves. To the extent that it is included as a justification for Congress' authority to legislate in this area, we recommend that it be mentioned in the beginning of the bill in a subsection describing Congress' findings. We also recommend that, instead of using the "deemed" construction, the subsection read as follows: "The Internet is an instrumentality of interstate commerce, and the use of the Internet by an online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug affects interstate commerce."

8. Civil Penalties

The draft bill provides for a civil penalty of \$500,000 per violation. This is an exceedingly stiff per-violation civil penalty, particularly for a “new” federal civil offense. We are aware of very few civil penalties in this dollar range. We would recommend a lower per-violation penalty, at least in the context of this regulatory certification process.

In addition, whatever amount is ultimately selected as the per-violation civil penalty, we recommend amending the bill to provide the courts with guidance on what factors they should consider in determining the amount of the penalty to impose. Other statutes imposing far less severe civil penalties list such factors, which aid courts or agencies in determining the appropriate penalty. *E.g.*, 15 U.S.C. § 45(m)(1)(C) (FTC Act - court to consider degree of culpability, history of such conduct, ability to pay, effect on business, and other matters as justice may require); 15 U.S.C. § 2069(b) (CPSC Act - Commission to consider nature of product defect, severity of risk of injury, occurrence of injury, number of defective products, and size of business of person charged). We recommend inserting a similar provision into this bill that could include these and/or other factors, such as economic benefit to the violator.

9. Tolling the Effective Date in the Event of Certification Backlog

The bill provides an effective date one year after enactment. Due process requires some mechanism to ensure that online pharmacies that are operating when the legislation is enacted and that satisfy statutory and regulatory standards are not exposed to liability simply because the Secretary is unable to complete the necessary certifications before the penalties become effective. To address this due process issue, a sentence could be added to section 2(d) such as, "To the extent that the Secretary requires additional time to complete the determinations of compliance for online pharmacies operating at the time of the statute's enactment, the Secretary may postpone the effective date of these amendments." Alternatively, the bill could provide that proof of compliance with the

statutory and regulatory standards is an affirmative defense for online pharmacies operating at the time of the statute's enactment and awaiting a determination of compliance by the Secretary.

10. Harmonization of Penalties Provisions with Existing Law

With respect to the relationship to existing law, a provision should be inserted stating that "the civil and criminal remedies provided in this section are in addition to, and do not displace, any statutes, regulations, or remedies under existing federal, state, or local law." This would make it clear that online pharmacies must continue to comply with all other federal and state laws.

11. False Statements

Any false statements made in the course of the certification process would presumably be subject to sanctions under 18 U.S.C. § 1001. Nevertheless, it would be useful to have a separate criminal provision targeted at false statements made in the certification process. *See* 18 U.S.C. §§ 1007, 1010, 1011, 1012, and 1014 for examples of statutes prohibiting false statements in particular circumstances.

Thank you for requesting our views. If further assistance on this matter is needed, please do not hesitate to contact this office.

Sincerely,

Robert Raben
Assistant Attorney General



Richard Durbin

UNITED STATES SENATOR ■ ILLINOIS

FAX

TO: Chris Jennings

OFFICE: _____

FAX NO: () 456-5557

FROM: Tom Faletti

PHONE: (202) 224-7017

DATE: 3-14-00

PAGES (including this cover sheet): 2

NOTE: FYI - sent today.

United States Senate

WASHINGTON, DC 20510

March 14, 2000

The President
The White House
Washington, DC 20500

Dear Mr. President:

We are writing to express our concern about an effort by the state of Arkansas to obtain a Medicaid waiver that would allow the state to enroll its Medicaid-eligible children in a program with higher co-payments and a more restrictive benefit package than regular Medicaid.

Any decision to grant Arkansas such a waiver has national implications. In 1995, Democrats united to maintain the Medicaid program's commitment to provide a comprehensive package of benefits to low-income children. We should not allow states to undermine the Medicaid program by channeling people into a Medicaid waiver program or separate state program that imposes cost sharing and provides fewer benefits. If low-income children are enrolled in a program with co-payments for most doctor visits and without the protection of Medicaid's full EPSDT benefit package, those children are less likely to receive the full range of services they need to stay well or get well quickly. This is a particular concern for disabled children with chronic health care needs.

If Arkansas is granted this waiver, this precedent could be used to defend similar actions in Illinois, New York, and other states, which would put the health of low-income and disabled children in Illinois and elsewhere in jeopardy.

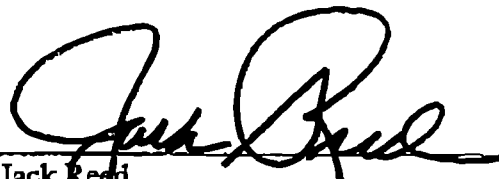
It is our understanding that these and other concerns led to an earlier decision to reject Arkansas' approach. We urge you to continue the Administration's stand for children by reaffirming the importance of full Medicaid coverage for Medicaid-eligible children in Arkansas, Illinois, and all across the nation.

Thank you for your longstanding commitment to quality health care for children and for your consideration of the national implications of this proposed waiver.

Sincerely,



Richard J. Durbin
United States Senator



Jack Reed
United States Senator



Richard Durbin

UNITED STATES SENATOR ■ ILLINOIS

FAX

TO: Chris Jennings

OFFICE: _____

FAX NO: () 456-5557

FROM: Tom Faletti

PHONE: (202) 224-7017

DATE: 3-14-00

PAGES (including this cover sheet): 2

NOTE: FYI - sent today.

United States Senate

WASHINGTON, DC 20510

March 14, 2000

The President
The White House
Washington, DC 20500

Dear Mr. President:

We are writing to express our concern about an effort by the state of Arkansas to obtain a Medicaid waiver that would allow the state to enroll its Medicaid-eligible children in a program with higher co-payments and a more restrictive benefit package than regular Medicaid.

Any decision to grant Arkansas such a waiver has national implications. In 1995, Democrats united to maintain the Medicaid program's commitment to provide a comprehensive package of benefits to low-income children. We should not allow states to undermine the Medicaid program by channeling people into a Medicaid waiver program or separate state program that imposes cost sharing and provides fewer benefits. If low-income children are enrolled in a program with co-payments for most doctor visits and without the protection of Medicaid's full EPSDT benefit package, those children are less likely to receive the full range of services they need to stay well or get well quickly. This is a particular concern for disabled children with chronic health care needs.

If Arkansas is granted this waiver, this precedent could be used to defend similar actions in Illinois, New York, and other states, which would put the health of low-income and disabled children in Illinois and elsewhere in jeopardy.

It is our understanding that these and other concerns led to an earlier decision to reject Arkansas' approach. We urge you to continue the Administration's stand for children by reaffirming the importance of full Medicaid coverage for Medicaid-eligible children in Arkansas, Illinois, and all across the nation.

Thank you for your longstanding commitment to quality health care for children and for your consideration of the national implications of this proposed waiver.

Sincerely,



Richard J. Durbin
United States Senator



Jack Reed
United States Senator

A BILL

To amend the Federal Food, Drug, and Cosmetic Act to provide for regulation of sales of prescription drugs on the Internet, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Internet Prescription Drug Sales Act of 2000".

SEC. 2. REGULATION OF INTERNET PRESCRIPTION DRUG SALES.

(a) IN GENERAL.—Chapter V of the Federal Food, Drug, and Cosmetic Act is amended by adding after section 503A the following new section:

"SEC. 503B. INTERNET PRESCRIPTION DRUG SALES.

“(a) DEFINITIONS.—

"(1) INTERNET.— The term 'Internet' means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

"(2) CONSUMER.—The term 'consumer' means a person (other than a pharmacy or other entity licensed under state or federal law to purchase prescription drugs for resale) that purchases or seeks to purchase prescription drugs through the Internet.

"(3) ONLINE PHARMACY.— The term 'online pharmacy' means a person that engages in, offers to engage in, or causes the delivery or sale of a prescription drug to a

consumer through the Internet.

"(4) PRESCRIPTION DRUG.— The term 'prescription drug' has the meaning given the term in section 503(b)(1).

"(b) REQUIREMENTS FOR ONLINE PHARMACIES.—

"(1) IN GENERAL.—Each online pharmacy shall demonstrate ~~to the Secretary's satisfaction that it complies and will continue to comply~~ **that it complies** with the requirements of this subsection with respect to the delivery or sale of prescription drugs through the Internet, and shall at all times display on the homepage of its Internet website a **demonstration** ~~declaration of the Secretary's determination~~ of compliance, in such form as the Secretary may require. ~~(and including such seal, symbol, or other evidence of such determination of compliance as the Secretary may specify).~~

"(2) LICENSURE.—The online pharmacy must be licensed to practice pharmacy in each State in which it operates, and in each State to which it delivers or offers to deliver prescription drugs ordered on the Internet.

"(3) COMPLIANCE WITH FEDERAL AND STATE LAWS.—The online pharmacy must comply with all applicable requirements of Federal and State law governing the practice of pharmacy.

"(4) REQUIREMENT OF VALID PRESCRIPTION.—The online pharmacy must ensure that each prescription drug dispensed to an individual is based on a prescription—

"(A) that is valid under the laws of the State in which the individual is located; ~~and~~

~~"(B) that is pursuant to a relationship between the individual and prescribing health care practitioner that is not based primarily on an online questionnaire or a similar document concerning the patient's current condition or medical history."~~

"(5) WEBSITE DISCLOSURE INFORMATION.—The online pharmacy must post **in a visible and clear manner** on the homepage of its Internet website or on a page directly linked to its homepage the following:

"(A) the name (or names) of the online pharmacy or pharmacies identified on its license (or licenses) in each State in which it is licensed to engage in the practice of pharmacy;

"(B) the street address of the online pharmacy's principal place of business;

"(C) the name, professional degree, and licensure of the pharmacist in charge;

"(D) a telephone number or numbers at which a licensed pharmacist may be contacted;

"(E) a list of the States in which the online pharmacy is licensed to dispense prescription drugs and the applicable license numbers; and

“(F) a declaration that the online pharmacy will dispense prescription drugs only upon a valid prescription by a licensed practitioner and only to an individual located in a State in which the online pharmacy is licensed to dispense such drugs.

(6) NOTIFICATION: On-line pharmacies must notify the relevant state authorities and FDA prior to launching any website. On-line pharmacies that are already operational as of the effective date of this Act, must notify relevant state authorities and the FDA within six months of the effective date of this act.

“(c) FAILURE TO COMPLY WITH REQUIREMENTS OF ACT ---EFFECTIVE PERIOD OF DETERMINATION.---

~~“(1) IN GENERAL. Subject to paragraph (2), a determination by the Secretary under subsection (b) shall be effective for a period of two years from the date of the determination.~~

~~“(2) WITHDRAWAL OF DETERMINATION. The Secretary may withdraw a determination of compliance under subsection (b) If, at any time, the Secretary finds that an online pharmacy fails to meet any of the requirements set forth in subsection (b) following an appropriate administrative process with full regard to the due process rights of the persons involved, Upon issuance of such withdrawal of determination, it shall be unlawful for the online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug to a consumer.~~

[NB -- I WOULD BE A LOT MORE COMFORTABLE DELETING THE ABOVE SECTION ALTOGETHER SINCE IT SUBSTANTIALLY STEPS ON STATE’S RIGHTS IN THIS AREA]

~~“(d) FEES. The Secretary is authorized to assess fees for determinations of compliance of online pharmacies under this section, in amounts not to exceed amounts that the Secretary finds to be sufficient in the aggregate to cover the costs (including costs for periodic inspections)~~

~~of such determinations. A determination of compliance of an online pharmacy shall not be effective until any applicable fee has been paid in full.~~

"(e) DESIGNATION OF EXAMINING ENTITY.—The Secretary may designate one or more private nonprofit organizations or State agencies to examine and inspect the records and facilities of applicants for a determination of compliance under this section. ~~Fees assessed under subsection (d) (or, as determined by the Secretary, an appropriate portion thereof) may be used to reimburse a designated entity for its costs related to such responsibilities.~~

"(f) SUBPOENAS.—

[REWRITE SECTION TO REFLECT TRANSFER OF SUBPOENA AUTHORITY TO DEPARTMENT OF JUSTICE]

"(1) COMMISSIONER'S AUTHORITY.— For the purpose of any audit, investigation, examination, analysis, review, evaluation, determination of compliance, or other proceeding with respect to this section, the Commissioner shall have power to sign and issue subpoenas to any person requiring the production of any books, records, or other documentary evidence. Subpoenas so issued by the Commissioner shall be served by anyone authorized by the Commissioner—

"(A) by delivering a copy thereof to the person named therein, or—

"(B) by registered mail or by certified mail addressed to such person at his or her last dwelling place or principal place of business. A verified return by the person so serving the subpoena setting forth the manner of service, or, in the case of service by registered mail or by certified mail, the return post office receipt therefor signed by the person so served, shall be proof of service.

"(2) JUDICIAL ENFORCEMENT.—In case of contumacy by, or refusal to obey or fully comply with a subpoena issued pursuant to paragraph (1) and duly served upon, any person, any district court of the United States for the judicial district in which such person charged with contumacy or refusal to obey is found or resides or transacts business, upon application by the Commissioner, shall have jurisdiction to issue an order requiring such person to produce the books, records, or other documentary evidence sought by the subpoena; and any failure to obey such order of the court may be punished by the court as a contempt thereof.

"(g) REGULATIONS.—The Secretary is authorized to promulgate such regulations as necessary to carry out the provisions of this section.

"(h) STATE CAUSE OF ACTION.—In any case in which the attorney general 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 the action of a person that violates the provisions of this section, the attorney general may bring a civil action on behalf of such residents in a district court of the United States with appropriate jurisdiction—

"(A) to enjoin such action;

"(B) to enforce compliance with this section;

"(C) to obtain damages, restitution, or other compensation; or

"(D) to obtain such other legal or equitable relief as the court may find appropriate.

"(i) INTERSTATE COMMERCE.— The use of the Internet by an online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug is deemed to be

a transaction in interstate commerce."

(b) PROHIBITED ACTS.—Section 301 of the Federal Food, Drug, and Cosmetic Act is amended by adding at the end the following new subsection:

'(aa) The violation of section 503B by—

**[REWRITE SECTION TO REFLECT CHANGES TO DETERMINATION AND SEALS
MADE ABOVE]**

"(1) operating an online pharmacy without a determination by the Secretary of compliance with the requirements of such section, without a seal or other required evidence of such determination, or otherwise in violation of the requirements set forth in section 503B(b);

"(2) dispensing a prescription drug in violation of section 503B; or

"(3) writing a prescription that is invalid under section 503B."

(c) PENALTIES.—Section 303 is amended by adding at the end the following new subsection:

"(h) Any person who violates the requirements of section 503B, as specified in section 301(aa), shall be subject to civil money penalties of up to \$500,000 per violation."

(d) EFFECTIVE DATE.—The amendments made by this Act shall become effective one year after the date of enactment.

[ADD A PROVISION THAT “directs the Secretary of Health and Human Services and the Secretary of Commerce to establish a joint process to consult with state authorities on ways to lessen the burden of requiring separate registration for each state, such as reciprocity or

mutual recognition, taking into account the states' traditional regulatory authority over pharmacies and the practice of medicine."

OFFICE OF MANAGEMENT AND BUDGET**Legislative Reference Division
Labor-Welfare-Personnel Branch****URGENT**

TO: Chris
Deborah
Dan

FROM: Robert Pellicci
Phone #: (202) 395-4871
Fax #: (202) 395-6148
E-mail Address: Robert_J_Pellicci@omb.eop.gov

Number of Pages (including cover page): 7

Date: 3/15 Time: 1 PM

Comments:

Advance Justice letter on
the internet drugs bill -
For today's meeting.



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

March 15, 2000

The Honorable Jacob J. Lew
Director
Office of Management and Budget
Washington, D.C. 20503

DRAFT

Dear Mr. Lew:

This letter presents the views of the Department of Justice on the draft legislation proposed by the Department of Health and Human Services, the "Internet Prescription Drug Sales Act of 2000." The Department strongly supports much of this bill, particularly to the extent it treats online and offline conduct in a consistent manner. See Report of the President's Working Group on Unlawful Conduct on the Internet at 11-12 (regulation of unlawful conduct should "apply in the same way to conduct in the cyberworld as it does to conduct in the physical world"). However, as we explain in Part I, the Department strongly opposes the administrative subpoena and judicial enforcement provisions of the proposed bill [which would provide the Food and Drug Administration (FDA) with authority that it does not possess with respect to traditional, brick-and-mortar pharmacies.] In Part II, we identify other concerns and offer suggestions on how the bill may be improved and clarified.

I. Subpoena Authority and Enforcement

The Department objects to the administrative subpoena authority and enforcement provisions in the proposed bill.

Section 503(B)(f) of the bill would give FDA the power to issue subpoenas for just about any purpose – "for the purpose of any audit, investigation, examination, analysis, review, evaluation, determination of compliance, or other proceeding with respect to this section[.]" The Department strongly opposes giving FDA such authority. As we have informed the FDA, the Department's longstanding policy is that subpoena authority should in nearly every instance reside with the prosecuting enforcement authority, not the investigative agency. In our long experience, when subpoena authority

DRAFT

resides outside the control of the enforcement authority, agencies often proceed without the involvement, expertise, guidance, and judgment of the prosecutor. Failure to place subpoena authority with the enforcement authority can also lead to inconsistent, overly aggressive, and potentially improper investigations and prosecutions. So far as we can determine, the FDA does not have subpoena authority with respect to other criminal enforcement matters.

It would be unwise, in our view, to depart from this traditional practice and grant the FDA subpoena authority as to online pharmacies, a new technology governed by a complex statute, the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 301 *et seq.* With all the new, cutting-edge legal and policy issues raised by the proposed legislation, subpoena authority should remain with the Department. To the extent that the Administration seeks to create subpoena authority to assist in the investigation of online pharmacies, that can be accomplished by placing such authority within the Department. Moreover, to the extent the FDA seeks additional tools with which to audit and inspect the books and records of online pharmacy operators -- which we wholeheartedly support -- that can be achieved short of providing subpoena authority.

There is also a related issue with respect to the enforcement of the subpoenas that are to be issued. Section 503B(f)(2), entitled "Judicial Enforcement," refers to enforcement in federal court "upon application by the Commissioner." It is unclear whether this provision seeks to divest the Attorney General of her well-established authority to represent the United States in federal court. If that is the intent of this provision, we strongly oppose it. In any event, we do not believe such language is sufficient to divest the Department of its litigating authority, but to eliminate any such uncertainty, we recommend making it explicit that the Attorney General has the authority to enforce Department-issued subpoenas.

II. DOJ Suggestions for Improving the Bill

The Department offers the following suggestions for improving the proposed legislation.

1. Offshore Online Pharmacies

OP
The proposed legislation should explicitly include pharmacies located overseas, which currently offer drugs to citizens of the United States. While the definition of "Online Pharmacy" is not restricted to those operating in the United States, we believe an explicit reference to extraterritorial application would avoid any uncertainties. For this reason, we would recommend adding a section at the end of the bill stating

DA

"Extraterritorial jurisdiction shall exist for violations of Section 503B if the online pharmacy operates, in interstate or foreign commerce or within the special maritime and territorial jurisdiction of the United States, or otherwise engages in commerce with an individual located within the United States."

2. Prohibition on Online Questionnaires

Section 503B(b)(4)(B) prohibits dispensing a prescription drug to an individual if the prescription is based "primarily on an online questionnaire or a similar document concerning the patient's current condition or medical history." The Department agrees that a prescription should not be based on an online questionnaire, but we believe this formulation will be easy to evade and is not sufficiently supple to account for advances in technology. For example, by describing what is not a valid prescription in very narrow terms, the proposed language could be evaded by an exchange of e-mails between a doctor and someone seeking a prescription; in that instance, the physician or other prescriber could claim that he or she relied "primarily" on the contents of the email rather than the questionnaire, thus easily defeating the narrow definition in the bill.

We leave alternative formulations to others more expert in this area, although one alternative may be to state that a prescription is valid only if "based on a legitimate practitioner-patient relationship." In our view, such a broadly-worded formulation would encompass changing circumstances and technology better than a narrow definition based on a current problem.

3. Information Regarding Doctors and Other Prescribers

Section 503B(b)(5) would require online pharmacies to post on their websites information regarding where it is located and licensed and the "name, professional degree and licensure of the pharmacist who is in charge." But no similar information must be posted for any prescriber who may be writing prescriptions or assisting in issuing prescriptions for consumers through the website. To the extent that online pharmacies offer consumers the services of a person authorized by law to write prescriptions (such as a doctor, dentist, or nurse-practitioner), the website should be obligated to post information analogous to that required to be posted concerning the pharmacist.

4. Applicable State Law

Section 503B(b)(3) of the draft bill requires pharmacies to comply with all "applicable requirements of federal and state law governing the practice of pharmacy."

DRAFT

The section does not define which states' laws are included – is it the laws of all states where the consumer, website, doctor, and/or pharmacist are located? This should be clarified.

Similarly, section 503B(4)(A) requires an online pharmacy to “ensure” that prescription drugs are dispensed pursuant to prescriptions that are valid under the laws of the state “where the individual is located.” The draft bill does not identify who the “individual” is intended to be, though it appears to refer to the individual to whom the drug is dispensed, that is, the consumer. Again, this should be made more explicit.

5. Delegation of Functions to the States

Section 503B(e) authorizes the Secretary to designate state agencies to perform certain functions, including examinations and inspections of records, on behalf of the Secretary. While the language is permissive as to the Secretary's power to designate, we recommend clarifying that State agencies are free to accept or reject any designation to conduct these examinations and inspections. While this appears to be the intent of the draft bill, such clarification would be useful to remove any federalism and Tenth Amendment concerns.

6. Civil Enforcement by States

The proposed legislation should also require that States notify the Department of Justice regarding filing of civil enforcement actions, and the legislation should define the scope of relief available in State-initiated actions.

Section 503B(h) creates a state cause of action by which State attorneys general could bring civil actions to enforce section 503B. It is essential that the Department of Justice have notice of the action before it is filed, and the right to participate in the litigation by intervention and appeal. Such rights are given to the Federal Trade Commission (an independent agency with its own litigating authority) in analogous situations by the Telephone Disclosure and Dispute Resolution Act, 15 U.S.C. § 5712(b), and by the Credit Repair Organizations Act, 15 U.S.C. § 1679h(c)(2). These protections would allow the Department to participate in litigation that may be crucial in the development of case law interpreting the section.

7. Use of the Term “interstate commerce”

Section 503B(i) provides “The use of the Internet by an online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug is

DRAFT

deemed to be a transaction in interstate commerce." Because the term "interstate commerce" is not referred to elsewhere in the draft bill, it is unclear what purpose this subsection serves. To the extent that it is included as a justification for Congress' authority to legislate in this area, we recommend that it be mentioned in the beginning of the bill in a subsection describing Congress' findings. We also recommend that, instead of using the "deemed" construction, the subsection read as follows: "The Internet is an instrumentality of interstate commerce, and the use of the Internet by an online pharmacy to engage in, offer to engage in, or cause the delivery or sale of a prescription drug affects interstate commerce."

8. Civil Penalties

The draft bill provides for a civil penalty of \$500,000 per violation. This is an exceedingly stiff per-violation civil penalty, particularly for a "new" federal civil offense. We are aware of very few civil penalties in this dollar range. We would recommend a lower per-violation penalty, at least in the context of this regulatory certification process.

In addition, whatever amount is ultimately selected as the per-violation civil penalty, we recommend amending the bill to provide the courts with guidance on what factors they should consider in determining the amount of the penalty to impose. Other statutes imposing far less severe civil penalties list such factors, which aid courts or agencies in determining the appropriate penalty. *E.g.*, 15 U.S.C. § 45(m)(1)(C) (FTC Act - court to consider degree of culpability, history of such conduct, ability to pay, effect on business, and other matters as justice may require); 15 U.S.C. § 2069(b) (CPSC Act - Commission to consider nature of product defect, severity of risk of injury, occurrence of injury, number of defective products, and size of business of person charged). We recommend inserting a similar provision into this bill that could include these and/or other factors, such as economic benefit to the violator.

9. Tolling the Effective Date in the Event of Certification Backlog

The bill provides an effective date one year after enactment. Due process requires some mechanism to ensure that online pharmacies that are operating when the legislation is enacted and that satisfy statutory and regulatory standards are not exposed to liability simply because the Secretary is unable to complete the necessary certifications before the penalties become effective. To address this due process issue, a sentence could be added to section 2(d) such as, "To the extent that the Secretary requires additional time to complete the determinations of compliance for online pharmacies operating at the time of the statute's enactment, the Secretary may postpone the effective date of these amendments." Alternatively, the bill could provide that proof of compliance with the

What brick & mortar pharmacies

"Internet Prescription Drug Sales Act of 2000"

Summary

SEC. 2. REGULATION OF INTERNET PRESCRIPTION DRUG SALES.

IN GENERAL.

Section 2(a) adds to chapter V of the Federal Food, Drug, and Cosmetic Act (the Act) a new section 503B (Internet Prescription Drug Sales) with the following provisions:

DEFINITIONS.

Section 503B(a) defines the terms "Internet", "consumer", "online pharmacy", and "prescription drug".

REQUIREMENTS FOR ONLINE PHARMACIES.

Subsection (b)(1) requires each online pharmacy to demonstrate to the Secretary's satisfaction that it complies with the requirements of this subsection, and to display on the homepage of its Internet website a ~~declaration of the Secretary's determination of~~ compliance, in such form as the Secretary may require. *regulate*

The remaining paragraphs of subsection (b) provide that the online pharmacy must:

(2) be licensed to practice pharmacy in each State in which it operates, and in each State to which it delivers or offers to deliver prescription drugs ordered on the Internet;

(3) comply with all applicable requirements of Federal and State law governing the practice of pharmacy;

(4) ensure that each prescription drug dispensed to an individual is based on a prescription that is (A) valid under the laws of the State in which the individual is located; and (B) based on a practitioner-patient relationship that involves more than use of an online questionnaire or similar document concerning the patient's current condition or medical history;

(5) post on its Internet homepage or a directly linked page: (A) the name (or names) of the online pharmacy or pharmacies identified on its license (or licenses) in each State in which it is licensed to engage in the practice of pharmacy; (B) the street address of its principal place of business; (C) the name, professional degree, and licensure

of the pharmacist in charge; (D) a telephone number or numbers at which a licensed pharmacist may be contacted; (E) a list of the States in which it is licensed to dispense prescription drugs and the applicable license numbers; and (F) a declaration that it will dispense prescription drugs only upon a valid prescription by a licensed practitioner and only to an individual located in a State in which it is licensed to dispense such drugs.

EFFECTIVE PERIOD OF DETERMINATION.

Subsection (c) provides that the Secretary's determination of compliance of an online pharmacy will be effective for a period of two years, except that the Secretary may withdraw the determination at any time upon finding that the pharmacy fails to meet any of the requirements of subsection (b).

FEES.

Subsection (d) authorizes the Secretary to assess fees for determinations of compliance of online pharmacies under this section, in amounts sufficient in the aggregate to cover the costs (including costs for periodic inspections) of such determinations. It further provides that a determination of compliance of an online pharmacy will not be effective until any applicable fee has been paid in full.

DESIGNATION OF EXAMINING ENTITY.

Subsection (e) authorizes the Secretary to designate private nonprofit organizations or State agencies to examine and inspect the records and facilities of online pharmacies seeking a determination of compliance. It further provides that fees assessed under subsection (d) (or a portion thereof) may be used to reimburse the costs of designated entities.

SUBPOENAS.

Subsection (f) authorizes the Commissioner of Food and Drugs, for the purpose of any audit, investigation, or other proceeding with respect to this section, to issue administrative subpoenas to any person requiring the production of any books, records, or other documentary evidence.

REGULATIONS.

Subsection (g) authorizes the Secretary to promulgate such regulations as necessary to carry out this section.

STATE CAUSE OF ACTION.

Subsection (h) permits a State attorney general to bring suit in United States district court, on behalf of residents of that State threatened or adversely affected by an action that violates this section, to enjoin such action; to enforce compliance with this section; to obtain damages, restitution, or other compensation; or to obtain such other relief as the court may find appropriate.

INTERSTATE COMMERCE.

Subsection (i) declares that the use of the Internet by an online pharmacy to engage in, offer to engage in, or cause the sale of a prescription drug is deemed to be a transaction in interstate commerce.

PROHIBITED ACTS.

Section 2(b) of the bill adds to section 301 of the Act a new subsection (aa), making it a prohibited act within the meaning of that section to violate new section 503B by (1) operating an online pharmacy without a determination of compliance by the Secretary, without a seal or other required evidence of the Secretary's determination of compliance, or otherwise in violation of the requirements set forth in section 503B(b); (2) dispensing a prescription drug in violation of section 503B; or (3) writing a prescription that is invalid under section 503B.

PENALTIES.

Section 2(c) of the bill adds to section 303 of the Act a new subsection (h), providing that any person who violates the requirements of section 503B, as specified in section 301(aa), shall be subject to civil money penalties of up to \$500,000 per violation.

EFFECTIVE DATE.

Section 2(d) provides that the bill's provisions will become effective one year after the date of enactment.

Medicaid Kids Enrollment: Change from 1996 to 1998

STATE	1996 Non-Disabled Children	1997 Non-Disabled Children	1998 Non-Disabled Children	96-97 Change	96-97 Percent Change	97-98 Change	97-98 Percent Change
ALL JURISDICTIONS	20,490,382	20,386,391	20,099,356	-103,991	-1%	-287,035	-1.4%
ALABAMA	296,107	324,253	331,073	28,146	10%	6,820	2.1%
ALASKA	49,784	46,242	48,619	-3,542	-7%	2,377	5.1%
ARIZONA	412,013	378,502	366,563	-33,511	-8%	-11,939	-3.2%
ARKANSAS	133,189	151,334	189,904	18,145	14%	38,570	25.5%
CALIFORNIA	3,110,773	3,333,143	3,230,432	222,370	7%	-102,711	-3.1%
COLORADO	175,643	175,416	173,628	-227	0%	-1,788	-1.0%
CONNECTICUT	201,085	201,119	207,306	34	0%	6,187	3.1%
DELAWARE	48,566	51,682	51,666	3,116	6%	-16	0.0%
DISTRICT OF COLUMBIA	74,079	72,762	68,025	-1,317	-2%	-4,737	-6.5%
FLORIDA	1,509,686	1,084,914	1,025,156	-424,772	-28%	-59,758	-5.5%
GEORGIA	691,067	693,452	695,133	2,385	0%	1,681	0.2%
HAWAII	n/a	n/a	n/a	n/a	n/a	n/a	n/a
IDAHO	72,505	65,659	67,466	-6,846	-9%	1,807	2.8%
ILLINOIS	937,590	1,029,258	955,011	91,668	10%	-74,247	-7.2%
INDIANA	344,361	326,722	344,153	-17,639	-5%	17,431	5.3%
IOWA	153,117	144,117	147,049	-9,000	-6%	2,932	2.0%
KANSAS	143,270	136,365	129,332	-6,905	-5%	-7,033	-5.2%
KENTUCKY	304,924	295,442	289,907	-9,482	-3%	-5,535	-1.9%
LOUISIANA	387,847	255,097	350,549	-132,750	-34%	95,452	37.4%
MAINE	84,714	89,202	89,248	4,488	5%	46	0.1%
MARYLAND	281,282	187,105	311,850	-94,177	-33%	124,745	66.7%
MASSACHUSETTS	356,014	352,314	464,409	-3,700	-1%	112,095	31.8%
MICHIGAN	697,523	706,043	569,400	8,520	1%	-136,643	-19.4%
MINNESOTA	350,859	335,862	316,538	-14,997	-4%	-19,324	-5.8%
MISSISSIPPI	278,342	263,929	259,140	-14,413	-5%	-4,789	-1.8%
MISSOURI	420,058	435,736	438,529	15,678	4%	2,793	0.6%
MONTANA	39,045	49,317	47,836	10,272	26%	-1,481	-3.0%
NEBRASKA	46,058	118,138	131,015	72,080	156%	12,877	10.9%
NEVADA	82,542	72,569	72,958	-9,973	-12%	389	0.5%
NEW HAMPSHIRE	56,829	60,439	58,633	3,610	6%	-1,806	-3.0%
NEW JERSEY	417,519	409,205	412,723	-8,314	-2%	3,518	0.9%
NEW MEXICO	215,370	218,809	223,053	3,439	2%	4,244	1.9%
NEW YORK	1,459,578	1,642,367	1,576,044	182,789	13%	-66,323	-4.0%

NORTH CAROLINA	569,203	630,600	633,496	61,397	11%	2,896	0.5%
NORTH DAKOTA	29,355	31,496	30,519	2,141	7%	-977	-3.1%
OHIO	815,020	698,713	687,773	-116,307	-14%	-10,940	-1.6%
OKLAHOMA	230,654	0	0	-230,654	-100%	0	NA
OREGON	114,841	234,806	154,045	119,965	104%	-80,761	-34.4%
PENNSYLVANIA	838,075	827,800	826,311	-10,275	-1%	-1,489	-0.2%
RHODE ISLAND	68,429	68,810	69,886	381	1%	1,076	1.6%
SOUTH CAROLINA	268,428	281,221	317,188	12,793	5%	35,967	12.8%
SOUTH DAKOTA	47,697	47,558	47,019	-139	0%	-539	-1.1%
TENNESSEE	459,331	595,401	558,090	136,070	30%	-37,311	-6.3%
TEXAS	1,665,087	1,663,606	1,565,407	-1,481	0%	-98,199	-5.9%
UTAH	118,172	119,680	119,480	1,508	1%	-200	-0.2%
VERMONT	57,914	60,022	59,568	2,108	4%	-454	-0.8%
VIRGINIA	394,180	381,694	364,938	-12,486	-3%	-16,756	-4.4%
WASHINGTON	515,458	521,931	536,223	6,473	1%	14,292	2.7%
WEST VIRGINIA	216,486	199,321	188,503	-17,165	-8%	-10,818	-5.4%
WISCONSIN	209,405	277,768	258,413	68,363	33%	-19,355	-7.0%
WYOMING	31,363	30,493	28,660	-870	-3%	-1,833	-6.0%
PUERTO RICO	n/a	n/a	n/a	n/a	n/a	n/a	n/a
VIRGIN ISLANDS	9,945	8,957	11,489	-988	-10%	2,532	28.3%



• FDA interstate
for mail •

**THE ELECTRONIC FRONTIER: THE CHALLENGE OF
UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET**
A Report of the President's Working Group
on Unlawful Conduct on the Internet

March 2000

TABLE OF CONTENTS

EXECUTIVE SUMMARY v

I. INTRODUCTION 1

- A. Executive Order 13,133 2
- B. The Working Group on Unlawful Conduct on the Internet 3
- C. Summary of Strategy 4

II. POLICY FRAMEWORK AND LEGAL ANALYSIS 5

- A. Understanding the Nature of Unlawful Conduct Involving Computers 7

- 1. Computers as Targets 7
- 2. Computers as Storage Devices 9
- 3. Computers as Communications Tools 9

- B. A Framework for Evaluating Unlawful Conduct on the Internet 11

- 1. Online-Offline Consistency 11
- 2. Appropriate Investigatory Tools 11
- 3. Technology-Neutrality 13
- 4. Consideration of Other Societal Interests 13

- C. Promoting Private Sector Leadership 14

- D. Sufficiency of Existing Federal Laws 17

- 1. Analysis of Substantive Laws 17
- 2. New Investigatory Challenges 19

III. LAW ENFORCEMENT NEEDS AND CHALLENGES 25

- A. Protecting Computers and Networks 25

- B. Federal Tools and Capabilities 26

• happening
state compliance

• alternative
subpoena

• rationale
for FDA

• Interstate
rules for
mail

• State
notification
as well as
federal

• prior
to
launch

• VA licensing

1. Personnel, Equipment, and Training 26
2. Locating and Identifying Cybercriminals 29
3. Collecting Evidence 33

C. State and Local Tools and Capabilities 34

1. Jurisdiction 34
2. Interstate and Federal-State Cooperation 35
3. Resources 36

D. Legal Authorities: Gaps in Domestic Laws 36

1. Pen Register and Trap and Trace Statute 37
2. Computer Fraud and Abuse Act 37
3. Privacy Protection Act 38
4. Electronic Communications Privacy Act 39
5. Telephone Harassment 40
6. Cable Communications Policy Act 40

E. Challenges for International Cooperation 41

1. Substantive International Criminal Law 41
2. Multilateral Efforts 42
3. Continuing Need for International Cooperation 42

IV. THE ROLE OF PUBLIC EDUCATION AND EMPOWERMENT 43

A. Educating and Empowering Parents, Teachers, and Children 43

1. Technological Tools 44
2. Non-technological Tools 46

B. Educating and Empowering Consumers 50

1. FTC Initiatives: Using Technology to Educate Consumers 51
2. Department of Commerce Initiatives 55
3. FDA's Outreach Campaign 55
4. SEC's Investor Education Efforts 56
5. CPSC's Consumer Outreach Efforts 56

C. Developing Cybercitizens 57

V. CONCLUSIONS AND RECOMMENDATIONS 58

APPENDICES

A EXECUTIVE ORDER 13,133

B INTERNET FRAUD

C ONLINE CHILD PORNOGRAPHY

D INTERNET SALE OF PRESCRIPTION DRUGS AND CONTROLLED SUBSTANCES

E INTERNET SALE OF FIREARMS

F INTERNET GAMBLING

G INTERNET SALE OF ALCOHOL

H ONLINE SECURITIES FRAUD
 I SOFTWARE PIRACY AND INTELLECTUAL PROPERTY THEFT
 J MULTILATERAL EFFORTS

**THE ELECTRONIC FRONTIER: THE CHALLENGE OF
 UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET**
**A Report of the President's Working Group
 on Unlawful Conduct on the Internet**
March 2000

EXECUTIVE SUMMARY

It should come as no surprise that the Internet is rapidly transforming the way we communicate, educate, and buy and sell goods and services. As the Internet's potential to provide unparalleled benefits to society continues to expand, however, its potential to serve as a powerful new medium for those who wish to commit unlawful acts has also grown.

Unlawful conduct involving the use of the Internet is just as intolerable as any other type of illegal activity. Ensuring the safety and security of those who use the Internet is thus a critical element of the Administration's overall policy regarding the Internet and electronic commerce, a policy that seeks to promote private sector leadership, technology-neutral laws and regulation, and an appreciation of the Internet as an important medium for commerce and communication both domestically and internationally. Indeed, the continued growth and maturation of this new medium depends on our taking a balanced approach that ensures that the Internet does not become a haven for unlawful activity.

"Unlawful is not unique to the Internet - but the Internet has a way of magnifying both the good and the bad in our society. [W]hat we need to do is find new answers to old crimes."

Vice
 President Al Gore
 August
 5, 1999

For these reasons, the President and Vice President established an interagency Working Group on Unlawful Conduct on the Internet, chaired by the Attorney General, to provide an initial analysis of legal and policy issues surrounding the use of the Internet to commit unlawful acts. Specifically, the Working Group considered (1) the extent to which existing federal laws are sufficient to address unlawful conduct involving the use of the Internet; (2) the extent to which new tools, capabilities, or legal authorities may be needed for effective investigation and prosecution of such conduct; and (3) the potential for using education and empowerment tools to minimize the risks from such conduct.

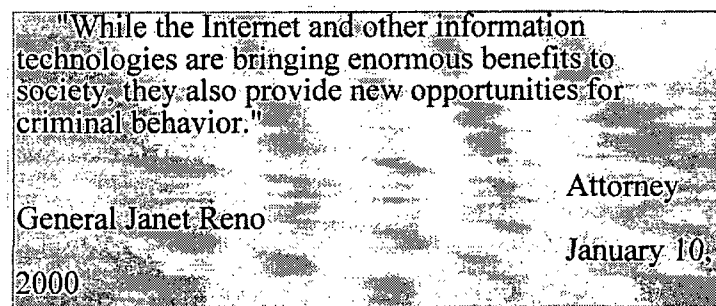
Consistent with the Administration's overall policy, the Working Group recommends a 3-part approach for addressing unlawful conduct on the Internet:

- *First*, any regulation of unlawful conduct involving the use of the Internet should be analyzed through a policy framework that ensures that online conduct is treated in a manner consistent with the way offline conduct is treated, in a technology-neutral manner, and in a manner that takes account of other important societal interests, such as privacy and protection of civil liberties;
- *Second*, law enforcement needs and challenges posed by the Internet should be recognized as significant, particularly in the areas of resources, training, and

the need for new investigative tools and capabilities, coordination with and among federal, state, and local law enforcement agencies, and coordination with and among our international counterparts; and

- *Third*, there should be continued support for private sector leadership and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users to prevent and minimize the risks of unlawful activity.

Prior technological advances – the automobile, the telegraph, and the telephone, for example – have brought dramatic improvements for society, but have also created new opportunities for wrongdoing. The same is true of the Internet, which provides unparalleled opportunities for socially beneficial endeavors – such as education, research, commerce, entertainment, and discourse on public affairs – in ways that we may not now even be able to imagine. By the same token, however, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, and the unlawful distribution of computer software or other creative material protected by intellectual property rights.



In its analysis of existing federal laws in these and other areas, the Working Group finds that existing substantive federal laws generally do not distinguish between unlawful conduct committed through the use of the Internet and the same conduct committed through the use of other, more traditional means of communication. For example, laws governing fraud – such as credit card fraud, identity theft, securities fraud, gambling, and unfair and deceptive trade acts or practices – apply with equal force to both online as well as offline conduct. To the extent these existing laws adequately address unlawful conduct in the offline world, they should, for the most part, adequately cover unlawful conduct on the Internet. There may be a few instances, however, where relevant federal laws need to be amended to better reflect the realities of new technologies, such as the Internet.

Despite the general adequacy of laws that define the substance of criminal and other offenses, the Working Group finds that the Internet presents new and significant investigatory challenges for law enforcement at all levels. These challenges include: the need for real-time tracing of Internet communications across traditional jurisdictional boundaries, both domestically and internationally; the need to track down sophisticated users who commit unlawful acts on the Internet while hiding their identities; the need for hand-in-glove coordination among various law enforcement agencies; and the need for trained and well-equipped personnel – at federal, state, local, and global levels – to gather evidence, investigate, and prosecute these cases. In some instances, federal procedural and evidentiary laws may need to be amended to better enable law enforcement to meet these challenges.

These needs and challenges are neither trivial nor theoretical. Law enforcement

agencies today, for example, are faced with the need to evaluate and to determine the source, typically on very short notice, of anonymous e-mails that contain bomb threats against a given building or threats to cause serious bodily injury. Other scenarios raise similarly significant concerns: If a hacker uses the Internet to weave communications through computers in six different countries to break into an online business' records of customer credit card information, consumer confidence in the security of e-commerce and the Internet may be damaged if law enforcement agencies are unable to cooperate and coordinate rapidly with their counterparts in the other countries to find the perpetrator.

Finally, an essential component of the Working Group's strategy is continued support for private sector leadership and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users so as to minimize the risks of unlawful activity. This Administration has already initiated numerous efforts to educate consumers, parents, teachers, and children about ways to ensure safe and enjoyable Internet experiences, and those efforts should continue. The private sector has also undertaken substantial self-regulatory efforts – such as voluntary codes of conduct and appropriate cooperation with law enforcement – that show responsible leadership in preventing and minimizing the risks of unlawful conduct on the Internet. Those efforts must also continue to grow. Working together, we can ensure that the Internet and its benefits will continue to grow and flourish in the years and decades to come.

**THE ELECTRONIC FRONTIER: THE CHALLENGE OF
UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET**
**A Report of the President's Working Group
on Unlawful Conduct on the Internet**
March 2000

On April 7, 1999, visitors to an online financial news message board operated by Yahoo!, Inc. got a scoop on PairGain, a telecommunications company based in Tustin, California. An e-mail posted on the message board under the subject line "Buyout News" said that PairGain was being taken over by an Israeli company. The e-mail also provided a link to what appeared to be a website of Bloomberg News Service, containing a detailed story on the takeover. As news of the takeover spread, the company's publicly traded stock shot up more than 30 percent, and the trading volume grew to nearly seven times its norm. There was only one problem: the story was false, and the website on which it appeared was not Bloomberg's site, but a counterfeit site. When news of the hoax spread, the price of the stock dropped sharply, causing significant financial losses to many investors who purchased the stock at artificially inflated prices.

Within a week after this hoax appeared, the Federal Bureau of Investigation arrested a Raleigh, North Carolina man for what was believed to be the first stock manipulation scheme perpetrated by a fraudulent Internet site. The perpetrator was traced through an Internet Protocol address that he used, and he was charged with securities fraud for disseminating false information about a publicly traded stock. The Securities and Exchange Commission also brought a parallel civil enforcement action against him. In August, he was sentenced to five years of probation, five months of home detention, and over \$93,000 in restitution to the victims of his fraud.

I. INTRODUCTION

The use of new technology to commit traditional crimes, such as securities fraud, is not new. Advances in technology – the advent of the automobile and the telephone, for instance – have always given wrongdoers new means for engaging in unlawful conduct. The Internet is no different: it is simply a new medium through which traditional crimes can now be committed, albeit through the use of inexpensive and widely available computer and telecommunications systems, and with unprecedented speed and on a far-reaching scale. At

the same time, as exemplified by the PairGain case, the tools and capabilities associated with new technologies can in many instances help law enforcement agencies solve such crimes.

How should society, and government in particular, respond to the advent of these new ways of committing traditional crimes? This report responds to a recent Executive Order from the President and sketches the preliminary contours of a legal and policy answer to that question. It provides a foundation and offers a framework for further dialogue among law enforcement officials and policymakers at all levels; members of the business community, trade associations, and the non-profit sector; and members of the public on one of the most important issues we face in response to this powerful new communications medium and our new digital economy.

A. Executive Order 13,133

In August 1999, President Clinton established an interagency Working Group on Unlawful Conduct on the Internet ("Working Group"). Executive Order 13,133 directed the Working Group, under the leadership of the Attorney General, to address the issue of unlawful conduct involving the use of the Internet and to prepare a report with recommendations on:

- The extent to which existing federal laws provide a sufficient basis for effective investigation and prosecution of unlawful conduct that involves the use of the Internet, such as the illegal sale of guns, explosives, controlled substances, and prescription drugs, as well as fraud and child pornography;
- The extent to which new technology tools, capabilities, or legal authorities may be required for effective investigation and prosecution of unlawful conduct that involves the use of the Internet; and
- The potential for new or existing tools and capabilities to educate and empower parents, teachers, and others to prevent or to minimize the risks from unlawful conduct that involves the use of the Internet.

The Executive Order further directed the Working Group to conduct its review in the context of current Administration policy concerning the Internet. That policy includes support for industry self-regulation where possible, support for technology-neutral laws and regulations, and an appreciation of the Internet as an important medium for commerce and free speech both domestically and internationally.¹ The full text of the Executive Order appears in Appendix A to this report.

This report responds to the directive of Executive Order 13,133 and sets forth a strategy for responding to unlawful conduct on the Internet and for ensuring a safe and secure online environment. As discussed in greater detail below, the Working Group's proposed strategy consists of a 3-part approach that includes: (a) a framework of policy principles for evaluating the need for Internet-specific laws to prohibit unlawful conduct; (b) recognition of the new and significant investigatory needs and challenges posed by the Internet; and (c) support for private sector leadership and the development of appropriate technological tools and outreach efforts to educate and empower Internet users to prevent and minimize the risks of unlawful acts facilitated by the Internet.

Part II of this report focuses on the first component of the strategy, describing the nature of unlawful activity on the Internet and proposing a framework for analyzing policy and legal responses to such activity. Part II also discusses efforts to promote private-sector leadership in this area and summarizes the Working Group's analysis of the adequacy of existing substantive federal laws, as applied to unlawful conduct on the Internet. Part III of the report then identifies several areas in which new technology tools, capabilities, or legal authorities may be required for effective evidence-gathering, investigation, and prosecution

of unlawful conduct that involves the use of the Internet. Part IV of the report focuses on the third component of the strategy, urging support for expanded educational efforts and technological tools to empower Internet users. Finally, Part V summarizes the report's conclusions and recommendations for further action.

B. The Working Group on Unlawful Conduct on the Internet

Pursuant to Executive Order 13,133, the Working Group included the Attorney General, who served as chair of the Working Group; the Director of the Office of Management and Budget; the Secretary of the Treasury; the Secretary of Commerce; the Secretary of Education; the Director of the Federal Bureau of Investigation; the Director of the Bureau of Alcohol, Tobacco and Firearms; the Administrator of the Drug Enforcement Administration; the Chair of the Federal Trade Commission; and the Commissioner of the Food and Drug Administration. In addition, given their interest and expertise in the subject matter, representatives from the Consumer Product Safety Commission, the U.S. Customs Service, the Department of Defense, the Department of State, the National Aeronautics and Space Administration, the National Commission on Libraries and Information Science, the Postal Inspection Service, the U.S. Secret Service, and the Securities and Exchange Commission also participated on the Working Group.

In preparing this report, the Working Group benefitted from the views of representatives of a variety of entities outside the federal government, including, for example:

- State and local groups, such as the National Association of Attorneys General; the National District Attorneys Association; the National Association of Boards of Pharmacies; and the National League of Cities;
- Industry groups, such as the Internet Alliance, the Computer Systems Policy Project, the Business Software Alliance, and representatives of Internet service providers and other high-technology companies; and
- Non-profit advocacy and civil liberties groups, such as the National Center for Missing and Exploited Children, the Center for Democracy and Technology, and the Electronic Privacy Information Center.

We look forward to continuing our dialogue with these and other groups on the important and substantial issues raised in this report.

C. Summary of Strategy

The Internet already is and will continue to be a major force for communication and economic growth in the decades ahead. Consistent with its 1997 Framework for Global Economic Commerce, the Administration is continuing to work toward providing a market-oriented policy environment to support the development of this new digital economy. In developing such an environment, it is essential to address some of the possible negative side effects associated with this new economy. These goals are not inconsistent; rather, they are mutually reinforcing: continued growth in economic commerce will require a stable, predictable legal environment that includes vigorous enforcement of consumer protections; and focused law enforcement efforts in turn will promote greater consumer confidence and trust in the Internet as a safe and secure medium of communications and commerce.

To further these goals, the Working Group recommends a 3-part approach for addressing unlawful conduct on the Internet:

- First, evaluating the need for Internet-specific regulation of unlawful conduct through a framework of general policy principles, including the principle that

online and offline conduct should be treated consistently and in a technology-neutral way;

- Second, recognizing the significant law enforcement needs and challenges posed by the Internet, particularly in the areas of resources, training, and the need for new investigatory tools and capabilities, coordination with and among federal, state, and local law enforcement agencies, and coordination with and among our international counterparts; and
- Third, supporting continued private sector leadership and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users so as to prevent and minimize the risks of unlawful activity.

Each of these components is an integral part of our overall proposed strategy and is discussed in greater detail in the report that follows.

II. POLICY FRAMEWORK AND LEGAL ANALYSIS

There can be little doubt that the Internet – a global electronic network of computer networks (including the World Wide Web) that connects people and information² – has revolutionized and will continue to revolutionize how we communicate, educate ourselves, and buy and sell goods and services. The Internet has grown from 65 million users in 1998 to over 100 million users in the U.S. in 1999, or half the country's adult population; the number of Internet users in the U.S. is projected to reach 177 million by the end of 2003; and the number of Internet users worldwide is estimated to reach 502 million by 2003.³ Business-to-business electronic commerce totaled over \$100 billion in 1999 (more than doubling from 1998) and is expected to grow to over \$1 trillion by 2003.⁴

There can also be little doubt that the Internet provides immeasurable opportunities for far-reaching social benefits. Communications over the Internet, for example, permits unparalleled opportunities for education, research, commerce, entertainment, and discourse on public affairs. Electronic mail ("e-mail") has become an entirely new medium for business and personal communications, allowing users a fast and inexpensive way to keep in touch, to send text, pictures, or sound files to individuals or to groups, and to buy and sell goods and services. News and other information can be made available to anyone with a computer and a modem virtually instantaneously, and more information (on an absolute scale) can be made available to more people, due to the open and decentralized nature of the Internet (anyone can put up a website and "publish" information for the world to see). Access to research databases, directories, encyclopedias, and other information sources previously available only to those with the time, money, and energy to obtain physical access to print material has opened up a world of information to the average citizen. And by making transactions of all kinds cheaper, faster, interactive, and hence more efficient, electronic commerce ("e-commerce") is transforming the way businesses operate and the way consumers work, shop, and play.

The Internet, like most new technologies, is an inherently value-neutral tool: It can be used in ways that are socially beneficial or socially harmful. New technologies can, of course, create new forms of socially undesirable behavior. More often, they provide new ways of committing traditionally undesirable behavior. For example, the advent of the telephone allowed innovative lawbreakers not only to develop new crimes (e.g., long-distance toll fraud), but also to commit traditional crimes in a new manner (e.g., harassment through the use of the telephone).

The Internet has fared no better than other technologies against resourceful and technologically sophisticated individuals who seek to commit unlawful acts. Last year, for example, tens of thousands of computer users were struck by "Melissa" and

"Explore.Zip.Worm," e-mail viruses that quickly spread around the world, erasing files, crashing systems, and costing companies millions of dollars in support and downtime. More recently, some of the most popular consumer and commercial websites were temporarily disabled as a result of "distributed denial-of-service" attacks. Other websites have been the targets of "page-jacking" schemes, in which websites and search engines are manipulated to drive unsuspecting users to unwanted (usually "adult") websites (see Appendix B for further discussion of page-jacking).

More generally, individuals who wish to use a computer as a tool to facilitate criminal activity may find the Internet as appealing, if not more so, as they did the telephone decades ago or the telegraph before that. Similar to the technologies that have preceded it, the Internet provides a new tool for wrongdoers to commit crimes, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, or the unlawful distribution of computer software or other creative material protected by intellectual property rights. In the most extreme circumstances, cyberstalking and other criminal conduct involving the Internet can lead to physical violence, abductions, and molestation. Although the precise extent of unlawful conduct involving the use of computers is unclear,⁵ the rapid growth of the Internet and e-commerce has made such unlawful conduct a critical priority for legislators, policymakers, industry, and law enforcement agencies.

A. Understanding the Nature of Unlawful Conduct Involving Computers

Although definitions of computer crime may differ, not every crime committed with a computer is a computer crime. For example, if someone steals a telephone access code and makes a long distance call, the code they have stolen is checked by a computer before the call is processed. Even so, such a case is more appropriately treated as "toll fraud," not computer crime. Although this example may seem straightforward, many cases cannot be so neatly categorized. For example, a bank teller who steals a \$10 bill from a cash drawer is embezzling. A bank teller who writes a computer program to steal pennies from many accounts (at random) and to funnel that money into another bank through the electronic funds transfer system may also be embezzling, but both committing and prosecuting this offense may require a working knowledge of the bank's computer system. Thus, such a crime may reasonably be characterized as a computer offense.

Broadly speaking, computers can play three distinct roles in a criminal case. First, a computer can be the target of an offense. This occurs when conduct is designed to take information without authorization from, or cause damage to, a computer or computer network. The "Melissa" and "Explore.Zip.Worm" viruses, along with "hacks" into the White House and other websites, are examples of this type of offense. Second, a computer can be incidental to an offense, but still significant for law enforcement purposes. For example, drug traffickers may store transactional data (such as names, dates, and amounts) on computers, rather than in paper form. Third, computers can be a tool for committing an offense, such as fraud or the unlawful sale of prescription drugs over the Internet. Each of these three roles can be and often are present in a single criminal case. Although this report focuses primarily on this third category of computer crime, it is important to understand the range of unlawful conduct that involves computers to appreciate the context of law enforcement needs and challenges relating to such conduct.

1. Computers as Targets

One obvious way in which a computer can be involved in unlawful conduct is when the confidentiality, integrity, or availability of a computer's information or services is attacked. This form of crime targets a computer system, generally to acquire information stored on that computer system, to control the target system without authorization or payment (theft of service), or to alter the integrity of data or interfere with the availability of the computer or server. Many of these violations involve gaining unauthorized access to the target system

(i.e., "hacking" into it).

Offenses involving theft of information may take a variety of forms, depending on the nature of the system attacked. Sensitive information stored on law enforcement and military computers offers a tempting target to many parties, including subjects of criminal investigations, terrorist organizations, and foreign intelligence operatives.

Hackers also target non-governmental systems to obtain proprietary or other valuable information. For example, a hacker might gain access to a hotel reservation system to steal credit card numbers. Other cases may fall into the broad category of intellectual property theft. This includes not only the theft of trade secrets, but also much more common offenses involving the unauthorized duplication of copyrighted materials, especially software programs. Other cases may involve a perpetrator who seeks private information about another individual, whether as a means to an end (e.g., to extort money or to embarrass the victim through public disclosure), to obtain a commercial advantage,⁶ or simply to satisfy personal curiosity. Targets in this category include systems containing medical records, telephone customer records (such as call records or unlisted directory information), or consumer credit report information.

Computers can also be the target of an offense in cases where an offender gains unauthorized access to a system. For instance, an offender may use his computer to break into a telephone switching system (including a private system, such as a PBX) to steal long-distance calling services. (This type of telephone equipment manipulation is often referred to as "phone phreaking" or simply "phreaking.") In some cases, hackers have used the resources of compromised systems to perform intensive computational tasks such as cracking encrypted passwords stolen from other sites. The theft-of-service offenses are often associated with the practice of "weaving," in which a hacker traverses multiple systems (and possibly multiple telecommunications networks, such as the Internet or cellular and landline telephone networks) to conceal his true identity and location. In this scenario, the sole reason for breaking into a given computer may be to use it as a stepping-stone for attacks on other systems.

A more insidious type of damage takes place in cases where the attacker compromises a system in furtherance of a larger scheme. The most well-known examples of this type of attack have involved telephone network computers. In one case, a hacker manipulated telephone switching equipment to guarantee that he would be the winning caller in several call-in contests held by local radio stations. The fruits of his scheme included two sports cars and \$30,000 in cash. Internet-connected computers are subject to similar types of attacks. Routers – which are computers that direct data packets traveling on the Internet – are analogous to telephone switches and thus are tempting targets for skilled hackers who are interested in disrupting, or even rerouting, communications traffic on the network.

In the category of attacks known collectively as "denial of service," the objective is to disable the target system without necessarily gaining access to it. One technically straightforward method of accomplishing this objective is "mailbombing," the practice of sending large volumes of e-mail to a single site (or user account) to clog the mail server or even to cause the target host to crash. Other methods – ranging from simply tying up incoming phone lines to more sophisticated attacks using low-level data transmission protocols – may also be used to achieve the same end: rendering the target system unavailable for normal use. These sorts of denial-of-service attacks recently received much publicity when several major websites, including Yahoo.com, Amazon.com, eBay.com, and Buy.com, were temporarily disabled as a result of such attacks.

2. Computers as Storage Devices

A second way in which computers can be used to further unlawful activity involves the use of a computer or a computer device as a passive storage medium. As noted above, drug

dealers might use computers to store information regarding their sales and customers. Another example is a hacker who uses a computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software). As discussed in Part III below, computers often can provide valuable evidence that may help law enforcement respond to unlawful conduct.

Indeed, computers have made it possible for law enforcement agencies to gather some information that may not have been previously even maintained in the physical world. For example, an unsophisticated offender, even after "deleting" computer files (as opposed to destroying paper records), might leave evidence of unlawful activity that a trained computer forensic expert could recover. In addition, because an average computer with several gigabytes of memory can contain millions of pages of information, a law enforcement agent might, pursuant to lawful authority (such as a warrant), find volumes of information in one place. Of course, that information is only useful if there are trained computer experts on hand in a timely fashion, familiar with the relevant computer hardware or software configuration, to search the computer for specific information and to retrieve it in readable form (see generally Part III.B below).

3. Computers as Communications Tools

Another way that a computer can be used in a cybercrime is as a communications tool. Many of the crimes falling within this category are simply traditional crimes that are committed online. Indeed, many of the examples in this report deal with unlawful conduct that exists in the physical, "offline" world – the illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling; and child pornography. These examples are, of course, only illustrative; online facilities may be used in the furtherance of a broad range of traditional unlawful activity. E-mail and chat sessions, for example, can be used to plan or coordinate almost any type of unlawful act, or even to communicate threats or extortion demands to victims (see cyberstalking box).

Just as legitimate use of the Internet is growing, so too is the Internet increasingly being used to facilitate traditional offenses. For example, because e-mail allows private communications between parties, individuals have used the Internet to send threatening e-mails (including threats to the President). The Internet's one-to-many broadcast capability has also allowed individuals to falsely advertise goods on the Internet or on a website.

The Internet's file transfer capability also enables the Internet to be used as a product delivery system. Because large files can be copied and transmitted reliably, quickly, and cheaply, software companies are now selling software over the Internet: the buyer simply provides a credit card number and downloads the software from the Internet to his or her personal computer. This same capability unfortunately allows for the unauthorized reproduction and distribution of copyrighted software.

Some criminal activities employ both the product delivery and communications features of the Internet. For example, pedophiles may use the Internet's file transfer utilities to distribute and receive child pornography, and use its communications features to make contact with children. Because users need not transmit their voice or appearance, it is easy for an adult to pose as a child and to gain the confidence of children online.

As noted above, this report's primary focus is on this third way in which computers can be used to commit unlawful acts – the use of computers and modern telecommunications facilities as tools (analogous to the use of telephones as tools) to commit an offense. Many of the enforcement and investigative challenges associated with unlawful conduct on the Internet, however, extend to all three ways in which computers can be used for unlawful activity. Consequently, the recommendations contained in this report, if acted upon, could assist law enforcement agencies in combating all types of unlawful conduct involving the use of the Internet.

B. A Framework for Evaluating Unlawful Conduct on the Internet

In its assessment of the extent to which existing federal laws are sufficient to address unlawful conduct involving the use of the Internet, the Working Group developed four general principles to guide its analysis. These principles form the basis for the analytical framework proposed by the Working Group for evaluating the need, if any, for Internet-specific regulation of the particular conduct at issue. The principles flow from the Administration's overall pursuit of policies that recognize and support the enormous potential economic and social benefits of the medium, without unintentionally stifling its growth.

1. Online-Offline Consistency

First, substantive regulation of unlawful conduct (e.g., legislation providing for civil or criminal penalties for given conduct) should, as a rule, apply in the same way to conduct in the cyberworld as it does to conduct in the physical world. If an activity is prohibited in the physical world but not on the Internet, then the Internet becomes a safe haven for that unlawful activity. Similarly, conduct that is not prohibited in the physical world should not be subject to prohibition merely because it is carried out in cyberspace.

Thus, the first step in any analysis of unlawful conduct involving the use of the Internet is to examine how the law treats the same conduct in the offline world. That is, unlawful conduct involving the use of the Internet should not be treated as a special form of conduct outside the scope of existing laws. For example, fraud that is perpetrated through the use of the Internet should not be treated any differently, as a matter of substantive criminal law, from fraud that is perpetrated through the use of the telephone or the mail. To the extent existing laws treat online and offline conduct inconsistently, they should be amended to remove inconsistencies.⁷ As the discussion below and the detailed analyses of several examples in the appendices to this report illustrate, however, existing substantive law is generally sufficient to cover unlawful conduct involving the use of the Internet.

2. Appropriate Investigatory Tools

Second, to enforce substantive laws that apply to online conduct, law enforcement authorities need appropriate tools for detecting and investigating unlawful conduct involving the Internet. For example, as discussed in greater detail below, to the extent existing investigative authority is tied to a particular technology, it may need to be modified or clarified so that it also applies to the Internet.

Indeed, new technologies may justify new forms of investigative authority. Before the invention of the telephone, for example, law enforcement had no need for wiretaps, but once it was clear that the telephone was being used to facilitate illegal activity, that new authority – circumscribed with protections for civil liberties and other societal interests – became necessary and appropriate. Similarly, features of the Internet that make it different from prior technologies may justify the need for changes in laws and procedures that govern the detection and investigation of computer crimes. These features, highlighted here in summary form, are discussed in greater detail below:

- The global and boundaryless nature of the Internet means that different law enforcement agencies in different jurisdictions will have to cooperate and coordinate their activities in ways that they have probably never before done.
- Anonymity on the Internet can provide social benefits, but misrepresentation of identity can also facilitate fraud and deception. Misrepresentation of identity can also result in access by children to inappropriate material and can create law enforcement investigatory challenges, especially if perpetrated by sophisticated computer users, for it can make

criminal activity on the Internet more difficult to detect and prove.

- The potential to reach vast audiences easily means that the scale of unlawful conduct involving the use of the Internet is often much wider than the same conduct in the offline world. To borrow a military analogy, use of the Internet can be a "force multiplier."
- The routine storage of information that can be linked to an individual can often provide more information to law enforcement (where an individual has been identified or a computer lawfully seized) than may be available in the offline world, but only if the electronic information is handled properly by a trained investigator and if the information obtained is ultimately available in useable form.

Thus, apart from ensuring that online and offline behavior is treated consistently as a matter of substantive law, legislators and policymakers should examine whether law enforcement agencies have appropriate tools to detect and investigate unlawful conduct involving the Internet. That is, even if Internet-specific laws are unnecessary to ensure that criminal and civil penalties apply to the use of the Internet to facilitate unlawful conduct, it may be necessary to alter or augment law enforcement's tools and authorities to meet the new investigatory challenges that such unlawful conduct presents.

3. Technology-Neutrality

Third, to the extent specific regulation of online activity may be necessary (in view of the consistency principle noted above), any such regulation should be drafted in a technology-neutral way. Regulation tied to a particular technology may quickly become obsolete and require further amendment. In particular, laws written before the widespread use of the Internet may be based on assumptions regarding then-current technologies and thus may need to be clarified or updated to reflect new technological capabilities or realities. For example, regulation of "wire communications" may not account for the fact that communications may now occur through wireless means or by satellite. Technology-specific laws and regulations may also "lock-in" a particular technology, hindering the development of superior technology.

4. Consideration of Other Societal Interests

Fourth, any government regulation of conduct involving the use of the Internet requires a careful consideration of different societal interests. In addition to society's strong interests in investigating and prosecuting unlawful conduct, society also has strong interests in promoting free speech, protecting children, protecting reasonable expectations of privacy, providing broad access to public information, and supporting legitimate commerce.

As applied to the Internet, consideration of other societal interests can present difficult issues, in part because the Internet is different in important ways from existing, "traditional" modes of communication. For example, the Internet is a multi-faceted communications medium that allows not only point-to-point transmission between two parties (like the telephone), but also the widespread dissemination of information to a vast audience (like a newspaper). Internet-specific laws and policies that operate by analogy to those designed for telephone communications or the press may not fit the new medium. The Internet also presents new issues relating to online expectations of privacy and confidentiality that may or may not have analogs in the offline world. Accordingly, rules and regulations designed to protect the safety and security of Internet users should be carefully tailored to accomplish their objectives without unintended consequences, such as stifling the growth of the Internet or chilling its use as a free and open communication medium.

Another aspect of the need to consider different societal interests is to appreciate the need for an appropriate balance among the roles of the government (whether federal, state, local, or other) and the role of the private sector in formulating solutions to Internet policy issues.

For example, because regulation of the practices of medicine and pharmacy has traditionally been the province of the states, regulation of online pharmacies presents difficult federal-state jurisdictional and coordination issues (see Appendix D). And, as discussed in the next section, given the Administration's support for private-sector leadership and market-based self-regulation regarding e-commerce, there must be ongoing and regular dialogue with interested parties and groups to ensure that government policies do not have unintended consequences.

C. Promoting Private Sector Leadership

Consistent with the Administration's overall e-commerce policy, the private sector has a critical role to play in ensuring a safe and secure online environment. The distributed, networked, and decentralized nature of the Internet now means that the "rules of the road" must be global, flexible, effective, and readily adaptable to technological change. In particular, the private sector must take the lead in areas such as the design of new technologies to protect children online, self-regulatory consumer protection initiatives, and coordination and cooperation with law enforcement authorities.

In response to the marketplace, for example, there are now many technological options for shielding children from inappropriate content. As discussed in more detail in Part IV.A below, these technological developments include filtering and blocking software, outgoing information blocks, filtered Internet browsers and search engines, filtered Internet service providers, time blocking mechanisms and monitoring tools. Similarly, child-friendly websites are now widespread on the Internet. These websites allow parents to limit a child's access to sites beyond the web service designated for the child's use. In July 1999, the private sector launched the "GetNet Wise" initiative, a new easy-to-access online resource for parents to help keep their children safe online. "GetNet Wise" is a resource containing information on Internet safety tips, consumer content filtering products, law enforcement contacts, and a guide to quality educational and age appropriate online content. Although none of these tools can guarantee that a child will be shielded at all times from inappropriate material on the Internet, their use gives parents the ability to restrict a child's use to the resources on the Internet that they may deem appropriate.

In addition, in response to challenges issued by Commerce Secretary Daley, industry has worked with consumer representatives to develop consumer protection practices, codes of conduct for business-to-consumer e-commerce, and alternative, easy-to-use mechanisms for consumer resolution, redress, and enforcement.

- For example, the Better Business Bureau's online division, BBBOnline, is working with industry, consumer, and government representatives to develop a voluntary code to provide online merchants with guidelines to implement consumer protections. The code includes guidance on key consumer protections such as disclosure of sale terms, data privacy, dispute resolution mechanisms, and non-deceptive advertising.
- Another group, the Electronic Commerce and Consumer Protection Group, whose members include America Online, American Express, AT&T, Dell, IBM, Microsoft, Time Warner, Inc., and Visa, is working with consumer leaders to develop an innovative approach to jurisdiction as it applies to consumer protection in a global electronic marketplace. This group is also developing a voluntary code of conduct. The goal of the group is to formulate concrete approaches to protect consumers and facilitate e-commerce.

These creative efforts are important to developing effective consumer protection in e-commerce, because as e-commerce expands to encompass more international business-to-consumer transactions, the traditional means of protecting consumers solely through national laws will become more difficult.

In addition to specific consumer protection initiatives, the private sector's dedication and support for a secure Internet system is crucial to curbing unlawful conduct on the Internet. Not only must industry continue to develop security policies and safeguards for their networks and systems, but it should also continue its efforts to identify security flaws that threaten the Internet. For example, computer experts from industry and the Computer Emergency Response Team Coordination Center of Carnegie-Mellon University recently warned of a new Internet security threat that wrongdoers could potentially use to place malicious programs on a victim's computer and to gather information that a person volunteers on websites, such as credit card and Social Security numbers.⁸ The Partnership for Critical Infrastructure Protection will provide a cross-sectoral forum for the private sector to address a variety of infrastructure assurance issues, including information sharing, development of best practices, promotion of needed R&D, and workforce development. Another example of private sector cooperation in this effort is InfraGard, which is an information sharing and analysis partnership among the FBI, private sector companies, academic institutions, and other federal, state, and local agencies. InfraGard serves to increase the security of the national infrastructure through ongoing exchanges of infrastructure-protection information and through education, outreach, and other awareness efforts.

The private sector also has a key role to play in continuing to coordinate and cooperate with law enforcement authorities as appropriate. Industry trade groups, such as the Internet Alliance and the Information Technology Association of America ("ITAA"), have been working to develop public-private cooperative efforts that will mutually benefit law enforcement, industry, and consumers. The Internet Alliance's Law Enforcement and Security Council has been developing parental control software and educational campaigns, opening channels of communication between industry and law enforcement representatives, and creating training programs for law enforcement and industry on issues of mutual interest. ITAA, through its Cybercitizen Project (see Part IV.C below), is working with the Department of Justice to develop education campaigns, personnel exchange programs, and a directory of industry contacts.

Although the private sector has taken important steps in the areas of prevention and online security, there is still much that industry can do to ensure that the Internet is a safe and secure environment. For example:

- Industry should continue to develop and embrace initiatives to protect consumers and children online. These may include technological tools (e.g., more sophisticated blocking, filtering, and parental control software) as well as non-technological tools (e.g., educational campaigns). In particular, industry should continue to be involved in education programs that teach younger Internet users about online responsibilities and online citizenship.
- Industry should continue to cooperate with law enforcement agencies as appropriate. This does not mean that industry ought to be a "co-regulator" with government or that industry needs to be an online police officer. But it does mean that industry should be a voluntary, responsible partner in society's fight against crime, educating its employees on how to recognize unlawful conduct on the Internet and what to do if they discover such conduct. It means working with law enforcement agencies to develop reliable and efficient procedures and channels of communication and cooperation for processing law enforcement requests and investigative information. As the "Melissa" virus case demonstrates, industry's involvement and reporting of information is often crucial to the investigation and prosecution of online offenders.
- Industry should carefully balance reasonable expectations of customer privacy with the need to ensure a safe and secure online environment. For example,

some industry members may not retain certain system data long enough to permit law enforcement to identify online offenders. This does not mean that data retention policies need to be uniform or mandatory. To the contrary, in evaluating the costs and benefits of data retention – which include a wide variety of considerations, including market needs, protection of consumer privacy, and public safety – industry should simply give appropriate weight to the wider value to itself and to society of retaining certain information that, among other things, may be essential to apprehending a lawbreaker.

- Industry should be encouraged to recognize that meaningful self-regulation is in its interest as well as in the interests of its customers. Information technology security programs (that teach employees about computer ethics, responsible online practices, and security policies), for instance, help protect computer systems from intruders as well as online offenders. Indeed, as we noted at the outset of this report (see Part I.C above), law enforcement and industry share a common mission in reducing unlawful online conduct, for a safe and secure online environment is essential to consumer confidence, which is in turn essential to ensuring that the Internet continues to grow as a medium for communications and commerce.

The Working Group looks forward to continuing to work with the private sector and other interested parties and groups in partnership on these important issues.

D. Sufficiency of Existing Federal Laws

Private sector leadership is, of course, necessary but not sufficient to address unlawful conduct involving the use of the Internet. Substantive criminal laws represent a societal determination, expressed through our democratic institutions of government, that certain conduct is so harmful or morally unacceptable that reliance on self-regulation or the market to regulate the conduct is inappropriate. There is thus a need to evaluate whether existing substantive laws apply to unlawful conduct that is committed through the use of the Internet.

Toward that end, and in the context of the framework of policy principles discussed above, the Working Group analyzed several examples of unlawful conduct involving the use of the Internet. The examples, as discussed in detail in appendices to this report, include not only those specifically mentioned in Executive Order 13,133, but also those taken from our experience with legislative proposals and from Executive branch agencies that have jurisdiction to respond to these forms of unlawful conduct.

1. Analysis of Substantive Laws

The Working Group's analysis reveals that existing substantive federal laws appear to be generally adequate to protect users from unlawful conduct on the Internet. As listed and summarized in Table 1 below, such laws generally do not distinguish between unlawful conduct committed through the use of the Internet and the same conduct committed through the use of other, more traditional means of communication.

For example, laws governing fraud – such as credit card fraud, identity theft, securities fraud, and unfair and deceptive trade acts or practices – apply with equal force to both online as well as offline conduct (see Appendix B). Laws prohibiting the distribution and possession of child pornography and the luring of minors across state lines for unlawful sexual activity have been used with success to prosecute and convict those who use the Internet to distribute such material or to communicate with child victims in violation of statutory prohibitions (see Appendix C). And laws that prohibit the dispensing of prescription drugs without a valid prescription from a licensed medical professional can be applied to online pharmacies that dispense prescription drugs without required regulatory

safeguards (see Appendix D).

Laws in other areas – the sale of firearms (Appendix E); interstate transmission of gambling information (Appendix F); sale of alcohol (Appendix G); securities fraud (Appendix H); and theft of intellectual property (Appendix I) – also generally apply to online conduct as well as offline conduct. Although existing federal laws generally prohibit Internet gambling, technological advances make it prudent to update existing federal laws to ensure that they are technology-neutral and prohibit gambling activities that did not exist before the advent of the Internet (see Appendix F). And, in the area of intellectual property protection, current Sentencing Guidelines pertaining to intellectual property crimes should be updated to ensure that law enforcement agencies and prosecutors commit the resources to continue to pursue these cases vigorously (see Appendix I).

Table 1 – Summary of Analysis of Existing Federal Law

Types of Unlawful Conduct	Examples of Potentially Applicable Federal Laws	Detailed Discussion in Appendix
Internet Fraud	15 U.S.C. §§ 45, 52 (unfair or deceptive acts or practices; false advertisements) 15 U.S.C. § 1644 (credit card fraud) 18 U.S.C. §§ 1028, 1029, 1030 (fraud in connection with identification documents and information; fraud in connection with access devices; and fraud in connection with computers) 18 U.S.C. § 1341 et seq. (mail, wire, and bank fraud) 18 U.S.C. § 1345 (injunctions against fraud) 18 U.S.C. § 1956, 1957 (money laundering)	B
Online Child Pornography, Child Luring, and Related Activities	18 U.S.C. § 2251 et seq. (sexual exploitation and other abuse of children) 18 U.S.C. § 2421 et seq. (transportation for illegal sexual activity)	C
Internet Sale of Prescription Drugs and Controlled Substances	15 U.S.C. § 45 et seq. (unfair or deceptive acts or practices; false advertisements) 18 U.S.C. § 545 (smuggling goods into the United States) 18 U.S.C. § 1341 et seq. (mail, wire, and bank fraud; injunctions against fraud) 21 U.S.C. § 301 et seq.	D

	(Federal Food, Drug, and Cosmetic Act) 21 U.S.C. §§ 822, 829, 841, 863, 951-971 (Drug Abuse Prevention and Control)	
Internet Sale of Firearms	18 U.S.C. § 921 et seq. (firearms)	E
Internet Gambling	15 U.S.C. § 3001 et seq. (Interstate Horseracing Act) 18 U.S.C. § 1084 (transmission of wagering information) 18 U.S.C. §§ 1301 et seq. (lotteries) 18 U.S.C. § 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises) 18 U.S.C. § 1953 (interstate transportation of wagering paraphernalia) 18 U.S.C. § 1955 (prohibition of illegal gambling businesses) 28 U.S.C. §§ 3701-3704 (professional and amateur sports protection)	F
Internet Sale of Alcohol	18 U.S.C. § 1261 et seq. (liquor traffic) 27 U.S.C. §§ 122, 204 (shipments into states for possession or sale in violation of state law)	G
Online Securities Fraud	15 U.S.C. § 77e, 77j, 77q, 77x, 78i, 78j, 78l, 78o, 78ff (securities fraud)	H
Software Piracy and Intellectual Property Theft	17 U.S.C. § 506 (criminal copyright infringement) 17 U.S.C. § 1201 et seq. (copyright protection and management systems) 18 U.S.C. § 545 (smuggling goods into the United States) 18 U.S.C. §§ 1341, 1343 (frauds and swindles) 18 U.S.C. § 1831 et seq. (protection of trade secrets) 18 U.S.C. §§ 2318-2320 (trafficking in counterfeit labels for phonorecords, copies of computer programs or computer program documentation or packaging, and copies of motion pictures)	I

or other audio visual works)

2. New Investigatory Challenges

As law enforcement agencies adapt to a more technology-based society, they need to be aware of the challenges, as well as the benefits, of online investigations. In certain circumstances, law enforcement agencies have available to them tools and capabilities created by the Internet and computers that can assist them in their fight against computer-facilitated unlawful conduct. For example, just as advances in telephone technology gave law enforcement agents the ability to determine the origin of fraudulent or threatening calls, the Internet has given law enforcement agencies the ability to find unsophisticated offenders who leave the equivalent of "fingerprints" as they commit unlawful acts. Indeed, someone who makes a threat in an Internet chat room to set off a bomb at a school and who makes little or no effort to hide his or her identity (e.g., where accurate identifying information exists for a particular "screen name") can often be traced and found with relative ease.

At the same time, law enforcement agencies must also acknowledge the growing sophistication of other computer users, who wear the equivalent of Internet gloves that may hide their fingerprints and their identity. The following is an overview of investigatory challenges – taken from actual experiences involving online investigations and discussed in greater detail in the appendices for each example of Internet-facilitated unlawful conduct – that law enforcement agencies must consider as they become more proficient with such investigations.

(a) Jurisdiction

In the physical world, one cannot visit a place without some sense of its geographic location. Whether a particular street address or an area of the world, human travel is spatially based. By contrast, because one can access a computer remotely without knowing where, in physical space, that computer is located, many people have come to think of the collection of worldwide computer linkages as "cyberspace" (a term coined by science fiction writer William Gibson). In short, cybercriminals are no longer hampered by the existence of national or international boundaries, because information and property can be easily transmitted through communications and data networks.

As a result, a criminal no longer needs to be at the actual scene of the crime (or within 1,000 miles, for that matter) to prey on his or her victims. Just as telephones were (and still are) used by traditional boiler-room operators to defraud victims from a distance, a computer server running a webpage designed to defraud senior citizens might be located in Thailand, and victims of the scam could be scattered throughout numerous different countries. A child pornographer may distribute photographs or videos via e-mail running through the communications networks of several countries before reaching the intended recipients. Likewise, evidence of a crime can be stored at a remote location, either for the purpose of concealing the crime from law enforcement and others, or simply because of the design of the network.⁹ To be sure, the Internet increases the ability of law enforcement officials and others to detect and gather evidence from a distance. For example, a website used in a fraud scheme can be spotted from an agent's office, whereas detecting a fraudulent telemarketing or mail-fraud scheme might well require extensive field work. Long-distance detection, however, may take the investigation and prosecution of these crimes out of the exclusive purview of any single jurisdiction, thereby creating yet other challenges and obstacles to crime-solving.

For example, a cyberstalker in Brooklyn, New York may send a threatening e-mail to a person in Manhattan. If the stalker routes his communication through Argentina, France, and Norway before reaching his victim, the New York Police Department may have to get

assistance from the Office of International Affairs at the Department of Justice in Washington, D.C. which, in turn, may have to get assistance from law enforcement in (say) Buenos Aires, Paris, and Oslo just to learn that the suspect is in New York. In this example, the perpetrator needs no passport and passes through no checkpoints as he commits his crime, while law enforcement agencies are burdened with cumbersome mechanisms for international cooperation, mechanisms that often derail or slow investigations. With scores of Internet-connected countries around the world, the coordination challenges facing law enforcement are tremendous. And any delay in an investigation is critical, as a criminal's trail often ends as soon as he or she disconnects from the Internet.

This does not mean that traditional legal structures cannot be meaningfully applied to the Internet. Even though connections may be of short duration, computers are still physically located in particular places. The challenge to law enforcement is identifying that location and deciding which laws apply to what conduct. The question is how sovereign nations can meaningfully enforce national laws and procedures on a global Internet.¹⁰

Inconsistent substantive criminal laws are only part of the problem, for investigative techniques are also controlled by national (or local) law. For example, law enforcement agencies must consider such issues as transborder execution of search warrants. If law enforcement agents in the United States access a computer and seize data from a computer, the fact that they have a search warrant makes that action lawful. If, with that same search warrant, they remotely access a Canadian computer (from the United States), might this constitute a criminal act under Canadian law notwithstanding the existence of the U.S. warrant? To the extent that agents know nothing more than an Internet protocol address (essentially, a series of numbers that identify a particular machine), the physical location of the computer to be searched may not be accurately known. Yet ignorance of physical location may not excuse a transborder search; consider how we would react to a foreign country's "search" of our defense-related computer systems based upon a warrant from that country's courts.

This transborder issue may raise domestic issues as well. Gambling and obscenity laws provide criminal sanctions for individuals based, in part, upon their location. One federal law prohibits transmitting information assisting in the placing of bets or wagers on sporting events or contests unless both the sender and receiver are in states or foreign countries where gambling is legal, see 18 U.S.C. §1084. Obscenity laws are also typically interpreted in light of local community standards, cf. *Miller v. California*, 413 U.S. 15 (1973). Even the search warrant provision in the federal rules requires that agents seek a warrant in the district where the property to be seized is located, see Fed. R. Crim. P. 41(a). To the extent the location of the sender, recipient, or data is unknown and perhaps unknowable, it may be difficult for law enforcement to investigate and prosecute online offenders.

(b) Identification

Another thorny issue stems from the lack of identification mechanisms on global networks, and the fact that individuals can be anonymous or take on masked identities (i.e., adopt false personas by providing inaccurate biographical information and misleading screen names). Simply stated, given the current state of technology, it can be difficult to accurately identify an individual (especially sophisticated users who take affirmative steps to hide their identity) on the Internet. As noted above, there are cases, such as the PairGain case, where law enforcement agencies have been able to track down online criminals who leave evidence of their unlawful conduct. Over time, the ability of criminals to use technology to evade identification and the ability of law enforcement to use technology to overcome such evasion will continue to evolve. Some of the challenges of identifying perpetrators of unlawful conduct on the Internet, as well as measures taken by law enforcement and the private sector¹¹ to respond to such challenges, are discussed below in Part III of this report.

At the very least, there needs to be widespread and extensive training of law enforcement

personnel in ways to identify those who use the Internet to commit unlawful acts. Moreover, as policymakers increasingly seek to protect certain classes of citizens, most notably minors, from unsuitable material (e.g., pornography and gambling), the potential problems of identification are evident. How can activities, such as gambling or the sale of prescription drugs or alcohol, be limited to adults when children can identify themselves as adults? Similarly, if adults can falsely identify themselves as children and lure real children into dangerous situations, how can these victims be protected?

These issues are frequently at the heart of legislative and investigative efforts. Although there have been proposals to build identification mechanisms into Internet protocols, such an approach would have to be supported by internationally-recognized, market-based, standards-making bodies whose agenda did not directly include public safety. Even if the market supported such an approach, however, such proposals are controversial, because there are strong reasons to allow anonymity in communications networks. For example, whistleblowers may wish to remain anonymous, as may a group of rape victims who wish to convene an electronic meeting to discuss their experiences without revealing their identities.

In an attempt to create a framework for evaluating identification mechanisms on the Internet, some have compared the Internet with other forms of communications, such as pay telephones and regular mail, which may offer users some degree of anonymity. Of course, the difference between these traditional means of communication and the Internet is significant, and attempting to solve Internet problems only by drawing analogies to existing technologies will often fail. The problem is that the analogies may capture some aspects of the new technology, but fail to capture others. For example, the telephone and mail systems cited above allow predominantly one-to-one communications. Although someone wishing to defame a public figure or harass others can, in theory, call thousands of people anonymously, the time and cost make this impractical. By contrast, the cost-free, simple, one-to-many nature of the Internet dramatically alters the scope and impact of communications. It is this difference which explains why children who would never spend their weekly allowance buying *The Anarchist Cookbook* at a college bookstore may download the same information from the Internet and possibly injure themselves or others testing a recipe for the making of a bomb.¹² Given the complexity of this issue, balancing the need for accountability with the need for anonymity may be one of the greatest policy challenges in the years ahead.

(c) Evidentiary Issues

Electronic data generated by computers and networked communications such as the Internet can be easily destroyed, deleted, or modified. Digital photographs are but one example of digital information that can be altered in ways that may be difficult to detect. As a result, law enforcement officials must be cognizant of how to gather, preserve, and authenticate electronic evidence. This will not only require substantial training of law enforcement personnel, but also sufficient experience with such evidence by investigators, prosecutors, defense counsel, courts, and others until clear rules and standards are established. The volume of electronic evidence that requires forensic analysis is also increasing substantially. The increasing use of computers and the Internet, of course, often means that information or records of communications that were previously never retained or routinely destroyed can (in some instances) now be recovered, but such recovery may still require sophisticated computer forensics.

Thus, for the reasons noted above, law enforcement agencies face significant challenges in dealing with electronic evidence. These challenges will continue to grow, because electronic evidence can become a part of any investigation. Electronic evidence, for example, can show up as any of the following items, each presenting distinct evidentiary challenges: a drug trafficker's computerized customer records; a digital photograph of a murder scene; an encrypted e-mail containing details of a terrorist plot or fraud scheme; or a system administrator's log files of a hacker attack.

(d) Infrastructure Protection

Protecting our information infrastructure is imperative but difficult for a host of reasons: the number of different systems involved, the interdependency of these systems, the varied nature of the threats (physical and cyber, military, intelligence, criminal, natural), and the fact that many of these infrastructures are maintained primarily by the commercial sector. Addressing cyberthreats to our infrastructure is particularly difficult, because of differing views regarding our vulnerabilities; the need to balance interests relating to privacy, economic competitiveness, commercial risk, national security, and law enforcement; and the overlapping authorities within the federal government for dealing with information infrastructure issues. Although such issues are beyond the scope of this report, see National Plan for Information Systems Protection (released Jan. 7, 2000), appreciating the importance and complexity of infrastructure protection is key to understanding the needs of law enforcement in countering unlawful conduct involving the Internet (see Part III.A below).

(e) Commingling

The ability of an individual to use one computer to conduct both lawful and unlawful activities or to store both contraband and legally possessed material presents another significant issue. Such commingling defies simple solutions. The fact is, one computer can be used simultaneously as a storage device, a communications device (e.g., to send, store, or retrieve e-mail), and a publishing device. Moreover, that same computer can be used simultaneously for both lawful and unlawful ventures, and the problem becomes more complex when a single machine is shared by many users.

For example, individuals who distribute child pornography or copyrighted software using their home computers may also publish a legitimate newsletter on stamp collecting or use an e-mail service with that same computer. By seizing the computer, law enforcement agencies can stop the illegal distribution of contraband, but may, at the same time, interfere with the legitimate publication of the newsletter and the delivery of e-mail, some of which may be between users who have no connection with the illegal activity. Similarly, a doctor who is illegally prescribing drugs over the Internet may not only have on her computer evidence relating to the illegal prescriptions, but files related to her lawfully treated patients. Likewise, an attorney accused of operating an Internet sportsbook may keep in the same folder on his computer materials relating to his gambling business and documents subject to the attorney-client privilege. Seizure of the doctor's or the lawyer's files in such circumstances could result in the seizure of legally privileged material.

III. LAW ENFORCEMENT NEEDS AND CHALLENGES

As the examples of Internet-facilitated unlawful conduct discussed above and in the appendices illustrate, the increasing sophistication and global reach of such conduct make it all the more important to adequately equip law enforcement agencies at all levels.

The following are some of the principal issues that should be considered when evaluating how to better equip federal, state, and local law enforcement agencies to ensure the safety and security of Internet users. We urge further analysis, in consultation with state and local law enforcement, industry, and privacy and other groups, to determine the most appropriate ways to promote private sector leadership in this area and to empower law enforcement – at all levels – with the needed tools, capabilities, and legal authorities to curb unlawful conduct on the Internet while protecting privacy and supporting the growth of the electronic marketplace.

A. Protecting Computers and Networks

In assessing the tools, capabilities, and legal authorities needed by law enforcement to address unlawful conduct on the Internet, we must consider the larger context of how to protect the systems and networks of this Nation that make our businesses run and operate our Nation's defenses and infrastructure. As we have become more dependent on technology, our energy production and distribution channels, our transportation networks, and our telecommunication systems have become increasingly reliant on a computer-based infrastructure.

Without a protected infrastructure, there could be no conduct, lawful or unlawful, on the Internet. Electronic commerce and the marketplace cannot thrive without a strong infrastructure that the public can trust and rely upon. Consequently, proposals relating to law enforcement challenges in this area (e.g., new investigative tools, capabilities, or legal authorities) need to be assessed in light of the broader need to protect the vital infrastructure, because cyberattacks on infrastructures and other cybercrimes can lead to telecommunications breakdowns that disable electronic commerce and destroy our citizens' confidence in the Internet and computer networks.

The protection of this country's computers and networks requires everyone's cooperation. It demands a partnership among all federal agencies with responsibilities for certain special functions, such as law enforcement, intelligence, and defense.¹³ It also requires all federal agencies to take appropriate preventive measures to protect their computer systems against attack. Most important, because the overwhelming majority of the Nation's infrastructure is in private hands, the private sector must take the steps necessary to prevent attacks against its systems.¹⁴ The Partnership for Critical Infrastructure Protection, which recently held a day-long kickoff meeting, will serve as a key catalyst for this activity. In addition, we must consider the needs of state and local law enforcement, which play a critical role in fighting the cybercriminals on the street.

Meeting its responsibility to protect critical infrastructures is one of the central challenges for law enforcement as we face the 21st Century. As our reliance on the Internet, on automated systems, and on other technological advances increases with every passing month, the potential impact of attacks on critical infrastructure expands as well. Law enforcement needs to be provided the legal mechanisms and financial resources to be prepared to confront this challenge in partnership with other federal agencies, with the private sector, and with state and local agencies. The Administration recognized this need for unprecedented cooperation between the private and public sectors in Presidential Decision Directive 63. That document provides a framework for federal agencies to cooperate with their private sector partners and for the formation of the National Infrastructure Protection Center, an interagency center for analysis, warning, and investigation of cybercrime. In addition, the Partnership for Critical Infrastructure Protection provides a cross-sectoral forum for the private sector to address a variety of infrastructure assurance issues.

B. Federal Tools and Capabilities

1. Personnel, Equipment, and Training

In 1986, an astronomer-turned-systems-manager at the University of California at Berkeley found a 75-cent accounting error in a computer's billing program, which led to the discovery that an unauthorized user had penetrated Berkeley's computer system. When the astronomer, Clifford Stoll, began to investigate further, he discovered that a hacker identified as "Hunter" was using Berkeley's computer system as a conduit to break into U.S. government systems and steal sensitive military information. The hacker's objective seemed to be to attain U.S. anti-ballistic missile technology.

As he began to pursue the hacker, Stoll encountered serious problems. To begin with, Stoll was unable to find computer-literate law enforcement personnel with an appreciation of the

technical nature of the criminal activity. Local and federal agencies that Stoll contacted, including the FBI and CIA, initially expressed little interest in pursuing what at first looked like a computer prank. (Moreover, until government investigators learned of the potential threat to national security, they had no interest in pursuing a case which appeared to have damages valued at less than one dollar.) Because Hunter's trail vanished each time he ended a communication, he could only be traced when he was online. But because it was often after business hours (and, indeed, sometimes in the middle of the night) when Hunter attacked, there were few (if any) law enforcement personnel available during those sessions. The call was eventually traced to Germany, but adding an international element to the case now meant that it was usually after business hours in at least one time zone where the communication was passing through. Stoll cleverly resorted to generating phony official-looking data to keep the hacker interested and online long enough for the trace to be completed. Eventually, the source of the attacks was identified as a German hacker, and he was successfully prosecuted there.¹⁵

Ironically, one reason this investigation was successful is that Stoll did not rely solely on law enforcement, but instead was able to work directly with telephone company personnel, who in turn worked with other telecommunications providers. His investigation brought to light a number of interdependent personnel and resource requirements that, unless fulfilled, will impede the success of law enforcement in this area. Despite significant progress since the time of this example, it remains a useful illustration of some of the fundamental issues that continue to need further attention at the domestic and international level to eliminate weak links in the chain of an investigation.

(a) Experts Dedicated to High-tech Crime

The complex technical and legal issues raised by computer-related crime require that each jurisdiction have individuals who are dedicated to high-tech crime and who have a firm understanding of computers and telecommunications. The complexity of these technologies, and their constant and rapid change, mean that investigating and prosecuting offices must designate investigators and prosecutors to work these cases on a full-time basis, immersing themselves in computer-related investigations and prosecutions. Many agencies, including the Departments of Justice, Treasury, and others, have already dedicated available resources to do so. The Federal Trade Commission ("FTC") adopted this approach when it formed an Internet Rapid Response Team and successfully halted several online fraud schemes in a matter of weeks. Some federal agency inspectors general have also established computer crime divisions, complete with forensics laboratories and technical experts, and many have information technology audit and inspection capabilities to assist their agencies in identifying vulnerabilities, best practices, and other critical infrastructure issues.

But more of such expertise and the resources to support the increasing cyber-workload are needed. Indeed, each state attorney general's office, each U.S. Attorney's office, each federal law enforcement squad, and each country's equivalent to the U.S. Department of Justice should have a dedicated high-tech crime unit that knows how to respond to a fast-breaking investigation and that knows who else to contact in the chain of a communication and how to reach those individuals. These experts will also be needed to support other law enforcement authorities faced with high-tech issues, such as when a computer is used to facilitate an otherwise traditional crime.

The Department of Justice has designated a prosecutor in each U.S. Attorney's Office to serve as a computer and telecommunications coordinator for that district, and the FBI has established the National Infrastructure Protection Center and the National Infrastructure Protection and Computer Intrusion program. Staffing levels for these programs are below the level needed to effectively address the concerns raised in this report. Given the magnitude of the challenges, the continually changing technology, and the complexity of these investigations, these are necessarily resource-intensive programs.

(b) Experts Available on a 24-Hour Basis

A unique feature of high-tech and computer-related crime is that it often requires immediate action to locate and identify criminals. The trail of a criminal may be impossible to trace once a communication link is terminated, because the carrier may not keep (or is not required by law to keep) records concerning each individual communication. This lack of information is due, in part, to the fact that there often is no longer a revenue-related reason for recording transmission information (i.e., connection times or source and destination) for individual connections. For example, many businesses no longer bill their customers by individual telephone call or Internet connection but, instead, by bulk billing (e.g., a single rate for one month of usage). When a carrier does not collect traffic data, a suspect's trail may evaporate as soon as the communication terminates.

Therefore, investigators and prosecutors with expertise in this field must be available 24 hours a day so that appropriate steps can be taken in a fast-breaking high-tech case. For example, the National Infrastructure Protection Center operates a 24-hour/7-day-a-week command post for around-the-clock coverage of computer intrusion matters. And, Attorney General Reno recently challenged the National Association of Attorneys General to work with the Department of Justice and other appropriate organizations (among other things) to create a 24/7 network of computer crime enforcement personnel in every state.¹⁶

(c) Regular and Frequent Training

Because of the speed at which communications technologies and computers evolve, and because criminal methods in these areas generally change more rapidly than those in more traditional areas of crime, experts must receive regular and frequent training in the investigation and prosecution of high-tech cases. Programs such as those offered by the FBI at its Quantico facility and elsewhere and under the National Cybercrime Training Partnership provide such training to federal, state, and local law enforcement personnel, but more is needed. Government computer professionals, such as systems operators and administrators, also need regular and frequent training, because they are often the first to detect unlawful conduct that targets federal computer systems.

In addition to domestic training, countries should participate in coordinated training with other countries, so transnational cases can be pursued quickly and seamlessly. By way of example, in the U.S., high-tech prosecutors at the federal level attend a 1-week training course every year, with training provided by both government and private sector personnel. Likewise, in 1998, the G-8 countries held an international high-tech training conference for its countries' law enforcement personnel.

(d) Up-to-date Equipment

In the past, a police officer would be given a gun, a flashlight, and a notepad when he or she was hired. Twenty years later, the three items would be returned to the police department when the officer retired, and the only intervening equipment expenses would have had to do with replacement bullets, batteries, and note paper. Today, keeping pace with computer criminals means that law enforcement experts in this field must be properly equipped with the latest hardware and software. Providing proper equipment, however, can be one of the more difficult challenges, because the cost of purchasing and upgrading sophisticated equipment and software places considerable burdens on the budget process.

Ultimately, personnel, training, and equipment needs require the direct involvement of senior officials, such as the Attorney General and FBI Director, because of the budget-request and budget-allocation processes that are involved with such expenditures. Moreover, in many jurisdictions, senior policymakers may not be as familiar with new computer and telecommunications technologies and with threats posed by cybercriminals. If senior government officials in those jurisdictions are unfamiliar with the technologies at

issue or the new threats and challenges they pose, they may be hesitant to support law enforcement by seeking appropriate legislative and budgetary changes. The need for adequate personnel, resources, and training is thus a critical issue in this increasingly important area of law enforcement.

2. Locating and Identifying Cybercriminals

When a hacker disrupts air traffic control at a local airport, when a cyberstalker sends a threatening e-mail to a public school or a local church, or when credit card numbers are stolen from a company engaged in e-commerce, investigators must locate the source of the communication. To accomplish this, they must trace the "electronic trail" leading from the victim back to the perpetrator. But the realities for law enforcement engaged in such a pursuit are very different from those of just a few years ago. Consequently, society faces significant challenges in the coming years as online criminals become more sophisticated and as technology may make anonymity more easily available. The following are some of the challenges facing both industry and law enforcement.

Divested and Diverse Environment. In today's communications environment, where telecommunication services are no longer provided by a monopoly carrier, a single end-to-end transmission is often carried by more than one carrier. As a result, the communications of a hacker or other criminal may pass through as many as a dozen (or more) different types of carriers, each with different technologies (e.g., local telephone companies, long-distance carriers, Internet service providers ("ISPs"), and wireless and satellite networks). The communication may also pass through carriers in a number of different countries, each in different time zones and subject to different legal systems. Indeed, each of these complications may exist within a single transmission. This phenomenon makes it more difficult (and sometimes impossible) to track criminals who are technologically savvy enough to hide their location and identity.

Wireless and Satellite Communications. Cellular and satellite-based telephone networks allow users to roam almost anywhere in the world using the same telephone. Although the social and commercial benefits of such networks are obvious, these networks can also provide a valuable communication tool for criminal use. Although sophisticated technology may allow law enforcement, under certain circumstances, to identify the general geographic region from which a wireless call is originating or terminating, the use of such technology raises profound and difficult issues at the intersection of privacy and law enforcement policies. Moreover, even identifying the owner of a particular mobile phone can be difficult, because mobile phones can be altered to transmit false identifying information. As the costs of mobile phones and mobile telephony service drop, we can expect to see the marketing of more "disposable phones," which will further complicate the ability of law enforcement agencies to gather evidence linking a perpetrator to the communication.

Satellite telephony presents additional issues. Current satellite-based networks transmit communications from users through one or more satellites and to earth-based gateways where the communications are routed using land-line systems. Providers of satellite-based telephony services typically do not need to build a gateway in each country to which service is to be provided. Indeed, it may be the case that one or two gateways can service an entire continent. The government's ability to protect the public's safety and privacy can be threatened in instances where a gateway servicing U.S. customers is located outside the U.S. In such cases, the content of the communications, as well as identifying information about the callers themselves, will be subject to the relevant laws (if any) of the host country and may not be protected in the same manner that the information is protected in the United States. More importantly to law enforcement, the location of a gateway in another country makes it difficult for law enforcement to meet its obligation to protect against criminal activities. In addition, law enforcement may have to rely on the willingness and technical and legal ability of the country in which the gateway is located to trace telephone calls, obtain information regarding suspected criminals in the United States, and provide that information to U.S. law enforcement agencies.

Recognizing the benefits and challenges created by advances in global telephony, the federal government has been working with telecommunications companies and foreign law enforcement agencies to ensure that the public interest is served in a global telephony environment. The government is also addressing global telecommunications issues in various international fora to ensure that the U.S. retains its ability to protect the U.S. public's privacy and safety.

Real-time Tracing. Tracing a communication from victim back to attacker may be possible only when the attacker actually is online. Sophisticated criminals can alter data concerning the source and destination of their communications, or they may use the Internet account of another. In addition, transmission information may not be retained or recorded by communications providers or may not be captured at all or held for only a short period of time. Even if it is generated and retained, it might be deleted by a skilled intruder to hide his identity.

Consequently, when law enforcement officials have information that a crime is being committed online, they often must attempt to trace a communication as it occurs. To do so, a law enforcement agency must know which computer crime expert to call in which jurisdiction, be able to contact the relevant individuals at various ISPs and carriers, and secure appropriate legal orders in each jurisdiction where a relevant carrier or ISP is located. (Notably, many ISPs already coordinate and cooperate with law enforcement agencies in this respect, and industry groups are developing "best practices" to encourage others to do the same.) Critical personnel must also be available when network-facilitated crimes occur after business hours. When these crimes occur across borders, real-time investigations must be able to proceed on an international scale.

Technical Infrastructure and Data Retention. If the communications network and the computers and software that run it have not been designed and configured to generate and preserve critical traffic data, information relating to the source and destination of a cyber-attack will likely not exist. Consider, for example, the use by many ISPs of modem banks to provide Internet access to incoming callers. An ISP may have 2 million customers, but maintain only 100,000 phone lines, based on an expectation that no more than 100,000 customers will ever dial in at any given time. The ISP may give only one access number to its customers and dynamically assign each incoming call to the next available line. Without a revenue-related reason for knowing the specific line used for each connection, the ISP's network may not be designed to generate the data necessary to link a customer with a specific incoming line. This, in turn, may make it impossible to trace the origin of the telephone call into the ISP's network. Such a network design can make it difficult to obtain traffic data critical to an investigation.

Even if a particular piece of the technical infrastructure is capable of generating and preserving needed data, such data are not useful if carriers do not collect and retain such records.¹⁷ Issues concerning whether, to what extent, and for how long critical data are retained are decided both by national laws (or the lack thereof) and by industry practices, which generally reflect market preferences and other revenue-related needs.¹⁸ In examining data retention practices and laws, careful consideration must be given to privacy concerns, market realities, and public safety needs.

U.S. law enforcement may be significantly affected by the 1995 and 1997 directives of the European Union ("EU") concerning the processing of personal data, including the deletion of traffic data. EU Member States are in the process of developing implementing legislation.¹⁹ As the directives are implemented into national legislation throughout the EU, it is vital that public safety be considered, along with the privacy and market force elements.

Anonymity. Anonymous e-mail accounts, which are e-mail accounts where subscriber

information is not requested or verified,²⁰ are the proverbial double-edged sword. Such anonymous accounts can protect privacy, but they add new complexities to identifying online lawbreakers, such as individuals who send child pornography, death threats, computer viruses, or copyright-protected works by e-mail.

Similarly, "anonymous re-mailer" services, which are e-mail services that strip the source address information from e-mail messages before passing them along to their intended recipients, raise difficult privacy and law enforcement policy issues. On the one hand, anonymous re-mailer services provide privacy and encourage freedom of expression. For example, in early 1999, these services allowed ethnic Albanians to provide first-hand accounts of Serbian atrocities in Kosovo without the fear of retribution. On the other hand, such services can plainly frustrate legitimate law enforcement efforts. Indeed, as early as 1996, one such service expressly touted itself as "a way to thwart attempts by intelligence agencies to trace illegal traffic It holds all incoming messages until five minutes after the hour, then re-mails them in random order. The messages are sent through five to twenty other re-mailers, with a stop in at least one of the several countries noted for lax law enforcement."²¹

To be sure, individuals can generally engage in many "real world" activities relatively anonymously, such as making small cash payments and attending public events. But they cannot remain anonymous in other contexts, such as opening a bank account or registering a car. Indeed, many financial institutions have substantial customer identification requirements. As discussed in Part II.B above, Internet-based activities should be treated consistently with physical world activities and in a technology-neutral way to further important societal goals (such as the deterrence and punishment of those who commit money laundering). National policies concerning anonymity and accountability on the Internet thus need to be developed in a way that takes account of privacy, authentication, and public safety concerns.

3. Collecting Evidence

When computers are used to store information, law enforcement agents generally can, upon securing a warrant, search the computer in the same way that they would a briefcase or file cabinet. The difference, of course, is that a computer can store a tremendous amount of information, including evidence that might not be known to the computer's owner.²² This feature of computer information can, of course, be both a benefit to and a challenge for law enforcement. It can benefit law enforcement by providing information (sometimes in a readily searchable way) that might not have existed in the non-computer world. But it can obviously present law enforcement challenges by highlighting the need for training and expertise (and time) for the information to be recovered. For example, one computer with 3 gigabytes of memory can contain the equivalent of one million pages of information. "Keyword" searches can miss relevant information, and the difficulty of the search and recovery of information may depend on how familiar the forensic expert is with the particular hardware and software configuration of the computer at issue. Moreover, if information on the computer is encrypted, it may be completely inaccessible to law enforcement and contribute little to solving the crime at issue (see box on encryption).

C. State and Local Tools and Capabilities

State and local law enforcement agencies play a significant role in addressing unlawful conduct on the Internet. These agencies have been crucial in combating online child pornography, prescription drug sales, gambling, and fraud. Consequently, any initiatives by the federal government to address unlawful conduct on the Internet must account for the important role state and local governments play in online investigations and prosecutions and should address the following three areas of fundamental concern to these state and local law enforcement authorities: (1) jurisdiction; (2) cooperation and coordination; and (3) resources.

The following is a brief discussion of the jurisdictional, cooperation and coordination, and resources issues facing state and local governments. Because the Executive Order that prompted this report focuses on federal law enforcement issues, we recommend that a more detailed analysis of state and local law enforcement issues be undertaken as a next step.

1. Jurisdiction

In responding to the challenge of law enforcement on the Internet, one of the problems that state and local governments face is that, although the crimes and schemes on the Internet may victimize local populations, the medium over which these crimes are committed permits a defendant to be located anywhere in the world. The traditional investigative tools available to the state – interviews, physical or electronic surveillance, and service of subpoenas for the production of documents or for testimony – are not necessarily adequate to compel information from a wrongdoer who is located out of state.

For example, if a fraud scheme is committed against Ohio residents by an operator of a website located in Florida, and the Ohio prosecutors issue a subpoena for records from the company in Florida, there is currently no formal procedural mechanism for the service and enforcement of that subpoena. Although the Ohio prosecutors may informally succeed in obtaining assistance from the Florida authorities, this is a matter of professional courtesy rather than legal process. There is no guarantee that the subpoena will be served, or, if served, enforced. Running into such a roadblock could well mean the end of the Ohio investigation. In the absence of any ability to investigate the case themselves, it remains possible for the Ohio prosecutors simply to refer the case to their Florida counterparts by reporting their complaints about the cybercriminal in Florida, but if the crime involves no Florida victims or is otherwise outside its jurisdiction, there is no guarantee that the case will be investigated by anyone.

This example illustrates the kinds of jurisdictional hurdles that are becoming increasingly common for state and local law enforcement authorities pursuing crime over the Internet. Another difficulty in this area arises from the disparate approaches taken by state courts to whether a state can exert long-arm jurisdiction over an Internet site accessible in that state. The lack of uniformity may make it more difficult for investigators in some jurisdictions to conduct meaningful investigations of Internet conduct. And, the enforcement of state electronic surveillance orders can also be a challenge. The Internet and modern satellite communications have made it more necessary for state wiretap orders to be served on and enforced against an out-of-state service provider. Unfortunately, no legal mechanism exists that would allow this. For example, drug traffickers operating entirely in New York, but using satellite telephones with signals that are received at a ground station outside of New York, potentially are completely immune from a New York wiretap order if the out-of-state ground station refuses to comply with a New York court's wiretap order.

2. Interstate and Federal-State Cooperation

Because the gathering of information in other jurisdictions and internationally will be crucial to investigating and prosecuting cybercrimes, all levels of government will need to develop concrete and reliable mechanisms for cooperating with each other. The very nature of the Internet – its potential for anonymity and its vast scope – may cause one law enforcement agency to investigate, inadvertently, the activities of another agency that is conducting an undercover operation. Likewise, the law enforcement agency of one state may require the assistance of another for capturing and extraditing a criminal to its state for prosecution. In other words, crimes that were once planned and executed in a single jurisdiction are now planned in one jurisdiction and executed in another, with victims throughout the United States and the world.

The effective coordination and cooperation between various branches of the law

enforcement community is crucial to any effort to combat unlawful conduct on the Internet. One area that may deserve further review concerns the extent to which federal, state, and local authorities can share and gather information about pending cases, potential targets, investigative procedures and tactics, and contact personnel. Such coordination is necessary for federal, state, and local law enforcement agencies to avoid duplicating and possibly undermining investigations.

In January 2000, Attorney General Reno challenged the National Association of Attorneys General and other state and local law enforcement groups to make it a priority to respond to these significant needs. Among other things, she specifically urged the groups to:

- Create a 24-hour cybercrime point of contact network, where each participating federal, state, and local law enforcement agency would provide a designated contact who is available 24 hours per day, 7 days per week to assist with cybercrime issues. This contact could be available via a pager system or coordinated through a centralized "command center."
- Create an online clearinghouse for sharing information to avoid duplication of effort and multiple investigations of the same unlawful conduct. Existing mechanisms, such as XSP, LEO, or Consumer Sentinel, may either serve this function or serve as building blocks for such a service.
- Develop conferences for all state and local Internet investigators and prosecutors, yearly or bi-annually, at which recent developments are discussed, case progress shared, and networks reinforced that will facilitate state, federal, and local cooperation.
- Develop additional policies and mechanisms to enhance cooperative interstate investigative and prosecutorial capacities and encourage coordination among their constituents.

3. Resources

Although state and local law enforcement organizations are responsible for investigating and prosecuting most forms of unlawful conduct involving the use of the Internet, they have limited resources with which to pay the substantial costs of developing the technical, investigative, and prosecutorial expertise and acquiring the new and often expensive technology necessary to address these crimes. Personnel, equipment, and training must be funded not only once but on a recurring basis. In addition, the structure of state and local law enforcement agencies is different from state to state and even county to county within a state. Resources must not be so restricted as to prohibit a state or local government from tailoring programs and initiatives within their current structures.

Federal funding can be useful in supplementing state and local spending on the necessary personnel, training, and equipment to properly investigate and prosecute high technology crime cases. To the extent that federal funds are expended on enhancing federal law enforcement's forensic capabilities, these projects should be structured in a way that allows state and local law enforcement to use these forensic resources. Regional computer forensic laboratories, such as the new laboratory in San Diego, have been successful and may be a model for other such facilities.²³

D. Legal Authorities: Gaps in Domestic Laws

Law enforcement agencies need strong laws to protect society against unlawful activity. This is as true in the online world as it is in the offline world. As discussed above in Part II and detailed in the appendices to this report, existing federal law is generally adequate to cover unlawful conduct involving the use of the Internet.

Strong substantive laws, however, that apply to the use of the Internet to commit traditional offenses such as fraud, child pornography, gambling, and the illegal sale of intellectual property are necessary but not sufficient to ensure a safe and secure online environment. To achieve that goal, law enforcement, in cooperation with the private sector, must also be able to gather evidence, investigate, and prosecute these cases. Unfortunately, in some areas, the legal authorities and tools needed to do this have lagged behind technological and social changes. This section examines several laws related to the investigation and prosecution of high-tech offenses that have not kept pace with technological changes. Although we do not offer specific solutions in this report, we are committed to working with interested parties to devise appropriate solutions.

1. Pen Register and Trap and Trace Statute

Pen registers (devices that record the numbers dialed on a telephone line) and trap and trace devices (devices that capture incoming electronic impulses that identify the originating number) are important tools in the investigation of unlawful conduct on the Internet. Unfortunately, the statute that governs such devices, 18 U.S.C. §§ 3121-3127, is not technology-neutral and has become outdated.

As an initial matter, advances in telecommunications technology have made the language of the statute obsolete. The statute, for example, refers to a "device" that is "attached" to a telephone "line," *id.* § 3127(3). Telephone companies, however, no longer accomplish these functions using physical hardware attached to actual telephone lines. Moreover, the statute focuses specifically on telephone "numbers," *id.*, a concept made out-of-date by the need to trace communications over the Internet that may use other means to identify users' accounts.

Moreover, the deregulation of the telecommunications industry has created unprecedented hurdles in tracing long-distance telephone calls. Many different companies, located in a variety of judicial districts, may handle a single call. Under the existing statute, however, a court can only order communications carriers within its district to provide tracing information to law enforcement. As a result, investigators have to apply for several, sometimes many, court orders to trace a single communication, causing needless waste of time and resources and hampering important investigations.

2. Computer Fraud and Abuse Act

Originally passed in 1984, and amended in 1986, 1994, and 1996, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, protects a broad range of computers that facilitate interstate and international commerce and communications. For example, section 1030(a)(2) makes it a crime to access a computer without or in excess of authority and obtain (1) financial information from a financial institution or credit reporting company; (2) any information in the possession of the government; or (3) any private information where the defendant's conduct involves interstate or foreign commerce. Section 1030(a)(5) makes it a crime for anyone to knowingly cause the transmission of a computer program, information, code, or command, that results in unauthorized damage to a protected computer. (A "protected computer" is one used exclusively or partly by the United States or a financial institution in which the defendant's conduct affects the government's or financial institution's operation of the computer; or any computer that is used in interstate or foreign commerce or communications, see 18 U.S.C. § 1030(e)(2).)²⁴

Despite its broad reach and relatively recent amendment, the statute nevertheless contains several flaws that could hinder law enforcement's ability to respond effectively to unlawful conduct on the Internet. For example, given the increasing interdependency and availability of global computer networks, it is increasingly likely that computer system intruders within the United States may begin to concentrate their unlawful activity on systems located

entirely outside the United States. Alternatively, individuals in foreign countries may route communications through systems located within the United States, even as they hack from one foreign country to another. In such cases, they may hope that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution. It is unclear whether section 1030, in its existing form, protects against such situations, which may affect the United States even though the perpetrator and the victim are located elsewhere.

The Department of Justice has encountered several instances where intruders have attempted to damage critical systems used in furtherance of the administration of justice, national defense, or national security, as well as systems (whether publicly or privately owned) that are used in the provision of "critical infrastructure" services such as telecommunications, transportation, or various financial services, but where proof of damage in excess of \$5,000, as required by section 1030(a)(5), has not been readily available. Although such activities may pose extreme risks to our infrastructure, section 1030(a)(5) currently does not allow law enforcement to proceed without evidence of over \$5,000 in damages.

Another problem is that prosecutions under section 1030(a)(5) carry a mandatory minimum sentence of at least six months. In some instances, prosecutors have exercised their discretion and elected not to charge some defendants whose actions otherwise would qualify them for prosecution under that section, knowing that the result would be mandatory imprisonment. It may be useful to examine whether requiring imprisonment for six months should be applied in more limited circumstances than allowed under existing law, or whether other punishments, such as reduced penalties and forfeiture of any instrumentalities or proceeds of the violation, might provide adequate punishment and deterrence.

3. Privacy Protection Act

The Privacy Protection Act of 1980 ("PPA"), 42 U.S.C. §2000aa, et seq., makes it unlawful for local, state, or federal law enforcement authorities to "search for or seize any work product materials" or any "documentary materials . . . possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication," 42 U.S.C. § 2000aa(a), (b) (emphasis added). The statute defines "work product materials" as materials prepared or possessed in anticipation of communicating such materials to the public, except if the materials constitute contraband or the fruits or instrumentalities of crime. *Id.* § 2000aa-7(b). "Documentary materials," on the other hand, consist of materials upon which information is recorded, once again with the exception of contraband and the fruits or instrumentalities of crime. *Id.* § 2000aa-7(a).

In enacting the PPA, Congress restricted searches for evidence of crime held by innocent third-parties who were engaged in First Amendment-protected activities. The PPA thus protects the confidentiality of non-evidentiary files held by this special group of innocent third-parties – such as drafts of articles not yet published and the research and other supporting information (e.g., notes and interviews) that are never intended to be published. To preserve the confidentiality of these designated materials, the PPA instructs investigators not to search for the evidence at all, but to compel the innocent third-parties to find and produce it themselves. Thus, subject to certain exceptions, the PPA generally limits searches for work-product and documentary materials held by third-parties who plan to use them to communicate to the public.

New issues arise with the PPA due to the exponential growth in computer use over the last decade. With the advent of the Internet and widespread computer use, almost any computer can be used to "publish" material. As a result, the PPA may now apply to almost any search of any computer. Because computers now commonly contain enormous data storage devices, wrongdoers can use them to store material for publication – material that the PPA protects – while simultaneously storing (in a commingled fashion) child pornography,

stolen classified documents, or other contraband or evidence of crime.

4. Electronic Communications Privacy Act

In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 et seq., in an effort to revise and expand the scope of the 1968 wiretap act. The statute attempted to strike a workable balance among the competing interests addressed in the statute at the time: the privacy interests of telecommunications users, the business interests of service providers, and the legitimate needs of government investigators.

Two factors have raised concerns about ECPA: (1) the statute treats wire and electronic communications inconsistently; and (2) use of the Internet has grown dramatically, and voice and non-voice data have converged. First, although ECPA attempted to create a technology-neutral framework for regulating the disclosure of electronic communications and records, it was only partially successful. For example, the 1986 legislation distinguished broadly between "wire communications" (such as voice telephone calls) and "electronic communications," which it accorded lesser protections. This inconsistency creates practical problems in today's converged network environment where voice and non-voice data may be intertwined in a single data stream.

These inconsistencies take on additional significance with the now widespread use of computers and the Internet, because the proportion of criminal activity occurring online, or using telecommunications technologies, has increased over time. E-mail, voice mail, user access logs, and remotely stored files play an important, and in many cases, critical role in investigating and prosecuting crimes ranging from large-scale consumer fraud to extortion and murder.

These developments suggest that ECPA be carefully evaluated to ensure that it (1) takes into account new communications technologies in its treatment of wire and electronic communications; (2) has appropriate penalties for a variety of criminal invasions of communications privacy; (3) resolves deficiencies in the rules for government access to customer records, especially with respect to access by civil and regulatory agencies; and (4) cures omissions and inconsistencies within the statutory framework.

5. Telephone Harassment

The Internet and the widespread use of computers have created a host of new tools for communication. Existing statutes provide criminal penalties for persons who use telephones to harass or abuse others. For example, one provision of 47 U.S.C. § 223 makes it a federal crime, punishable by up to two years in prison, to use a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the called number. The statutory prohibition applies only if the perpetrator does not reveal his or her name. See 47 U.S.C. § 223(a)(1)(C).

The new means of communication by computer, however, have given computer users a new method of inflicting such abuse not covered by the existing laws. A malicious computer user, for example, can post an electronic message in which he pretends to be the person that he intends to harass (see cyberstalking box in Part II.A above). In this fraudulent message (that may reach thousands of people), he can state, for example, that he (posing as the victim) likes to participate in some particular sexual act and then invite anyone who reads the message to call the victim's home telephone number. Yet this form of harassment evades the prohibitions of 47 U.S.C. § 223, which applies only to direct communications between the perpetrator and the victim.

6. Cable Communications Policy Act

The Cable Communications Policy Act of 1984, which regulates various aspects of the cable television industry, includes provisions that protect the privacy of individual cable

subscribers' records. See 47 U.S.C. § 551(c), (h). Such records should indeed remain private under most circumstances. The statute, however, did not take into account the changes in technology that have occurred over the last 15 years. Cable television companies now often provide Internet access and telephone service in addition to television programming. Some cable companies have interpreted the statute as overriding their obligations to disclose certain records pursuant to other statutes, such as the Electronic Communications Privacy Act, 18 U.S.C. § 2701, and the trap and trace statute, 18 U.S.C. § 3121. This interpretation – which courts have not accepted – would create greater protections for subscribers who receive Internet service from cable companies than for those who access the Internet by other methods.

Such an interpretation is inconsistent with the technology-neutrality principle discussed in section II.B above. Moreover, some cable companies that provide Internet service have relied on the Act to refuse to disclose subscriber information pursuant to state grand jury subpoenas, even though these records would otherwise be available through legal process under existing law. As more and more Internet users shift to high-speed cable access from traditional analog telephone equipment, it will be important to ensure that privacy standards are harmonized for all Internet users.

* * *

These examples are only some of the areas in which the law has not kept up with new technology. Specific legislative proposals to update these laws are beyond the scope of this report. The gaps illuminate, however, the investigatory challenges posed by the use of the Internet for unlawful conduct, and they deserve prompt legislative consideration and attention.

E. Challenges for International Cooperation

1. Substantive International Criminal Law

When one country's laws criminalize high-tech and computer-related crime and another country's laws do not, cooperation to solve a crime, as well as the possibility of extraditing the criminal to stand trial, may not be possible. Inadequate regimes for international legal assistance and extradition can therefore, in effect, shield criminals from law enforcement: criminals can go unpunished in one country, while they thwart the efforts of other countries to protect their citizens.

International legal assistance can be requested and provided through several means. The United States is party to over 20 bilateral mutual legal assistance treaties ("MLATs"). Where there is no MLAT in force, international legal assistance is governed by domestic mutual legal assistance laws and practices, which include the letters rogatory process. (A letter rogatory is a letter request for assistance from one country's judicial authority – e.g., a U.S. District Court – to that of another country. See, e.g., 28 U.S.C. § 1782.) MLATs and domestic laws vary with regard to the requirements relating to a request for assistance. To issue subpoenas, interview witnesses, or produce documents, some MLATs and some laws permit assistance as long as the conduct under investigation is a crime in the requesting state, even where it is not also a crime in the requested state.

In the more sensitive area of searches and seizures, however, dual criminality (i.e., that the conduct under investigation is a crime in both the requesting and requested countries and is punishable by at least one year in prison) is often required (e.g., U.S./Netherlands MLAT). In other circumstances, a country can refuse a request if the request "relates to conduct in respect of which powers of search and seizure would not be exercisable in the territory of the Requested Party in similar circumstances" (e.g., U.S./U.K. MLAT). Finally, some MLATs and domestic laws permit assistance only if dual criminality exists and if the offense is extraditable (e.g., mutual assistance laws of Germany). With regard to extradition, the United States has entered into bilateral treaties with over 100 countries. These treaties are

either "list treaties," containing a list of offenses for which extradition is available, or they require dual criminality and that the offense be punishable by a specified minimum period. Therefore, if one country does not criminalize computer misuse (or provide for sufficient punishment), extradition may be prohibited.

The issue of dual criminality is not an academic or theoretical matter. In 1992, for example, hackers from Switzerland attacked the San Diego Supercomputer Center. The U.S. sought help from the Swiss, but the investigation was stymied due to lack of dual criminality (i.e., the two nations did not have similar laws banning the conduct), which in turn impeded official cooperation. Before long, the hacking stopped, the trail went cold, and the case had to be closed.

The solution to the problems stemming from inadequate laws is simple to state, but not as easy to implement: countries need to reach a consensus as to which computer and technology-related activities should be criminalized, and then commit to taking appropriate domestic actions. Unfortunately, a true international "consensus" concerning the activities that universally should be criminalized is likely to take time to develop. Even after a consensus is reached, individual countries that lack appropriate legislation will each have to pass new laws, an often time-consuming and iterative process.

2. Multilateral Efforts

Although bilateral cooperation is important in pursuing investigations concerning unlawful conduct involving the use of the Internet, multilateral efforts are a more effective way to develop international policy and cooperation in this area. The reason for this stems from the nature of the Internet itself. Because Internet access is available in over 200 countries, and because criminals can route their communications through any of these countries, law enforcement challenges must be addressed on as broad a basis as possible, because law enforcement assistance may be required from any Internet-connected country. That is, even if two countries were able to resolve all the high-tech crime issues they faced, they would still (presumably) only be able to solve those crimes that involved their two countries. Multilateral fora allow many countries to seek solutions that will be compatible to the greatest extent with each country's domestic laws.

Several multilateral groups currently are addressing high-tech and computer-related crime. Of these groups, the Council of Europe ("COE"), and the Group of Eight ("G-8") countries are the most active. To begin to address the need to harmonize countries' computer crime laws, the COE is drafting a Cybercrime Convention, which will define cybercrime offenses and address such topics as jurisdiction, international cooperation, and search and seizure. The Convention may be completed as soon as December 2000. After approval by a high-level committee, the Convention will be open for signature by COE members and non-member states which participated in the drafting. The G-8 Subgroup on High-tech Crime has been focusing on ways to enhance the abilities of law enforcement agencies to investigate and to prosecute computer- and Internet-facilitated crimes, such as establishing a global network of high-tech crime experts and developing capabilities to locate and identify those who use the Internet to commit crimes. In May 1998, President Clinton and his G-8 counterparts adopted a set of principles and an action plan, developed by the Subgroup, for fighting computer crime. The COE and G-8 efforts, as well as other international efforts, are described in more detail in Appendix J to this report.

3. Continuing Need for International Cooperation

As these multilateral efforts progress and as more formal mechanisms for cooperation are developed, law enforcement agencies in the U.S. and other countries are cooperating informally and have undertaken joint initiatives to achieve their goals. For example, the Customs Service has been involved in joint cyber-investigations with the German Federal police. These joint investigations have resulted in 24 referrals from Customs'

Cybersmuggling Center to field offices during the last three months. In most instances, these referrals have led to the issuance of federal or state search warrants. Customs is also involved in joint efforts on Internet-related investigations involving money laundering and child pornography distribution with officials in countries such as Indonesia, Italy, Honduras, Thailand, and Russia.

As international issues become more prevalent in investigations of Internet-facilitated offenses, U.S. law enforcement agencies must continue to develop cooperative working relationships with their foreign counterparts. The 24/7 high-tech point-of-contact network established among the G-8 countries and others must continue to be developed and expanded to include more countries. In addition, the U.S. should continue to work with other countries, international groups, and industry to develop comprehensive and global plans for addressing the complex and challenging legal and policy issues surrounding jurisdiction raised by unlawful conduct on the Internet.

IV. THE ROLE OF PUBLIC EDUCATION AND EMPOWERMENT

The third component of the Working Group's 3-part strategy for responding to unlawful conduct involving the use of the Internet is to implement aggressive efforts to educate and empower the public to minimize risks associated with the Internet and to use the Internet responsibly through technological and non-technological tools. Although both types of tools can be extremely useful when used appropriately, "one size does not fit all." One must weigh the advantages and disadvantages in determining which set of tools will work best for an individual's particular situation.

This part of the report therefore discusses existing and potential new tools and resources that can be used to educate and empower parents, teachers, and others to prevent or minimize the risks from unlawful conduct involving use of the Internet. First, we review the technological and non-technological tools that are available for parents and teachers to use to help ensure that children have a safe and rewarding experience online. Next, we discuss how consumers can educate themselves in order to avoid fraudulent and deceptive practices on the Internet. In particular, this part highlights how several federal agencies are using technology to educate consumers and how they are working with the private sector to develop effective consumer protection practices. Many other agencies are undertaking similar efforts. Last, we discuss government-industry cooperation efforts to educate the public on the importance of being good "cybercitizens."

A. Educating and Empowering Parents, Teachers, and Children

With the growing number of U.S. classrooms connected to the Internet and the rising number of personal computers used in the home, more and more children are now able to access the Internet. Almost 90 percent of public schools – including over 1 million classrooms – in the U.S. are connected to the Internet. Over 40 percent of American households own computers and one-quarter of all households have Internet access.²⁵

One of the greatest benefits of the Internet is the access it provides children to such things as educational materials, subject matter experts, online friendships, and penpals. Nevertheless, like many other pursuits that children engage in without adequate parental supervision, the Internet should also be approached with careful consideration of risks and benefits. One concern of course is that the Internet may allow children unrestricted access to inappropriate materials. Such materials may contain sexually explicit images or descriptions, advocate hate or bigotry, contain graphic violence, or promote drug use or other illegal activities. In the worst instances, children have become victims of physical molestation and harassment by providing personal information about themselves over the Internet and making contact with strangers.

To protect children from such risks, parents and teachers therefore need to empower themselves with the tools, knowledge, and resources to supervise and guide children's online experience and to teach children how to use the Internet responsibly.

1. Technological Tools

Technology provides tools that may assist in preventing children from accessing inappropriate materials on the Internet or divulging personal information about themselves or their families online. The most common technological tools are "blocking" and "filtering" software, as described more fully below.

(a) Blocking Software

"Blocking" software uses a "bad site" list and prevents access to those sites. The vendor of the software identifies specified categories of words or phrases that are deemed inappropriate and configures the blocking software to block sites on which the prohibited language appears. Although some vendors allow parents to customize the "bad site" list by allowing them to add or remove sites, others keep the list secret and do not permit parents to modify it.

Although such software can be a useful tool for restricting access to inappropriate websites in certain circumstances, they can also create a false sense of security, because they cannot restrict access to all inappropriate sites for children. The number of websites published each day far exceeds the ability of software companies to review the sites and categorize them for their "bad site" lists.²⁶ "Out of approximately 3 million separate websites in existence (each website may contain two or more separate webpages and the number of separate files, pages and graphics online is estimated at 330 million), only a small fraction have been reviewed, in aggregate, by child protection software companies."²⁷ Because the gap widens daily, with an estimated 160,000 new websites registered each month, "bad sites" will inevitably get through.²⁸

Another potential drawback is that most blocking software does not differentiate between the age of the users. What may be inappropriate for an eight year old, may be appropriate for a teenager. However, because most software only has one user setting to determine what should be blocked, either the teenager will be denied access to sites that are beneficial or the eight-year-old will be given access to sites that are inappropriate. In addition, in cases where software vendors do not allow parents to customize the "bad site" list, parents cannot make an informed decision on what material should be restricted. They must rely on the judgment of an unknown third party to decide what sites are acceptable for their children.

(b) Filtering Software

"Filtering" software blocks sites containing keywords, alone or in context with other keywords. For example, if parents wanted to restrict their child's access to sites related to drug use, the software would be configured to deny access to sites containing such words as "marijuana," "cocaine," "heroin," etc. Filtering software is available both directly and through some Internet service providers ("ISPs") such as Lycos or FamilyNet.

Filtering software can also be used to restrict access to inappropriate websites, but, like blocking software, they can be both underinclusive and overinclusive. They can, for example, filter sites that are either harmless or even desirable. With the example above, sites that promote drug rehabilitation, seeking help for a drug problem, or drug prevention would be blocked simply because they use the keywords. Another example of how filtering is over inclusive is denying access to the word "sex." While this filter would block certain sites with inappropriate sexual content, it would also block harmless sites that contained the words "sextuplets," "sexton," "Mars Exploration," among many others. In addition, some website operators have learned to bypass the filtering mechanism by misspelling the typical

keywords.29

Filtering software may also be used to block sites that have a particular label or rating. The content provider or a labeling service classifies the site in a particular category (e.g., "romance: no sex" or "explicit sexual activity") and the filtering software is programmed to deny access to sites with particular ratings. As with "bad sites," parents must rely on the judgment of unknown third parties to determine what is appropriate for their children. In this case, the content provider must self-label the site accurately or a labeling service must assign the appropriate label to the site. Another major drawback is that very few sites are labeled. Parents must decide whether to block or allow access to unrated sites. Blocking all unrated sites would deny access to harmless and educational material, while allowing access to all unrated sites would undoubtedly allow inappropriate material to get through.

(c) Other Software

Other types of software enable parents to monitor and control their children's use of the computer. For example, "monitoring and tracking" software allows parents to track how much time their children spend online, where their children go online, and how much time their children spend on the computer offline. "Outgoing filtering" software prevents children from sharing certain information with others over the Internet, such as their name, telephone number, and address. Every time the child tries to send the prohibited information to someone online, it shows up as "XXX."

2. Non-technological Tools

(a) What Parents Can Do

One of the most effective ways of protecting children from inappropriate material on the Internet is to teach them to use the Internet responsibly. Parents play a major role in this by taking responsibility for children's online computer use. By doing so, parents can greatly minimize any potential risks of being online.

There are certain safety tips parents can follow to ensure that their children use the Internet safely. These tips include:

- never give out personal information, such as home address, school name, or telephone number, in a public message such as a chat room or bulletin board;
- do not post photographs of children on websites or news groups that are available to the public;
- never allow a child to arrange a face-to-face meeting with another computer user without parental permission;
- if a meeting is arranged, make the first one in a public place and be sure to accompany the child;
- never respond to messages that are suggestive, obscene, belligerent, threatening or make you feel uncomfortable;
- encourage children to tell you if they encounter such messages;
- report any inappropriate messages you receive immediately;
- consider keeping the computer in a room other than the child's bedroom to monitor his or her online use;

- get to know your children's online friends just as you get to know all of their other friends;
- set up specific rules for your children's online use, such as the time of day and length of time that they can be online and appropriate sites for them to visit.³⁰

There are many useful publications and websites for parents on this topic. For example, *The Parent's Guide to the Internet* (published by the U.S. Department of Education), *Site Seeing on the Internet: A Guide to Traveling in Cyberspace* (published by the FTC and the National Association of Attorneys General), and *The Parent's Guide to the Internet: Raising Your Family on the Information Superhighway* (by Travis West) explain the basics of the Internet, how it works, what is available online, and give guidance on how to ensure safe use of the Internet. For additional publications on responsible use of the Internet, visit www.childrenspartnership.org for a list of resources.

Likewise, there are many websites that give parents guidelines to promote safe, rewarding online experiences for children. For example:

- www.getnetwise.org – This website was created by 15 Internet companies as a comprehensive resource guide for parents. It includes instant access to tools representing the latest technologies that allow parents to block and filter inappropriate content, monitor the websites and chat rooms that their children visit, and set strict time limits on their children's online sessions. It also includes access to information on how to report a crime or other troubling activity online and provides a guide to quality, educational websites beneficial to children. The website also provides safety tips for online use.
- www.americalinksup.org – This website seeks to bring the online industry, families, teachers, librarians and other children's advocates together to ensure that children have a rewarding and educational online experience. It provides safety tips for parents and children; access to discussion groups of parents, teachers and other Internet users on critical safety issues; links to more than 700 quality websites for children reviewed and recommended by children's librarians; and information on local events where parents and children can learn about Internet basics and tools that promote rewarding online experiences.
- www.cyberangels.org – This website has been in existence since 1995 and is considered the largest Internet safety and education program. In addition to providing parents guidance on how to supervise their children online, it teaches children how to use the Internet safely with material geared toward them. For example, children can join Sophia's Safe Surfing Club, take a safe surfing quiz, and earn a safe surfing permit. Cyberangels also has Net Patrol teams that regularly monitor the Internet for child-crimes, cyberstalkers, and fraudulent scams and report it to law enforcement authorities. The website provides support groups for victims of stalking and harassment over the Internet and gives tips on how to document and report cyber-stalking. CyberAngels also provides links to safe sites and reviews and recommends blocking/filtering software.
- www.parentech.org – This site provides families and educators of middle school children (grades 6-8) with free resources focusing on how technology affects education, careers, and society. It includes parent and teacher guides in these three areas. For example, the parent's guide on technology and education has articles on how to help middle schoolers get the most out of learning with technology, a parent's guide to classroom technologies, and technology standards for middle schools. The teacher's guide to technology and careers includes articles on what skills are necessary for these careers and how to

develop those skills at the middle school level. In addition, the site has a discussion corner where parents and educators can share ideas, concerns, and questions with each other and with experts from across the nation.

- www.safekids.com – This website contains various articles about Internet basics and online safety, guidelines for parents on how to supervise their children on the Internet, safety tips for children, and filtering/blocking software reviews. In addition, the site has links to other sites that offer Internet advice to parents and includes a link to report online crime against children.

(b) What Schools and Libraries Can Do

As increasing numbers of children have access to the Internet from their schools and neighborhood libraries, we need to address the issue of how best to ensure that these children have positive, age-appropriate, educational online experiences. The Administration has taken the view that empowering parents, teachers, and librarians with a wide range of tools with which they can protect children in their community in a manner consistent with their values is ultimately the most effective approach and one that is most compatible with the First Amendment.³¹

Schools and libraries are currently using a wide range of technology tools and monitoring techniques to ensure that children do not encounter inappropriate material or dangerous situations while online. These schools and libraries are determining what will work best in their particular schools and communities. Absent proof that local decision making is not working to protect our children, the federal government should not mandate a particular type of technology, such as filtering or blocking software. Rather, we should encourage "acceptable use" policies ("AUPs") by all public institutions that offer access to online resources, including the Internet. Such policies may include the use of blocking and filtering technologies, or they may involve the use of monitoring, smart cards, or codes of conduct. An AUP should, while being sensitive to local needs and concerns, offer reasonable assurances to parents that safeguards will be in place in the particular school or library setting that permit users to be empowered to have educational experiences consistent with their values.

In addition to AUPs, schools may also use "intranets" to restrict student access to inappropriate material. An intranet is a controlled computer network that uses similar software and transmission mechanisms as the Internet, but is accessible only to those who have permission to use it (an intranet is generally confined to users within an organization). These controls permit the intranet system managers to limit user access to Internet material as well as to restrict those outside the network from being able to reach it.

Schools and districts may also use Regional Technology and Education Consortia organizations ("RTECs") as a resource. Six regional consortia, funded by the Department of Education, assist and support states, districts, schools, and other educational institutions in the use of advanced technologies to improve teaching and student achievement. In helping schools and districts with planning and implementation of technology, RTECs can help schools identify Internet safety solutions that meet the schools' needs and policy preferences. In addition, RTECs also provide resources for teacher training in technology.

(c) Next Steps

The Department of Justice and the Department of Education have funded a study by the National Academy of Sciences on how to protect children from inappropriate material on the Internet. This study will include a description of the risks and benefits of various tools and strategies that can be used to protect children from inappropriate material, an analysis of how the different tools and strategies can be used together, and case studies of how different communities have approached this problem. The final report is scheduled to be completed

in November 2001.

In addition, in October 1998, Congress passed the Child Online Protection Act ("COPA")³² that, among other things, established a Commission on Online Child Protection to examine the extent to which current technological tools effectively help protect children from inappropriate online content. The members of the commission were appointed last year, with the final members coming on board in October 1999, and the commission's report is due to Congress in November 2000.

Finally, the Departments of Commerce, Education, and Justice are planning a joint effort to host a roundtable discussion with industry representatives, especially those in the software industry, to discuss the benefits and limitations of existing blocking and filtering software. These discussions can lay the groundwork for future software contributions to Internet safety.

B. Educating and Empowering Consumers

The electronic marketplace offers consumers unprecedented choice and around-the-clock accessibility and convenience. It gives established marketers and new entrepreneurs low-cost access to a virtually unlimited customer base. With these benefits, however, comes the challenge of ensuring that the virtual marketplace is a safe and secure place to purchase goods, services, and digitized information. Consumers must be confident that the goods and services offered online are fairly represented and the merchants with whom they are dealing – many of whom may be located in another part of the world – deliver their goods in a timely manner and are not engaged in illegal business practices like fraud or deception. Consumer confidence also requires that consumers have access to fair and effective redress if they are not satisfied with some aspect of the transaction.

This section highlights some of the Federal Trade Commission's initiatives to educate consumers through technology; the Department of Commerce's coordination efforts with the private sector to develop effective consumer protection practices; and the Food and Drug Administration's outreach campaign regarding medical products on the Internet. As described more fully below, the FTC has made innovative use of the Internet to educate and alert consumers about fraud and deceptive practices online, to disseminate its publications, to investigate potential violations, and to receive and respond to consumer complaints. The Department of Commerce has also worked with consumer and business representatives to develop codes of conduct for electronic commerce and mechanisms for consumer dispute resolution, redress, and enforcement. In addition, the FDA has used the Internet to educate consumers and health professionals about the possible risks of ordering prescription medications and other medical products on the Internet, and the Securities and Exchange Commission ("SEC") has likewise used the Internet to help investors avoid online securities fraud. The Postal Inspection Service posts consumer fraud prevention "tip sheets" and other fraud prevention information on its website (www.usps.gov/postalinspectors). And, as part of its Internet Fraud Initiative, the Department of Justice has been active in public education and outreach efforts to prevent online fraud (e.g., establishing a website on identity theft and fraud (www.usdoj.gov/criminal/fraud/idtheft)), and the FBI has prepared an online Parent's Guide to Internet Safety (www.fbi.gov).

1. FTC Initiatives: Using Technology to Educate Consumers

The FTC is committed to stemming fraudulent, misleading, and deceptive trade practices through actions that involve both law enforcement and education. Acting on the belief that the most effective consumer protection is education, the FTC has sought to help alert as many consumers as possible to the telltale signs of fraud, the importance of privacy in the information age, and other critical consumer protection issues. Use of the Internet to develop and disseminate information about fraud and technology-related matters is integral to the FTC's education, deterrence, and enforcement efforts and has allowed the agency to

reach vast numbers of consumers and businesses quickly, simply, and at low cost.

(a) Fraud Prevention Information for Consumers

More than 200 of the consumer and business publications produced by the FTC's Bureau of Consumer Protection are available on the agency's website in text and .pdf format. Indeed, the difference in the number of publications viewed online in 1996 and 1999 (140,000 versus 2.5 million page-views) tells the story of the Internet's coming of age as a mainstream medium and its importance to any large-scale dissemination effort. Those 2.5 million page views are in addition to the 6 million print publications distributed each year to organizations that disseminate them on the FTC's behalf.

(b) Link Program

The FTC also actively encourages "partners" – government agencies, associations, organizations, and corporations with an interest in a particular subject – to link to the FTC's website from their sites and to place banner public service announcements provided by the FTC on their sites. Links from the banners allow visitors to click through to the FTC site quickly to get the information the user is looking for exactly when they want it. Among the organizations that have helped drive traffic to the consumer information on www.ftc.gov are the Alliance for Investor Education, the Arthritis Foundation, the American Association of Retired Persons, American Express, the Better Business Bureau, CBS, Circuit City, motleyfool.com, the National Institutes of Health, the North American Securities Administrators Association, Shape Up America!, the U.S. Patent and Trademark Office, and Yahoo!.

(c) "Sting" Pages

Many Internet shoppers looking for weight loss products will find an attractive-looking site that trumpets NordiCaLite, a "safe and natural" way to lose weight. Three clicks into the sales pitch, the FTC seal appears, alerting consumers that the site was put up by the federal agency, that the product is a fake, and that certain words and phrases are tip offs to help them avoid most rip offs.

Too often, warning information about frauds reaches consumers after they've been scammed. For the FTC, the challenge is how to reach consumers before they fall victim to a fraudulent scheme. Knowing that many consumers use the Internet to shop for information, agency staff develop "sting" sites that mimic the characteristics of a site selling fraudulent products or services. "Metatags" embedded in the FTC websites make them accessible to consumers who are using major search engines and indexing services as they look for products, services, and business opportunities. The "sting" websites link back to the FTC's webpage, where consumers can find the practical, plain English information they need. The agency has developed 13 "sting" sites on topics ranging from health care products to scholarship services to vacation deals and investments, and feedback from the public has been overwhelmingly positive. Many visitors express appreciation – not only for the information, but also for the novel, trouble-free, and anonymous way it is offered.

(d) Tutorials

The FTC has also developed interactive puzzles and games to reinforce the concepts spelled out in its brochures, 1-page "news you can use" consumer alerts, and graphics. For example, to mark the first anniversary of the Telemarketing Sales Rule in December 1996, the FTC placed a recording of a fraudulent telemarketing call on its website and developed a quiz to test a consumer's ability to tell the difference between a legitimate call and fraudulent one. Later, the Field of Schemes investment fraud initiative included the launch of an online quiz called "Test Your Investment I.Q." A series of typical telephone misrepresentations asked consumers to define an investment offering as solid or risky and

then explained the answers. As part of Project Mousetrap, which dealt with fraudulent invention promotion firms, the FTC created an activity designed to test a reader's "patent-ability": a crossword puzzle containing critical terms from the world of patents and idea promotion. And to support the first National Consumer Protection Week, an online crossword puzzle, a true-false quiz, and a word find that focused on credit terms were developed for the National Consumer Protection Weekly, a newsletter that was distributed electronically to consumer agencies, law enforcement officials, and corporations across the country.

(e) Consumer.gov

Armed with a vision of the Internet as a powerful tool for consumer education and empowerment, the FTC convened a group of five small federal agencies in 1997 to develop and launch a website that would offer 1-stop access to the array of federal consumer information. On the theory that consumers may not know one federal agency from another, the information is arranged topically. Federal agencies and consumers have responded well to www.consumer.gov. The site includes contributions from over 100 federal agencies and logs some 79,000 user sessions a month, each of which last an average of over four minutes. The site also houses special initiatives: The President's Council on Y2K Conversion asked the FTC to establish a Y2K consumer information site; the Quality Interagency Coordination Task Force requested a special site on health care quality; and the U.S. Postal Inspection Service asked that www.consumer.gov house the site to support the "kNOw Fraud" initiative, a public-private campaign that involved sending postcards about telemarketing fraud to 115 million American households in the fall of 1999. The original www.consumer.gov team received the Hammer Award for its efforts. The FTC continues to maintain the site.

(f) Spam Mailbox

Millions of consumers are besieged by unsolicited commercial e-mail ("UCE") or "spam" every time they open their e-mailboxes. At best, spam is annoying. At worst, it is costly and disruptive to consumers.³³ Hoping to relieve consumer frustration and gain a foothold on deceptive e-mail offers, the FTC invited consumers to forward their spam to a special address (uce@ftc.gov). With 3,000 e-mails arriving each day, the FTC has been able to build a spam database that is an extremely helpful resource for investigators. With partners from the Postal Inspection Service, the agency lets "junk e-mailers" know how not to break the law, and lets consumers know how to recognize the 12 most common types of e-mail fraud, known as the "dirty dozen."

(g) Online Complaint Handling

By 1998, with consumer use of the Internet to access information, entertainment, products and services becoming routine, the FTC began accepting consumer complaints electronically. The consumer response to the online complaint feature indicates that the FTC is meeting a real need: The agency receives online – and responds online to – an estimated 1,000 complaints and inquiries a week.

(h) Business Education for Online Marketers

As part of its mission, the FTC provides guidance to online marketers on how to assure that basic consumer protection principles apply online. Many of these entrepreneurs, new to the Internet and to marketing in general, may be unfamiliar with consumer protection laws. But even experienced marketers have raised novel issues in their efforts to apply traditional consumer protection laws to the online environment. The FTC has used a variety of approaches to get its consumer protection messages out to the business community, from compliance guides, brochures and speeches at industry and academic meetings and conferences to e-mails and Web-based public service announcements, staff advisory letters

on www.ftc.gov, use of the trade press to promote the availability of information on the agency site, and workshops on issues of interest and posting the transcripts.

(i) Publications for Business

Among the publications for business that have been distributed widely in print and online are Advertising and Marketing on the Internet: Rules of the Road, which has had a print distribution of over 22,000 and over 33,000 page-views of the online version. In addition, two business alerts – Selling on the Internet: Prompt Delivery Rules and Website Woes: Avoiding Web Service Scams – have been widely disseminated.

(j) Surfs

Just as consumers were discovering the benefits of "surfing" the Internet for instant access to information, FTC staff saw the value of surfing to educate businesses and to investigate potential legal violations. Since December 1996, when the FTC organized its first "surf" to ferret out pyramid schemes, it has become clear that this tool gives new meaning to efficiency. To date, the FTC has led some 20 surfs, with over 250 agencies and consumer protection agencies around the world, identifying some 4,000 commercial websites that make dubious claims, largely in the promotion of health and diet products, pyramid schemes, business opportunities, investments, and credit repair.

Internet surfs allow law enforcement officials to survey the nature and scope of particular violations online. They also offer an opportunity to educate website operators – many of whom are new entrepreneurs unaware of existing laws – instantly and directly. When agency staff surfers identify a site that may have problems, they send an e-mail message that explains why the site may violate the law. Their message also provides a link to the FTC website for more information and gives notice about a follow-up visit. These follow-up surfs reveal that about 20 to 70 percent of the problem sites in a particular area are improved or removed. Those sites that continue their problem practices may be subject to further investigation and enforcement.

(k) Protecting Privacy Online

In May 1998, at the request of the Vice President, the FTC used www.consumer.gov to unveil a 1-stop shop for information about how to protect one's privacy both on and off the Internet. The "About Privacy" site explains consumer privacy rights and provides visitors with contact information to ask that their personal information not be shared with third parties. For example, the page provides information on how to contact credit bureaus, state motor vehicle offices, and marketing organizations via the web, telephone, or mail. It includes sample opt-out letters that consumers can tailor to their own needs, as well as hyper-links to each of the three major credit reporting bureaus and the Direct Marketing Association's opt-out pages.

In addition, the FTC has initiated a major multi-pronged information campaign focused on the provisions of the recent Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506, which requires parental permission before collecting data from those under 13 years old. See Children's Online Privacy Protection Rule, 16 C.F.R. pt. 312 (1999). Businesses are being alerted to their responsibilities, and parents and youngsters are learning about their rights under the law.

2. Department of Commerce Initiatives

U.S. government policymakers and law enforcement officials are working to ensure consumer confidence in the virtual marketplace by enforcing existing legal protections and encouraging private sector leadership. Last spring, the Department of Commerce challenged the private sector to work with consumer representatives to develop effective

consumer protection practices, including developing codes of conduct for business-to-consumer electronic commerce and alternative, easy-to-use mechanisms for consumer dispute resolution, redress, and enforcement. This approach recognizes that as e-commerce expands to encompass more international business-to-consumer transactions, alternative, easy-to-use mechanisms for consumer dispute resolution, redress and enforcement can help to ensure strong and effective consumer protection in the online environment and obviate the need for immediate resolution of the difficult issues surrounding jurisdiction and choice of law that would result if disputes had to be resolved in the courts.

There have been several significant responses to this challenge. In June 1999, the Better Business Bureau's online division, BBBOnline, announced a project to develop a Code of Online Business Practices (see www.bbbonline.org). BBBOnline will work with industry, consumer representatives and government to develop a code to provide online merchants with guidelines to implement important consumer protections, such as disclosure of sale terms, data privacy, dispute resolution mechanisms, and non-deceptive advertising.

A similar effort was initiated in August 1999 with the formation of the Electronic Commerce and Consumer Protection Group, whose members include a number of industry leaders such as America Online, American Express, AT&T, Dell, IBM, Microsoft, Time Warner Inc., and Visa. This group is committed to working with consumer leaders to address electronic commerce confidence issues by formulating concrete approaches to protect consumers and facilitate e-commerce (see www.ecommercegroup.org).

3. FDA's Outreach Campaign

As part of a major public education campaign, the FDA is informing consumers about the potential public health risks of buying medical products on the Internet. To increase awareness, FDA has developed a multimedia education campaign that includes messages targeted to specific audiences and the formation of partnerships for creating and disseminating information through government agencies, national organizations, consumer groups, and the Internet industry. The campaign will include public service announcements, brochures, newspaper articles, media interviews, and an FDA website (www.fda.gov).

FDA's website on buying medical products online provides information on how consumers can protect themselves from certain online practices involving the sale of FDA-regulated products; reports on FDA's enforcement efforts; advice on spotting health care fraud; and answers to frequently asked questions about online drug sales. Consumers who suspect that a website is illegally selling human or animal drugs, medical devices, biological products, foods, dietary supplements, or cosmetics can also complete and submit to FDA an electronic complaint form provided at the site.

4. SEC's Investor Education Efforts

The Securities and Exchange Commission ("SEC") believes that an educated investor is the best defense – and offense – against securities fraud. Investors who know what questions to ask and how to detect fraud will be less likely to fall prey to con-artists, on or off the Internet. And, because they are more likely to report wrongdoing to the SEC and their state securities regulators, educated investors serve as an important early warning system to help regulators fight fraud. In particular, the SEC's Internet mailbox (help@sec.gov) and online complaint form have made it easy and convenient for investors to express concerns and to report complaints to the agency.

The SEC publishes and distributes more than a dozen free brochures that explain in plain English how the securities industry works, how to invest wisely, and what to do if something goes wrong. They include Internet Fraud: How to Avoid Online Investment Scams, which helps investors identify different types of Internet fraud, describes what the

SEC is doing to fight Internet investment scams, and explains how to use the Internet to invest wisely. These and other materials are available on the SEC's website (www.sec.gov/consumer/online.htm).

Because investors increasingly use the Internet to research investment opportunities and to buy and sell securities, the SEC in 1999 launched a revised investor education page on the SEC's website (www.sec.gov/invkhome.htm). The new page features interactive quizzes and calculators, information about online investing, tips for avoiding Internet fraud, and a special section for students and teachers. The page also features the SEC's latest investor alerts, such as Tips for Online Investing: What You Need to Know About Trading in Fast-Moving Markets and Day Trading: Your Dollars at Risk. In addition to individual securities firms, a number of financial services industry associations, educational organizations, consumer groups, media outlets, and publicly traded companies provide links from their websites to the SEC's website.

5. CPSC's Consumer Outreach Efforts

An important part of the mission of the Consumer Product Safety Commission ("CPSC") is to inform and to communicate with the public about consumer product safety issues. Because banned or recalled products can find their way into commerce via the Internet, it is important for consumers to have direct access to safety information. Through its web site (www.cpsc.gov), the CPSC educates the public about critical product safety issues; provides a secure and efficient means by which consumers can report unsafe products; and provides a medium through which manufacturers, importers and distributors of consumer products can report substantial hazards associated with their products.

C. Developing Cybercitizens

Children and young adults are the fastest growing group using the Internet. Helping children draw conclusions about behavior and its consequences in cyberspace is an important part of educating responsible (future) online users. Although most children are taught at an early age that it is wrong to break into a neighbor's house or read their best friend's diaries, we must also emphasize that it is equally wrong, and potentially more damaging, to break into their neighbor's computers and snoop through their computer files. Computer hacking "for fun" is a very serious problem, not only for the targets of the attacks, but also for law enforcement personnel who often have no way to determine the motivation for and the identity of the person behind the intrusion.

Educating children (and adults) about acceptable online behavior is crucial for the Internet to continue to grow as a safe and useful medium. Likewise, there is a need to educate the public on the dangers posed by cybercrimes and how harm can be reduced if people use technology responsibly. As the proliferation of low-cost computers and networks has spread information technology to every corner of society, people of all ages who use this technology must understand that along with the obvious benefits of technology comes a set of corresponding responsibilities. To this end, the Attorney General announced in April 1999 that the Department of Justice had joined with the Information Technology Association of America ("ITAA") for a partnership on a national campaign to educate and raise awareness of computer responsibility and to provide resources to empower concerned citizens.

The Cybercitizen Awareness Program seeks to engage children, young adults, and others on the basics of critical information protection and security and on the limits of acceptable online behavior. The objectives of the program are to give children:

- An understanding of cyberspace benefits and responsibilities;
- An awareness of potential negative consequences resulting from the misuse of the medium;

- An understanding of the personal dangers that exist on the Internet and techniques to avoid being harmed; and
- An ability to commit to adhere to these principles as they mature.

Thus far, the campaign has received \$300,000 in grants from the Department of Justice's Office of Justice Programs. The partnership awarded a contract to a public relations firm in December 1999 to implement the objectives of the campaign. The Department of Justice and ITAA believe that the program will play a significant role in deterring potential hacking, educating the public about the potential dangers of the Internet, raising awareness about the potential consequences of online activities, reducing the threat to the nation's critical infrastructure, increasing online security in the United States, and providing savings to information technology resources owners and users who suffer economic losses as a result of computer crimes.

In addition to the awareness program detailed above, the Cybercitizen Partnership also has initiated a personnel exchange program between private business and federal agencies that is designed to educate both groups about how the other responds to threats and crimes over the Internet. This initiative will allow companies to find out how best to help law-enforcement agencies, and government officials will learn what business interests and influences drive industry decisions. The exchange program will be coordinated by the ITAA, which intends to detail personnel from the private sector to the FBI's National Infrastructure Protection Center. The partnership also expects to create a directory of computer experts and computer security resources so that law enforcement will know where to turn when they need assistance from industry.

V. CONCLUSIONS AND RECOMMENDATIONS

Ensuring the safety and security of those who use the Internet is a critical element of the Administration's overall policy regarding the Internet and electronic commerce, a policy that seeks to promote private sector leadership, technology-neutral laws and regulation, and an appreciation of the Internet as an important medium for commerce and communication both domestically and internationally

Consistent with the Administration's overall policy, the Working Group recommends a 3-part approach for addressing unlawful conduct on the Internet:

- First, any regulation of unlawful conduct involving the use of the Internet should be analyzed through a policy framework that ensures that online conduct is treated in a manner consistent with the way offline conduct is treated, in a technology-neutral manner, and in a manner that accounts for other important societal interests such as privacy and protection of civil liberties;
- Second, law enforcement needs and challenges posed by the Internet should be recognized as significant, particularly in the areas of resources, training, and the need for new investigative tools and capabilities, coordination with and among federal, state, and local law enforcement agencies, and coordination with and among our international counterparts; and
- Third, there should be continued support for private sector leadership and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users to prevent and minimize the risks of unlawful activity.

The challenges to the federal government of unlawful conduct involving the use of the

Internet are many. On one hand, the Internet offers unparalleled opportunities for socially beneficial endeavors. At the same time, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, and the unlawful distribution of computer software or other creative material protected by intellectual property rights.

In its analysis of existing federal laws, the Working Group finds that existing substantive federal laws generally do not distinguish between unlawful conduct committed through the use of the Internet and the same conduct committed through the use of other, more traditional means of communication. To the extent these existing laws adequately address unlawful conduct in the offline world, they should, for the most part, adequately cover unlawful conduct on the Internet. There may be a few instances, however, where relevant federal laws need to be amended to better reflect the realities of new technologies, such as the Internet.

Despite the general adequacy of laws that define the substance of criminal and other offenses, however, the Working Group finds that the Internet presents new and significant investigatory challenges for law enforcement at all levels. These challenges include the need for real-time tracing of Internet communications across traditional jurisdictional boundaries, both domestically and internationally; the need to track down sophisticated users who commit unlawful acts on the Internet while hiding their identities; the need for hand-in-glove coordination among various law enforcement agencies; and the need for trained and well-equipped personnel – at federal, state, local, and international levels – to gather evidence, investigate, and prosecute these cases. In some instances, federal procedural and evidentiary laws may need to be amended to better enable law enforcement to meet these challenges.

Indeed, the Working Group concludes that the federal government must continue to devote further attention to these important challenges. The report contains specific suggestions on areas on which additional resources and further evaluation are needed. These recommendations recognize that there are no easy answers to the challenges posed by unlawful conduct on the Internet. At the very least, however, significant attention should be given to the issues, and open dialogue and partnerships among law enforcement agencies, industry, and the public must continue.

In light of its mandate, the Working Group confined its analysis to existing federal laws. A logical next step would be an expanded analysis of state (and, to the extent relevant, local) laws that focuses on whether those laws are adequate to investigate and prosecute unlawful conduct on the Internet. Because coordination and cooperation among federal, state, and local law enforcement agencies are key to our efforts to prevent, deter, investigate, and prosecute such unlawful conduct, such an analysis would provide states and others with a blueprint for translating the conclusions in this report into a more comprehensive approach to meeting the substantial challenges presented.

Finally, an essential component of the Working Group's strategy is continued support for private sector leadership, industry self-regulation, and the development of methods – such as "cyberethics" curricula, appropriate technological tools, and media and other outreach efforts – that educate and empower Internet users so as to prevent and minimize the risks of unlawful activity. This Administration has already initiated numerous efforts to educate consumers, parents, teachers, and children about ways to ensure safe and enjoyable Internet experiences, and those efforts should continue. The private sector has also undertaken substantial self-regulatory efforts – such as voluntary codes of conduct and appropriate cooperation with law enforcement – that show responsible leadership in preventing and minimizing the risks of unlawful conduct on the Internet. Those efforts must also continue to grow. Working together, we can ensure that the Internet and its benefits will continue to

grow and flourish in the years and decades to come.

- **Appendices to "The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet (March 9, 2000)"**
- **More Information on: Prosecuting Crimes Facilitated by Computers and by the Internet**
- **More information on: Electronic Commerce**

Go to . . . [CCIPS Home Page](#) || [Justice Department Home Page](#)

Last updated March 9, 2000
usdoj-crm/mis/mdf

CLINTON-GORE ADMINISTRATION UNVEILS NEW INITIATIVE TO PROTECT CUSTOMERS BUYING PRESCRIPTION DRUG PRODUCTS OVER THE INTERNET

December 28, 1999

Today, the White House announced that the President will include a new initiative to prevent the illegal sale of pharmaceuticals over the Internet in his fiscal year 2001 budget that would: establish new Federal requirements for all Internet pharmacy sites to ensure that they comply with state and Federal laws; create new civil money penalties for the illegal sale of pharmaceuticals; give Federal agencies new administrative authority to swiftly gather the information necessary to build a case against offenders; and launch a new public education campaign about the potential dangers of buying pharmaceutical products on the Internet. The President's FY 2001 budget will include \$10 million to fund these and other activities.

UNSUSPECTING CONSUMERS MAY FALL PREY TO FLY-BY-NIGHT INTERNET COMPANIES SELLING UNSAFE PRESCRIPTION DRUG PRODUCTS. The number of people who use the Internet for the purchase of medical products is growing rapidly, and many consumers, including those in rural areas or those who cannot leave their homes, benefit from the convenience and privacy of this new option. However, the safe use of the Internet by both consumers and businesses is being threatened by fraudulent or disreputable Internet sites that sell products illegally.

- **Internet pharmacies can bypass traditional safeguards against the use of unsafe or inappropriate drugs.** Traditionally, there are several safeguards to protect consumers against unsafe use of drugs, including the issuance of new prescriptions only after performing a physical exam and meeting state and Federal requirements to ensure that pharmacies only dispense drugs with a valid prescription. However, the Internet makes it easy to bypass these safeguards. Unethical doctors can illegally prescribe pills on-line to consumers they have never met in states where they are not authorized to work. Unscrupulous, unlicensed pharmacies can ship pills across state lines. Policing against this type of conduct is difficult because website ownership is difficult to track.
- **Fly-by-night Internet pharmacies put on-line consumers at increased risk.** Consumers who buy prescription drugs on-line from illegitimate websites are at risk for adverse effects from inappropriately prescribed medications, dangerous drug interactions, or contaminated drugs. Some on-line pharmacies are not employing licensed pharmacists, removing an important safety check for consumers. In addition, because patients can easily provide false information to obtain medications, the potential for serious abuse exists. Unlike traditional pharmacies, consumers cannot physically observe the operations behind an on-line pharmacy, and have no way to determine whether the entity is legitimate.
- **Federal authority to prosecute offenders is limited.** Because of some limitations on Federal authority, it has been difficult for FDA to take action against an on-line corporation employing licensed physicians who prescribe drugs without taking the consumer's medical history or checking for potential drug interactions or on-line corporations dispensing drugs in bulk to individuals claiming to be pharmacies in order to receive drugs without a prescription.

- **Penalties for the violation of current Federal authority are inadequate.** FDA has the authority to take action against any entity who sells a prescription drug to an individual without a valid prescription, unapproved new drugs, counterfeit drugs, expired or illegally diverted pharmaceuticals, and the marketing of products based on fraudulent health claims. However, the penalty for these actions in most cases is limited, even if they result in harm to patients, and may not be adequate to deter these fly-by-night operations.

CLINTON-GORE ADMINISTRATION TAKES NEW STEPS TO PROTECT CUSTOMERS BUYING PHARMACEUTICALS ON-LINE. Today, the Clinton-Gore Administration will unveil a new legislative proposal that:

- **Establishes new Federal requirements for Internet pharmacy sites.** This proposal would establish a new Federal requirement to enable consumers to identify legitimate internet pharmacy sites. Sites would have to demonstrate to the FDA their compliance with Federal and state law on pharmaceutical sales before they received approval to operate. Sites operating without previously demonstrating their compliance to FDA would be subject to sanction. This system would allow for rapid, coordinated Federal-state investigations and prosecutions without disturbing state systems regulating the practice of medicine and pharmacy.
- **Strengthens the current penalty structure for illegal pharmaceutical sales over the Internet.** This proposal would create new civil money penalties of \$500,000 per violation for the sale of prescription drug to an individual without a valid prescription.
- **Provides new authority to FDA in order to ensure rapid and effective investigation of on-line sites.** In order to streamline the investigative process, this proposal would provide FDA with administrative subpoena authority when investigating potentially illegal Internet drug sales. The issuance of administrative subpoenas would be conducted in accordance with the standards established by the Administration's draft privacy regulations.

In addition, the White House will:

- **Announce a new, \$10 million investment to target and punish those who engage in illegal prescription drug sales over the Internet.** The FY 2001 budget will invest \$10 million to develop a rapid response team of personnel dedicated to this initiative and upgrade FDA's computer technology to identify, investigate, and prosecute websites selling prescription drugs to individuals without a valid prescription, unapproved new drugs, counterfeit drugs, expired or illegally diverted pharmaceuticals, and the marketing of products based on fraudulent health claims.
- **Announce plans to launch a new public education campaign to inform the public about the potential dangers of buying pharmaceutical products on the Internet.** FDA will launch a new, public education campaign to inform the public about safe ways to purchase pharmaceutical products over the Internet, including: placing advertisements on health related websites; providing public service announcements for distribution to radio and television stations nationwide; and the development of a 'safety checklist' to be posted on-line and distributed through health care provider and consumer advocacy organizations.

From: Robert J. Pellicci on 03/08/2000 04:02:33 PM

Record Type: Record

To: Deborah R. Adler/OPD/EOP@EOP

cc:

Subject: LRM RJP238 - - HEALTH & HUMAN SERVICES Draft Bill on Internet Prescription Drug Sales Act of 2000

Comments from Dan Chenok--

----- Forwarded by Robert J. Pellicci/OMB/EOP on 03/08/2000 04:04 PM -----



Daniel J. Chenok
03/08/2000 03:44:42 PM

Record Type: Record

To: Robert J. Pellicci/OMB/EOP@EOP

cc: Wendy A. Taylor/OMB/EOP@EOP, Peter P. Swire/OMB/EOP@EOP, Matthew Vaeth/OMB/EOP@EOP,
Lewis W. Oleinick/OMB/EOP@EOP

Subject: LRM RJP238 - - HEALTH & HUMAN SERVICES Draft Bill on Internet Prescription Drug Sales Act of 2000

I endorse Wendy's comments and add additional comments on **bold** below.

----- Forwarded by Daniel J. Chenok/OMB/EOP on 03/08/2000 03:25 PM -----

Wendy A. Taylor 02/28/2000 05:58:14 PM

Record Type: Record

To: Sally Katzen/OMB/EOP@EOP, Daniel J. Chenok/OMB/EOP@EOP, Peter P. Swire/OMB/EOP@EOP

cc: Matthew Vaeth/OMB/EOP@EOP, Robert J. Pellicci/OMB/EOP@EOP

Subject: LRM RJP238 - - HEALTH & HUMAN SERVICES Draft Bill on Internet Prescription Drug Sales Act of 2000

I continue to have concerns with the HHS approach on internet prescription drug sales. Several of the major issues that we raised in previous meetings remain in the bill. The following outlines my concerns. I will be out of the office in training for the rest of the week. If you need to reach me, you can leave a message for me at the Inn at Perry Cabin (410) 745-2200.

1. Determination of Compliance [503B (b)(1)] : While HHS has eliminated the word "certify" from the bill, each online pharmacy must demonstrate to the Secretary's satisfaction that it complies and will continue to comply with the applicable requirements. This "determination of compliance" must be displayed on the homepage of the website in such form that the Secretary requires (e.g. a seal, symbol, or other evidence specified by the Secretary).

- Under this bill, it appears the Secretary must conduct a "determination of compliance" for *each* online pharmacy. I see very little difference between this and a certification to which we have strongly objected. (The bill authorizes the Secretary to designate a private nonprofit organization or State to

examine and inspect the records and facilities of online pharmacies seeking a determination. While this is a marginal improvement, the underlying issue still remains.)

- In addition, I assume that this requirement would also apply to pharmacies that operate only within one State -- not just interstate (otherwise consumers would have difficulty distinguishing between these legitimate intrastate pharmacies and the non-legitimate online pharmacies since neither would get a "seal"). This gets HHS involved with State-only issues.

2. Website Disclosure Information [503B (b)(5)]: HHS requires the online pharmacy to disclose basic information on its website including: the name of the online pharmacy in each State in which it is licensed; the street address; the name, degree, and licensure of the pharmacist in charge; a phone number to reach a licensed pharmacist; a list of States in which the online pharmacy is licensed to dispense prescription drugs and the applicable license numbers; and a declaration that the online pharmacy will dispense prescription drugs only upon a valid prescription.

- While FDA has previously argued that some kind of easily recognizable symbol is necessary to help consumers distinguish between good and bad sites, I believe that the basic disclosure information is sufficient.
- I'm also not convinced that the extra step of requiring an individual determination of compliance would deter the bad actors. If the information were misrepresented, the Feds or States could take action. A site misrepresenting this information would be subject to penalties under the Act. HHS could catch the sites through compliance checks.
- I recommend that the determination of compliance section be deleted.

Agree. The disclosure requirement should be sufficient, along with penalties for violation. FDA does not enforce compliance of off-line pharmacies. FDA should work with the States to develop enforcement schemes that treat on-line and off-line as consistently as possible.

Also, I would question (b)(5)(F) on the grounds that , as we heard in a meeting, mail order pharmacies do not always have to be licensed in the states to which they sell -- but if this is incorrect I am ok with (F)

3. Valid Prescription [503B (b) (4)(B)]: The bill requires that the each prescription drug dispenses to an individual be based on a prescription (A) that is valid under the laws of the State in which the individual is located **AND** (B) based on a practitioner-patient relationship that involves more than use of an online questionnaire or similar document.

- I have significant concerns with subpart (B) of this provision. This moves FDA well into the business of regulating the practice of medicine -- a role traditionally left to the States. I see this as a big political landmine which will raise widespread concerns from a host of medical groups (doctors, pharmacists) who may see this as a slippery slope for FDA. I strongly recommend that this provision be removed. **I strongly agree. This is clearly an area where such regulation would create a highly asymmetric relationship between on-line and off-line regulation. The State determines what constitutes a dr-patient relationship.**

4. Effective Period of HHS Determination [503B (c)(1)]: The bill specifies that a determination of compliance made by the Secretary would only be effective for a period of two years.

- Not only does the Secretary have to issue a determination of compliance for each online pharmacy, but the pharmacies will have to be re-reviewed every two years. See concerns raised in items 1 and 2 above.

Agree. What is the standard relicensing period for traditional pharmacies?

5. Fees 503B (d): The Secretary is authorized to assess fees for determinations of compliance in

amounts sufficient to cover the costs of such determinations (including costs of periodic inspections).

- Do brick and mortar pharmacies face similar licensing fees from the States? If not, doesn't this raise concerns that online pharmacies are treated differently than their brick and mortar counterparts?

Agree.

6. Subpoenas (f): What is the current authority for subpoenas for off-line pharmacies? Would this introduce a new, easier subpoena that could set a precedent for enforcement of other on-line commerce? (same question on State AG ability to bring suit, (h)).

7. Definition of interstate commerce (i): This bill defines the internet as always involving interstate commerce. Does such a definition break new ground that could set a precedent elsewhere?

Comments on Draft Internet Prescription Drug Bill

1. I assume “consumer” means a person located in the United States of America. We should say that in the statute because it sets an important precedent about how other governments should focus their regulatory efforts (and avoids multiple, overlapping rules)./

2. The proposal seems quite government-centric, with self-regulation relegated to subsection (e). That seems different from the way the proposal was framed initially. Is this really the message we want to convey?

3. I am very troubled by the knee-jerk acceptance of state-by-state regulation (in (b)(2) especially but also in (b)(3)). What about mutual recognition and reciprocity? Our barriers to e-commerce process seeks to identify requirements just like this one and devise ways to address it, but here we are automatically applying licensing requirements that will be especially burdensome to small entities (pharmacies just across state lines, for example) competing for a wider market using the Internet. We are setting a terrible precedent, both domestically for other licensing situations and internationally. I hope there will be an opportunity to discuss this issue.

Additional Department of Commerce Comments on HHS Draft Bill re: Online Pharmacies
(Not yet cleared by all DOC policy officials)

In general: We recommend that additional interagency discussions take place before this bill is cleared in order to: (1) make the legislation more technology-neutral (that is, to limit the degree to which it sets up differing rules for online drug sales and sales by other media or means.); (2) adopt a less regulatory approach; and (3) discuss and correct numerous apparent technical deficiencies.

First commenter:

This legislation appears diametrically opposite the "light touch" approach that FDA has said in testimony that it would adopt toward this issue. It also sets up a fight with Chairman Bliley, who has clearly indicated (see letter of January) that he won't accept a heavily regulatory approach. Specific issues: (All references are to the "503B" amendment)

* (a)(1) definitions. The definition of "Internet" raises several points. First, nothing in the FDA justification identifies why existing authorities (e.g., direct mail subscriptions, etc.) cannot either be applied affectively or -- more importantly -- modified in a minimal, predictable way to achieve this goal. Instead, the bill develops a new framework. Second, even CDA didn't define internet. This puts the Administration in an awkward position vis-a-vis no regulation specifically related to the Internet as a medium. Third, TCP/IP may disappear in a few years. Note that this definition would apply to a Hospital intranet..... Finally, term any successor protocol used to communicate information of all kinds by wire or radio" is incredibly broad. BTW, TCP/IP is NOT used to communicate information of "all kinds" by "radio".

* (a)(2). Licensure. By saying that each OLP (Online Pharmacy) "must be licensed" ... "in each State" to which it "offers", this seems to indicate that the drafters have never read Zippo.... This effectively means that any OLP must be licensed in each and every state which requires licensing... To make the obvious point, this phrasing raises serious questions in light of our domestic and international discussions on jurisdiction.

* (b) generally. This section puts the HHS Secretary in the middle of determining adequacy of meeting existing state laws and regulations, including all those to which the OLP "delivers or offers". What happens if the Secretary and the state authority don't see eye-to-eye...

* (b)(5). Website disclosure. It is not clear where these specific are drawn from. What happens if they conflict with state requirements -- all the states where the OLP "delivers or offers". What is the alternative? This is hard. The FDA currently has jurisdiction -- as I understand it -- for mail order pharmacies. The states have jurisdiction for brick-and-mortar.

Second set of DOC comments: (JOINT ITA and OGC staff):

We are concerned about establishing an Internet-specific regulatory regime. It would appear that all the concerns about sale of prescription drugs over the would also apply, for example, to mail order or telemarketing.

It also seems we should be cautious about having HHS act as a licensing authority in an area where the states have traditionally regulated. What does the HHS determination of compliance add when online pharmacies have to be licensed in every state in which they operate or deliver prescription drugs?

Also, the bill generally places different and more stringent requirements in the on-line world than are required by law for off-line commerce. For example, the fact that a person shows up at CVS with a handwritten prescription does NOTHING to "ensure" a valid doctor-patient relationship.

Federal Trade Commission - comments to OMB March 2000

This is a generally solid proposal that will make it much easier for State and Federal law enforcement agencies to crack down on unlicensed rogue Web sites peddling prescription medications without a valid prescription and for consumers to obtain critical information about an online pharmacy. The disclosure requirements and the provision providing for expanded state law enforcement authority are consistent with the recommendations the Commission made to Congress in July. See Prepared Statement of the Federal Trade Commission on "Drugstores on the Net: The Benefits and Risks of Online Pharmacies," before the Subcommittee on Oversight and Investigations of the Committee on Commerce, July 30, 1999.

The certification requirement (section 503B(b)(1)), however, appears to be a federal licensing requirement and may be viewed as an encroachment on the state's traditional role of licensing and regulating pharmacies. The other requirements for online pharmacies contained in section 503B(b) could be retained without a certification program. Moreover, the effective date could be shortened if the certification requirement is dropped or modified.

Section 503B(b)(4) of the proposed legislation establishes an online pharmacy's obligation to ensure that a prescription is valid and not based primarily on an online questionnaire before dispensing a prescription drug to an "individual." The use of the term "individual" in this section in lieu of the term "consumer," which is defined in section 503B(a)(4), could be confusing because it implies that the two terms have different meanings. In fact, other than in section 503B(c)(2), the term "consumer" does not appear in the substantive provisions of the legislation. Section 503B(c)(2) declares that it is unlawful for an online pharmacy to deliver or sell a prescription drug to a "consumer" if the Secretary withdraws the pharmacy's certification. For consistency purposes, sections 503B(b)(4) and 503B(c)(2) should use the same term, either consumer or individual.

The \$500,000 civil penalty will strike some as excessive. An alternative approach would be to use a smaller, but still substantial, penalty and clarify that each sale may constitute a separate violation.

LRM ID RJP238

**VA Comments on Draft Bill on Internet Prescription Drug
Sales Act of 2000**

The proposed bill would subject "on line pharmacies" to state licensure and regulation. An on line pharmacy would have to be licensed in every State in which it operates and to which it delivers or offers to deliver prescription drugs. Applying this proposed bill to VA would require the Department to be licensed in all 50 states and subject to regulation by each as we refill prescriptions on line. VA pharmacies are not now subject to state licensure or regulation, and the draft bill would not change that. That is because the definition of a "person" under the Food Drug and Cosmetic Act, which this bill would amend, does not include Federal agencies. 21 U.S.C. § 321(e). However, in order to avoid any confusion on the part of Federal officials responsible for pharmacy operations, or on the part of state entities charged with pharmacy oversight, the proposed bill should be revised to specifically exclude Federal entities from its coverage.



Daniel J. Chenok
03/08/2000 03:44:42 PM

Record Type: Record

To: Robert J. Pellicci/OMB/EOP@EOP
cc: Wendy A. Taylor/OMB/EOP@EOP, Peter P. Swire/OMB/EOP@EOP, Matthew Vaeth/OMB/EOP@EOP, Lewis W. Oleinick/OMB/EOP@EOP
Subject: LRM RJP238 - - HEALTH & HUMAN SERVICES Draft Bill on Internet Prescription Drug Sales Act of 2000

I endorse Wendy's comments and add additional comments on **bold** below.

----- Forwarded by Daniel J. Chenok/OMB/EOP on 03/08/2000 03:25 PM -----

Wendy A. Taylor 02/28/2000 05:58:14 PM

Record Type: Record

To: Sally Katzen/OMB/EOP@EOP, Daniel J. Chenok/OMB/EOP@EOP, Peter P. Swire/OMB/EOP@EOP
cc: Matthew Vaeth/OMB/EOP@EOP, Robert J. Pellicci/OMB/EOP@EOP
Subject: LRM RJP238 - - HEALTH & HUMAN SERVICES Draft Bill on Internet Prescription Drug Sales Act of 2000

I continue to have concerns with the HHS approach on internet prescription drug sales. Several of the major issues that we raised in previous meetings remain in the bill. The following outlines my concerns. I will be out of the office in training for the rest of the week. If you need to reach me, you can leave a message for me at the Inn at Perry Cabin (410) 745-2200.

1. Determination of Compliance [503B (b)(1)] : While HHS has eliminated the word "certify" from the bill, each online pharmacy must demonstrate to the Secretary's satisfaction that it complies and will continue to comply with the applicable requirements. This "determination of compliance" must be displayed on the homepage of the website in such form that the Secretary requires (e.g. a seal, symbol, or other evidence specified by the Secretary).

- Under this bill, it appears the Secretary must conduct a "determination of compliance" for *each* online pharmacy. I see very little difference between this and a certification to which we have strongly objected. (The bill authorizes the Secretary to designate a private nonprofit organization or State to examine and inspect the records and facilities of online pharmacies seeking a determination. While this is a marginal improvement, the underlying issue still remains.)
- In addition, I assume that this requirement would also apply to pharmacies that operate only within one State -- not just interstate (otherwise consumers would have difficulty distinguishing between these legitimate intrastate pharmacies and the non-legitimate online pharmacies since neither would get a "seal"). This gets HHS involved with State-only issues.

2. Website Disclosure Information [503B (b)(5)]: HHS requires the online pharmacy to disclose basic information on its website including: the name of the online pharmacy in each State in which it is licensed; the street address; the name, degree, and licensure of the pharmacist in charge; a phone number to reach a licensed pharmacist; a list of States in which the online pharmacy is licensed to dispense prescription drugs and the applicable license numbers; and a declaration that the online pharmacy will dispense

prescription drugs only upon a valid prescription.

- While FDA has previously argued that some kind of easily recognizable symbol is necessary to help consumers distinguish between good and bad sites, I believe that the basic disclosure information is sufficient.
- I'm also not convinced that the extra step of requiring an individual determination of compliance would deter the bad actors. If the information were misrepresented, the Feds or States could take action. A site misrepresenting this information would be subject to penalties under the Act. HHS could catch the sites through compliance checks.
- I recommend that the determination of compliance section be deleted.

Agree. The disclosure requirement should be sufficient, along with penalties for violation. FDA does not enforce compliance of off-line pharmacies. FDA should work with the States to develop enforcement schemes that treat on-line and off-line as consistently as possible.

Also, I would question (b)(5)(F) on the grounds that , as we heard in a meeting, mail order pharmacies do not always have to be licensed in the states to which they sell -- but if this is incorrect I am ok with (F)

3. Valid Prescription [503B (b) (4)(B)]: The bill requires that the each prescription drug dispenses to an individual be based on a prescription (A) that is valid under the laws of the State in which the individual is located **AND** (B) based on a practitioner-patient relationship that involves more than use of an online questionnaire or similar document.

- I have significant concerns with subpart (B) of this provision. This moves FDA well into the business of regulating the practice of medicine -- a role traditionally left to the States. I see this as a big political landmine which will raise widespread concerns from a host of medical groups (doctors, pharmacists) who may see this as a slippery slope for FDA. I strongly recommend that this provision be removed. I strongly agree. This is clearly an area where such regulation would create a highly asymmetric relationship between on-line and off-line regulation. The State determines what constitutes a dr-patient relationship.

4. Effective Period of HHS Determination [503B (c)(1)]: The bill specifies that a determination of compliance made by the Secretary would only be effective for a period of two years.

- Not only does the Secretary have to issue a determination of compliance for each online pharmacy, but the pharmacies will have to be re-reviewed every two years. See concerns raised in items 1 and 2 above.

Agree. What is the standard relicensing period for traditional pharmacies?

5. Fees 503B (d): The Secretary is authorized to assess fees for determinations of compliance in amounts sufficient to cover the costs of such determinations (including costs of periodic inspections).

- Do brick and mortar pharmacies face similar licensing fees from the States? If not, doesn't this raise concerns that online pharmacies are treated differently than their brick and mortar counterparts?

Agree.

6. Subpoenas (f): **What is the current authority for subpoenas for off-line pharmacies? Would this introduce a new, easier subpoena that could set a precedent for enforcement of other on-line commerce? (same question on State AG ability to bring suit, (h)).**

7. Definition of interstate commerce (i): **This bill defines the internet as always involving**

interstate commerce. Does such a definition break new ground that could set a precedent elsewhere?

FEB-25-2000 11:30 TO:92 - OPM

FROM:RODGERS M

P. 2/14

LRM ID: RJP238
Drug Sales Act of 2000

SUBJECT: HEALTH & HUMAN SERVICES Draft Bill on Internet Prescription

**RESPONSE TO
LEGISLATIVE REFERRAL
MEMORANDUM**

If your response to this request for views is short (e.g., concur/no comment), we prefer that you respond by e-mail or by faxing us this response sheet. If the response is short and you prefer to call, please call the branch-wide line shown below (NOT the analyst's line) to leave a message with a legislative assistant.

You may also respond by:

(1) calling the analyst/attorney's direct line (you will be connected to voice mail if the analyst does not answer); or

(2) sending us a memo or letter

Please include the LRM number shown above, and the subject shown below.

TO: Robert J. Pellicci Phone: 395-4871 Fax: 395-6148
Office of Management and Budget
Branch-Wide Line (to reach legislative assistant): 395-7362

FROM: 2/25/00 (Date)
DON JANSEN (Name)
OPM (Agency)
606-1424 (Telephone)

The following is the response of our agency to your request for views on the above-captioned subject:

☐ Concur☐ No Objection☒ No Comment☐ See proposed edits on pages _____☐ Other: _____☐ FAX RETURN of _____ pages, attached to this response sheet