Chapter III: The International Impact of Domestic U.S. Restrictions on the Availability of Data

A. *Limitations on the Export of Data*

As noted in Chapters I and II, U.S. regulatory agencies increasingly have deregulated both domestic and international facilities for data transmission. The conduits of communication thus are less restricted than ever before. Clearing the international channels, however, does not per se assure a free flow of information. Like other countries, the United States has many restrictions upon the availability of certain types of information – for reasons ranging from personal privacy to national security. Indeed, the trend towards both domestic and international deregulation makes these restrictions particularly significant. With the removal of substantial impediments to international transmissions, domestic restrictions on the availability of data may become the most significant burden on the free flow of information from the United States side.

Chapter Three thus gives a sampling of the major domestic U.S. restrictions on the availability of data – whether for domestic or international transmission. As noted in the Introduction, no overall scheme exists for this patchwork of laws. Nevertheless, an overview is useful.

In general, the U.S. regulatory regime does not impose restrictions upon the import or export of data and data processing or similar services. There are numerous restrictions, however, on the domestic use and transmission of security-related information. These regulations naturally affect international telecommunications.

Both cooperatively with several Western-bloc nations and on its own, the United States restricts the transfer of technology and technological information to hostile or non-aligned nations. This section briefly reviews the domestic and multilateral regulatory schemes for controlling the export of sensitive data. Current U.S. export controls fall into three categories:

- *Nuclear information* is regulated by the Nuclear Regulatory Commission (NRC) and the Department of Energy (DOE) under the Atomic Energy Act of 1954, as amended by the Nuclear Non-Proliferation Act of 1978;

- *Munitions and related information* is controlled by the State Department, under the Arms Export Control Act of 1976; and
- *»Dual use« information and technology* (e.g., information with both military and civilian applications) is regulated by the Commerce Department under the Export Administration Act of 1979.

1. *Atomic Energy Information*

The Atomic Energy Act imposes criminal sanctions for divulging »restricted data« to unauthorized recipients.[180] Restricted data is:

> all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category.[181]

A quirk in this law is that data remains restricted until declassified – even if it already is in the public domain. This led to the celebrated *Progressive* case,[182] in which a federal district court enjoined publication of a magazine article explaining how to build a hydrogen bomb. This appears to be the only case in U.S. history in which a lower court imposed a prior restraint on a print medium.

2. *Munitions Information*

Under the Arms Export Control Act, the State Department maintains a »Munitions List« and licenses the import as well as export of any items on the list.[183] The State Department's International Trade in Arms Regulations (ITAR) restrict the disclosure of technical data pertaining to weapons, including »any unclassified information that can be used or adapted for use in the design, production, operation, maintenance or reconstruction« of items on the Munitions List.[184] The ITAR also prohibit the export of technology or information that »advances the state-of-the-art or estab-

180 42 U.S.C. §§ 2011–2296 (1982).
181 *Id.* § 2014(y).
182 United States v. The Progressive, 467 F. Supp. 990 (D. Wisc. 1979).
183 22 U.S.C. § 2751 (1982).
184 22 C.F.R. § 125.01 (1986).

lishes a new art in an area of significant military applicability in the United States« without State Department authorization.[185]

3. *»Dual Use« Technology and Technical Information*

Under the Export Administration Act (EAA),[186] the Commerce Department controls the export of commodities, technologies and data on industrial processes that affect national security, foreign policy or limited domestic resources. Technical information about industrial processes is defined in the Department's Export Administration Regulations (EAR) as »information of any kind that can be used or adapted for use in the design, production, manufacture, utilization, or reconstruction of articles or materials.« This information is placed on a Commodities Control list – an approach similar in concept to the State Department's Munitions List.[187] The EAR define »export« not only as the transmission of technical data outside of the United States but also as the verbal or written release of such data to foreign nationals within the United States. Unlike nuclear-information restrictions, however, the EAR exempt public-domain information from export restrictions.[188] The reasoning of the *Progressive* case thus presumably would not justify a prohibition on the publication of such data.

Items on the Commodity Control List and information related to these items may be exported only with a license from the Commerce Department. »Validated licenses« are required for some exports, depending upon both the nature and the destination point of an item. »General licenses« cover exports not requireing a validated license.[189]

Both the ITAR and EAR definitions of technical data are broad enough to require export licenses for a wide range of information. These regulations require information providers to determine whether their information includes »technical data« and whether the information will be available to aliens. If so, an information provider must obtain a license from either the Commerce or the State Department prior to disclosure. (Exemptions for material in the public domain sometimes are applicable, as noted above.) The State Department may deny, revoke, suspend or amend licenses

185 *Id.* § 379.3
186 50 U.S.C. § 2401 (1982).
187 15 C.F.R. § 379.1 (1986).
188 *Id.* § 379.3.
189 50 U.S.C. § 2404(e)(2), (3) (1982).

without notice if it determines that such action is necessary in the interests of world peace, national security or U.S. foreign policy.[190] Similar provisions apply to the Commerce Department.[191]

4. *Multilateral Export Controls*

In 1950 the United States, Canada, the United Kingdom, France, West Germany, Italy and Japan created a multilateral consulting organization to coordinate export controls for mutual security – the Coordinating Committee (COCOM). This agency controls 150 items for export to the U.S.S.R., other Warsaw Pact nations, Albania, North Korea, Mongolia, Vietnam and the People's Republic of China. COCOM reviews this list approximately every three to four years. All member-nations must concur in additions to or deletions from the list. Exceptions may be obtained – and the United States has received more than any other nation – upon the approval of member-nations.[192]

B. *Privacy*

The United States has been active in protecting personal privacy against *governmental* intrusion. A number of laws prohibit the collection of personally identifiable data by both public and private entities in a comparatively narrow set of circumstances. A melange of federal, state and local statutes protects personal data on a piecemeal basis. In most cases, federal or state legislatures have acted upon highly particularized fears – e.g., governmental data processing for administration of welfare payments or use of interactive cable television for audience research.

Although these restrictions mainly inhibit domestic activities, they also might impact on a variety of international transactions. For example, credit

190 22 C.F.R. § 123.05(a)(1–3) (1986).

191 15 C.F.R. § 370.3(b) (1986).

192 *See, e.g.*, Maly, *Technology Transfer Controls*, 23 JURIMETRICS JOURNAL 33 (1982). Flow of information between signatory nations is also regulated by the Agreement for Facilitating the International Circulation of Visual and Auditory Materials of an Educational, Scientific and Cultural Character, 17 U.S.T. 1578, T.I.A.S. No. 6116 (1967). This Agreement curtails import duties, licenses and special taxes through the issuance of exemption certificates. For a detailed discussion, compare Barnett, *Part II: Mass Media, infra* at 232–35.

ratings on U.S. investors might not be available for overseas entities because of federal or state laws to protect personal privacy.

1. *Restrictions on the U.S. Government*

The Privacy Act of 1974 regulates the collection, maintenance, use and dissemination of information by federal agencies.[193] The Act defines a »record« as any piece, collection or grouping of information about an individual that is maintained by a federal agency. This includes data on an individual's education, medical history, financial transactions, criminal activities or employment history, if it contains his or her name, identifying number, symbol or other identification.[194]

Under the Act, no agency may disclose any record to another person or agency except pursuant to a written request by – or with the prior written consent of – the individual affected, unless the record falls within one of several exemptions. For example, exceptions exist if disclosure of a record would be pertinent to a civil or criminal law enforcement activity, which is authorized by law and carried out by any properly authorized U.S. law enforcement agency or pursuant to an appropriate court order.[195]

If an agency maintains records, an individual may gain access to any information about him or her. The agency must: (1) permit the individual to review the record and have a copy made; (2) allow the individual to request the agency to amend any such record; and (3) upon refusal to amend a record, grant an administrative review of such refusal within thirty days.[196] A final agency decision is reviewable, of course, in the federal courts.

An agency also may keep only such information about an individual as is relevant and necessary to accomplish the agency's goals. It must, to the extent possible, collect data from a person directly, if the information might result in adverse determinations about an individual's rights, benefits and privileges under federal programs.[197]

The Act does not create a central administrative or enforcement agency. The executive Office of Management and Budget, however, oversees agencies' compliance with the Act's procedural guidelines.[198]

193 5 U.S.C. § 552 *et seq.* (1982).
194 *Id.* § 552a(a)(4).
195 *Id.* § 552a(b).
196 *Id.* § 552a(d)(1), (2), (3).
197 *Id.* § 552a(e).
198 *Id.* § 552a(g), (i).

2. *Governmental Interception of Wire and Oral Communications*

The Omnibus Crime Control Act regulates the government's interception of »wire« and »oral communication.«[199] These terms have specific statutory definitions. A »wire communication« is any message conveyed wholly or partially through a wire, cable or like connection operated by a common carrier. An »oral communication« is any communication by a person who reasonably expects that his or her conversation is private and not subject to interception by third parties. An »interception« occurs when a communication is achieved through the use of mechanical, electrical or other devices.[200]

A party to a communication may intercept the communication without violating the Act, however, unless the purpose of the interception is to commit a crime or other injurious act. The theory behind this provision is that the conversation is no longer private, because at least one participant has consented to the interception. Unless an interception is exempt, a person may be fined up to $10,000 and imprisoned up to five years for wire tapping.[201] For example, agents of a common carrier may intercept wire communications in the course of their employment. FCC employees may intercept communications while performing official duties. Law enforcement personnel may intercept communications if they have the consent of one or more of the communicating parties or act with a court order.[202]

The use of intercepted communications as evidence in judicial, administrative or legislative proceedings is restricted.[203] Evidence is not admissible in federal, state or local proceedings if its gathering was not authorized by the Act. The Act provides for disclosure of intercepted information if it is derived from a court-authorized interception and if the parties opposed to disclosure have been notified of the impending disclosure and furnished with a copy of the court order authorizing the interception.[204] A person may move to suppress disclosure of wire or oral communications on the grounds that the authorization for the interception was insufficient or that

199 18 U.S.C. § 2510 (1982).
200 *Id.* § 2510(1), (2), (4).
201 *Id.* § 2511(1).
202 *Id.* § 2511(2).
203 *Id.* § 2515.
204 *Id.* § 2517.

the interception did not conform to the authorizing order.[205] A person whose communication is intercepted or disclosed in violation of the law can sue the perpetrators. Good-faith reliance on a court-ordered interception, however, is a complete defense to such a lawsuit.[206]

A court may order the interception of a communication if there is probable cause to believe that: (a) an individual is involved in one of several enumerated crimes (e.g., transmission of betting information, bribery, extortion); (b) information relating to that offense will be obtained through an interception; (c) normal investigative techniques have failed or appear unlikely to succeed; and (d) the communications at issue are commonly used by suspects in the case.[207] Another clause provides emergency grounds for interception without prior court approval for communications concerning activities that threaten national security or involve organized crime. In these cases, however, application for court approval must be made within forty-eight hours of the interception.[208]

In addition, under the Foreign Intelligence Surveillance Act, the president, through the attorney general, may authorize electronic surveillance to obtain foreign intelligence information without a court order.[209] The surveillance must be directed solely at intercepting communications between foreign powers or at acquiring technical intelligence information emanating from premises under a foreign country's exclusive control. There must be no substantial likelihood that the surveillance will intercept communications with a U.S. citizen.[210] Where communications of U.S. citizens are involved or are likely to be involved, surveillance cannot be undertaken without court approval.[211] The attorney general may direct a common carrier to furnish all information, facilities or technical assistance necessary to carry out surveillance and to keep records of the communications under strict security procedures.[212]

3. *Governmental Access to Financial Data*

The Right to Financial Privacy Act of 1978 generally denies government

205 *Id.* § 2518(a).
206 *Id.* § 2520.
207 *Id.* § 2518(3).
208 *Id.* § 2518(5).
209 50 U.S.C. § 1801 (1982).
210 *Id.* § 1802(a).
211 *Id.* § 1802(b).
212 *Id.* § 1802(4).

authorities access to customer financial information held by banking and other financial institutions.[213] But exceptions exist, such as authorization by the customer, compliance with an administrative subpoena, a valid search warrant or court order or a formal written request.[214] All of these activities must further a legitimate law enforcement inquiry in order to create an exemption.

A government agency must notify the subjects of an inquiry that their financial records are being sought and disclose the purpose of the request. A person subject to an inquiry may challenge the inquiry in federal court on the ground that the information sought is not relevant to a legitimate law enforcement inquiry.[215] The government may obtain a court order for direct access without notice, upon a showing that notice would allow the subject party to flee or to destroy evidence.[216] Upon receipt of financial records, one government agency may not disclose them to another agency without notifying the subject-party and without a certification from the receiving agency that the records are relevant to a legitimate law enforcement inquiry.[217]

4. *Electronic Funds Transfer Act*

The Electronic Funds Transfer Act (EFTA) requires financial institutions to inform their customers about their rights and obligations for EFT services.[218] It provides procedures for resolving inaccuracies in customer accounts and penalties for banks' errors in transmitting or documenting EFT transactions.

The EFTA defines an »electronic funds transfer« as any transfer of funds initiated through an electronic terminal, telephonic instrument, computer or magnetic medium (e.g., tape, disc, RAM) to authorize a financial institution to debit or credit an account. This includes point-of-sale transfers, automated teller machine transactions, direct deposits or withdrawals and transfers by telephone.[219] The Act covers state and national banks, state and federal savings and loan associations, mutual savings banks, state and fed-

213 12 U.S.C. § 3401 (1982).
214 *Id.* §§ 3405–3408.
215 *Id.* § 3408.
216 *Id.* § 3409.
217 *Id.* § 3412(a).
218 15 U.S.C. § 1693 (1982).
219 *Id.* § 1693a(6).

eral credit unions, and any other entity that directly or indirectly holds customer accounts.[220]

The Act requires a financial institution to disclose the terms and conditions of EFT accounts when a consumer orders EFT service, including information on issues such as: the consumer's liability for unauthorized transfers; the types of services offered; rates for all services; the institution's liability to the consumer; and the conditions under which EFT consumer information will be disclosed to third parties.[221] The consumer is liable for an unauthorized EFT transaction if it took place either with an access card or device issued by the institution for EFT transactions or through a code or other means of access issued by the institution. A consumer's liability for an unauthorized transaction, however, does not exceed fifty dollars.[222] A financial institution is liable for failing to make a transfer in the correct amount or time period if it had proper instructions from the consumer – subject to exceptions, of course, such as insufficient funds in the account or force majeure.[223]

A financial institution is liable to a consumer for failure to comply with the Act's provisions. But an unintentional violation – that is, a bona fide error that took place despite all reasonable precautions – does not create liability.[224] Compliance with EFTA's provisions is enforced by the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Commission and other federal agencies.[225]

5. *Private Collection of Credit and Other Financial Information*

The Fair Credit Reporting Act (FCRA) regulates the information-gathering and -disclosure practices of »consumer reporting agencies« (CRAs) and the use of »consumer credit reports.«[226] A CRA is »any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.«[227] If businesses gather but

220 *Id.* § 1693a(8).
221 *Id.* § 1693c.
222 *Id.* § 1693g.
223 *Id.* § 1693h.
224 *Id.* § 1693m(a), (c).
225 *Id.* § 1693.
226 *Id.* § 1681.
227 *Id.* § 1681a(f).

do not disclose information to third parties or disclose only information about their own dealings with a consumer, they are not deemed to be »reporting agencies.« A »consumer report« is »any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used ... as a factor in establishing a consumer's eligibility for (1) credit or insurance, ... (2) employment purposes, or (3) other purposes« (i.e. government benefits, licenses or business transactions).[228]

A consumer reporting agency may furnish a financial report under the following circumstances:

1. in response to a valid court order;
2. with the consumer's permission;
3. to parties that intend to use the information for a consumer credit transaction (e.g., extension of credit, review or collection of an account) or for employment purposes;
4. for underwriting insurance for a consumer;
5. to parties using the information to determine a consumer's elegibility for a government license or benefit; or
6. to parties with a legitimate business need for the information in connection with a business transaction with the consumer.[229]

A CRA need not allow consumers to see their files but must disclose to them the »nature and substance« of all information (except medical information) in its files, the source of the information and any third-party access to the data within the last six months. The Act prohibits reporting of obsolete information – e.g., paid tax liens that antedate the report by seven years.[230]

Consumers may dispute the contents of their file.[231] Upon verification of discrepancies, the agency must delete inaccuracies and notify parties who had received the information.[232] If a third party denies credit, insurance or employment to a consumer on the basis of a CRA's report, the third party must identify the CRA to the consumer.[233]

Willful noncompliance with these provisions by CRAs or third parties creates liability for actual and punitive damages.[234] Negligent noncom-

228 *Id.* § 1681a(d) (1982).
229 *Id.* § 1681b.
230 *Id.* § 1681c.
231 *Id.* § 1681i.
232 *Id.* § 1681i(d).
233 *Id.* § 1681m(a).
234 *Id.* § 1681n.

pliance also gives rise to liability. The Act's requirements are enforced primarily by the Federal Trade Commission and secondarily by the Federal Deposit Insurance Corporation, the Comptroller of the Currency and others.[235]

6. *Collection of Information by Cable Television Systems*

a. *Federal law*

The Cable Communications Policy Act of 1984 (Cable Act) is a general codification of cable television law, including provisions on subscriber privacy.[236] The Act requires cable operators to give initial and thereafter annual written notice to cable subscribers informing them of: (1) the type of personally identifiable information to be collected on them and the nature of its use; (2) the nature, purpose and frequency of disclosure of such data, as well as the types of persons to whom disclosure will be made; (3) the time period during which data will be maintained by the operator; and (4) the times and places at which subscribers can examine this information.[237]

The Cable Act prohibits a cable operator from collecting personally identifiable information concerning any subscriber without the subscriber's prior written or electronic consent.[238] For example, on an interactive or two-way system, a computer might need to ask subscribers whether they consented to the release of information about their transaction before processing transaction requests. Without a subscriber's consent, a cable operator may only collect data necessary to render cable service or to detect unauthorized reception of cable communications.[239]

A cable operator may not disclose personally identifiable information about subscribers without their consent.[240] An exception to this prohibition exists if disclosure is necessary to conduct a legitimate cable television business activity or is pursuant to a court order, after the subscriber has received notice of the order.

Cable subscribers have access to all information about them maintained by

235 *Id.* § 1686s.
236 47 U.S.C. § 521 (Supp. 1986).
237 *Id.* § 551(a)(1).
238 *Id.* § 551(b)(1).
239 *Id.* § 551(b)(2)(A), (B).
240 *Id.* § 551(c)(1).

a cable operator.[241] A subscriber must have a reasonable opportunity to correct any error in such data. A cable operator must destroy personally identifiable information that is no longer necessary.[242] Any person aggrieved by a cable operator's violation may bring a civil action in a federal district court. The court may award punitive as well as actual damages and reasonable attorneys fees as well as litigation costs.[243]

As a corollary to a subscriber's access rights, a government agency may obtain information about a subscriber only if it shows a court through clear and convincing evidence that the subject of the request is reasonably suspected of engaging in criminal activity and that the information would be material evidence in the case. In any event, the subscriber has a right to contest the government's claim.[244]

The Act does not prevent state or local franchising authorities from enacting or enforcing laws consistent with the Act in order to protect subscriber privacy.[245] An number of states and cities in fact do so, as discussed below.

b. *State law: The Wisconsin, California and Illinois examples*

Under Wisconsin law, upon a subscriber's request, any terminal capable of transmitting a message from a subscriber's location to an operator's central processing facilities must provide the subscriber with equipment to prevent transmission of such messages – except for signals necessary to monitor security, fire and utility services.[246] A cable operator must notify each subscriber in writing of the availability of such devices and may not make any additional charge for them.[247]

Unless an operator obtains the written consent of a cable subscriber every two years, an operator may not: (1) monitor the subscriber's cable equipment or use, except for purposes of billing or of checking the system's technical performance; (2) disclose information on a subscriber's personal behavior, including individual viewing habits, finances or programming preferences; or (3) conduct research that requires subscriber response (except by mail or personal interview), unless the subscriber has been notified in writ-

241 *Id.* § 551(d).
242 *Id.* § 551(e).
243 *Id.* § 551(f).
244 *Id.* § 551(h).
245 *Id.* § 551(g).
246 WIS. STAT. ANN. § 134.43(1)(a) (1982).
247 *Id.* § 134.43(1)(c), (d).

ing before the research begins.[248] Violators are subject to a forfeiture of up to $50,000 for a first offense and $100,000 for subsequent offences.

The Illinois Communications Consumer Privacy Act makes it unlawful for a cable operator to: (1) observe activities in a subscriber's household without the subscriber's knowledge or permission; (2) provide lists of subscribers without prior notice to them; (3) disclose a subscriber's television viewing habits without his or her prior consent; or (4) install a home security device without the resident's express written consent.[249] Violations of the Act are punishable by fines of up to $10,000.

California prohibits cable operators from recording or monitoring conversations without the subscriber's express written consent. A cable operator also may not disclose any individually identifiable information – such as a subscriber's viewing habits, shopping choices, interests, opinions, banking data or any other personal or private information – without the subscriber's written consent.[250]

The California statute also prohibits a cable operator from giving individually identifiable subscriber data to government agencies in the absence of legal compulsion, such as a court order or subpoena. An operator must notify a subscriber of the nature and origin of any request prior to disclosing information, unless otherwise prohibited by law.[251] Individually identifiable subscriber information gathered by a cable operator must be made available for subscriber inspection. If a subscriber shows that the information is inaccurate, an operator must correct the data.[252] A cable operator must notify all subscribers of their privacy protections.[253]

7. *Unauthorized Interception of Programming*

The Communications Act includes a general prohibition on the unauthorized interception and commercial exploitation of signals not transmitted to the general public.[254] Divulging the contents of these signals to third parties without the sender's consent violates the Act. The prohibition does not apply, however, to radio communications relating to ships, aircraft,

248 *Id.* § 134.43(2)(a), (b), (c).
249 ILL. STAT. ANN., ch. 38, § 87–1 (1982).
250 CALIF. STAT. ANN. § 637.5(a)(1), (2) (1982).
251 *Id.* § 637.5(c).
252 *Id.* § 637.5(d).
253 *Id.* § 637.5(e).
254 47 U.S.C. § 705(a) (Supp. 1985).

vehicles or persons in distress, or transmitted by amateur or citizens band operators.

As amended by the Cable Act, section 705 also prohibits the interception of channels on a cable television system without the program supplier's specific authorization. In effect, it creates a federal »theft of service« statute to prevent viewers from receiving programming without paying for cable service. The severity of criminal penalties for violating this section depends on the nature of the intercepted signal. Willful violations for personal use may result in fines of up to $1,000 and imprisonment for up to six months. But if a person willfully intercepts signals for purposes of »commercial gain« (e.g., to attract customers to a restaurant), he or she is liable for fines of up to $50,000 and imprisonment for up to two years.

Along somewhat similar lines, another Cable Act amendment attempts to create a new »marketplace« system for cable and other programming transmitted by satellite.[255] Most cable channels – such as the pay channel Home Box Office (HBO) – are transmitted via satellite and intended for receipt only by cable television operators, who then resell them to their subscribers. Many viewers have bought inexpensive – $1,000 to $2,000 – satellite receivers, in order to pick up these signals for free. Section 705 now allows reception of programs if they are not encrypted and if a »marketing system« is not established by the national programming source, such as HBO.

If a marketing system has been established, a user may receive such programming upon paying the programmer for a license.[256] Unauthorized private viewing of these signals is punishable by a fine of up to $1,000 and imprisonment for up to six months. If people intercept these signals without authorization and for commercial gain, however, they may be fined up to $50,000 and imprisoned for up to two years.[257] Violators face civil liability for all revenues received by their interceptions. Programmers also may seek injunctions and damages.

In practice, the unauthorized reception of satellite transmissions has been growing by leaps and bounds, particularly in rural areas that are not served by cable television. Some observers believe that almost two million homes now have satellite receivers.[258] Satellite programmers recently adopted a uniform scambling protocol, however, and will begin encrypting their signals in 1986 – a move that naturally will force viewers to buy service from

255 *Id.* § 705(b).
256 *Id.* § 705(b)(1), (2).
257 *Id.* § 705(d)(1), (2).
258 Cablevision, Dec. 9, 1985, at 11.

the programmers.[259] The trend appears to be that local cable operators will sell programming for satellite reception within their operating areas, thus adding a new revenue flow to their operations.

C. *Anti-Espionage Laws and Classified Information Statutes*

U.S. law contains a large number of data-classification provisions relating to espionage.[260] An intensive discussion of these provisions is not feasible here. Nevertheless, a brief description of several major provisions may be in order, since all of them impact upon the availability of data for international transmission.

The Espionage Act imposes fines of up to $10,000 and imprisonment for up to ten years on persons convicted of engaging or conspiring to engage in three broad categories of proscribed activity.[261] The terms of the Act are quite comprehensive in scope. They include the following.

1. *Gathering, Transmitting or Losing Defense Information*

It is illegal to obtain information regarding national defense by entering military installations, government buildings or research laboratories, or by intercepting defense-related telephone, telegraph or radio transmission.[262] Unauthorized copying or other obtaining of documents, plans, photographs and items connected with the national defense also violates the Act.[263] If a person receives or attempts to receive illegally procured national defense materials, he or she is in violation of the Act.[264] If people

259 *Id.*

260 *See, e.g.*, 50 U.S.C. § 401 note, Ex. Ord. No. 12356, section 1.3(1) (1982) (classification of military plans); 50 U.S.C. § 401 note, Ex. Ord. No. 12356, section 1.3(2) (1982) (information regarding national security installations); 50 U.S.C. § 401 note, Ex. Ord. No. 12356, section 1.3(3) (1982) (information regarding foreign governments); 50 U.S.C. § 401, Ex. Ord. No. 132356, section 1.3(40) (1982) (information regarding intelligence activities); 50 U.S.C. § 401 note, Ex. Ord. No. 12356, section 1.3(5) (1982) (information regarding foreign relations); 50 U.S.C. § 401 note, Ex. Ord. No. 12356, section 1.3(7) (1982) (information regarding nuclear materials and facilities).

261 18 U.S.C. § 791 (1982).

262 *Id.* § 793(a).

263 *Id.* § 793(b).

264 *Id.* § 793(c).

with lawful access to defense-related materials communicate such information to unauthorized persons or fail to deliver such information to an authorized U.S. official, they also violate the Act.[265]

2. *Delivering Defense Information to Foreign Governments*

If people have reason to believe that information in their possession may be used to jeopardize national security, they may not communicate it to any foreign government or its agents.[266] Violation of this section is subject to punishment by execution or life imprisonment. Attempting to communicate defense and security-related information to an enemy in wartime also may be punished by execution or life imprisonment.[267]

3. *Disclosure of Classified Information*

The law prohibits any knowing communication to unauthorized persons of classified information concerning: (1) the nature, preparation or use of any U.S. or foreign code, cipher or cryptographic system; (2) the design, construction or use of U.S. or foreign cryptographic or intelligence-related devices; (3) the communications intelligence activities of the United States or any foreign government; or (4) confidential communications of foreign governments.[268]

265 *Id.* § 793(d).
266 *Id.* § 794(a).
267 *Id.* § 794(b).
268 *Id.* § 798(a)(1), (2), (3), and (4).

Conclusion

This survey of restrictions on data flows out of or into the United States shows that such restrictions are relatively limited and are diminishing outside the area of national security. Historically, the United States has exercised some control over international communications by regulation of the channels of communication rather than the content of the communications themselves. This regulation was premised initially on the scarcity of the electromagnetic spectrum and later of geosynchronous orbit positions. Coupled with the absence of a governmental monopoly, this scarcity necessitated an allocation among private firms. The regulation of communications channels, in turn, focused primarily on industry *structure* rather than on *behavior*, on the grounds that structure determines behavior and that structural regulation avoids free speech problems under the first amendment of the U.S. Constitution.

Historically, the U.S. policy in international telecommunications had been to carve up the market into distinct segments, each assigned to different types of carriers. Underlying the restrictive licensing scheme was the desire to regulate behavior and at least partly limit AT&T's power – by restricting it to the voice market, regulating its rates and insulating the international record carriers from competition. When satellite communications emerged as a potential disruption to this system, fear of AT&T's expanding powers led the U.S. government to create Comsat as a monopoly, initially serving as a carriers' carrier without any competition for users' business.[269]

This system of neat, compartmentalized service categories functioned as a cartel mechanism by dividing markets and separating competitors from each other. Partly because it was profitable, it proved unstable when its underlying conditions changed, namely, when: (a) voice and record service distinctions broke down as telephone carriers became major data carriers; (b) new entrants did not conform to traditional market divisions; (c) transmission capacity grew and costs fell rapidly due to high-capacity satellites as well as submarine cables; and (d) government policies opened competition in domestic telecommunications, dismembered AT&T and extended deregulation to the international sector.[270]

269 *See* discussion in text at note 155 *supra*.
270 *See* discussion in text at note 141 *supra*.

These factors combined to eliminate in rapid succession many of the structural rules that had characterized U.S. communications. The few remaining rules may also change, along with INTELSAT's position. The United States is in transition to an environment in which carriers – such as AT&T, MCI, Sprint, RCA, Western Union, Comsat, Tel-Optic and Orion – will compete to provide all types of domestic as well as international transmission services, with little governmental supervision except for initial frequency and orbital allocations.[271]

The limit on this scenario, of course, is the necessity of accommodation with overseas carriers and governments, which do not share the United States' competitive views for reasons of ideology, politics or economics. The United States faces in every international telecommunications body a front that includes most of its traditional allies and trading partners. At the same time, the competition among U.S. carriers allows those countries' telecommunications authorities to play off U.S. carriers against each other, thus transforming a previously bilateral monopoly situation into a unilateral one.

At the extreme, foreign carriers could enter the U.S. market by connecting with local BOC exchange companies; they thus could bypass U.S. long-distance and international carriers while discriminating against the latter's access in their home territories. In this situation, a variety of U.S. measures – such as the »anti-whipsawing« rules – may survive and even expand. While inconsistent with true deregulation, these rules would be a rational response to the realities of an international environment that prevents unilateral deregulation in a multilateral world.

With these caveats, most U.S. regulation of transmission channels and market segments is about to disappear. In terms of regulation of international communications flows, this leaves primarily those restrictions that also affect domestic communications. In other words, the international effect is merely an extension of domestic law, including special provisions as to national security. Among the former category – that is, general restrictions on information flows – are the following, which for purposes of brevity have not been discussed in this paper:

(a) privileged information (such as medical or accounting data);
(b) defamation;
(c) proprietary information, protected by copyright or contract;
(d) financial information, which the financial securities laws may require to conform to certain standards of completeness, timeliness and accuracy;

271 *See* discussion in text at note 147 *supra*.

(e) false advertising;
(f) obscenity and indecency;
(g) information that can be construed to be part of the unauthorized practice of a profession requiring a license;
(h) information violating people's privacy, appropriating their likeness or personality, holding them up to ridicule, causing mental and emotional distress or interfering with their civil rights;
(i) »fighting words« that are likely to provoke an immediate violent response;
(j) advocacy of violent behavior, where such behavior is imminent, intended and likely;
(k) advertising of controlled products and services, such as liquor, cigarettes and gambling;
(l) the manner of political speech, in instances where public campaign financing is accepted; and
(m) in general, regulation concerning the reasonableness of time, place and manner of information dissemination. For example, the provision of sexually oriented »adult« pornographic telephone tape messages outside of evening hours may be limited.

While these general categories of restrictions exist, they almost never prohibit information flows in advance. Only *after* such dissemination has taken place can an injured individual or the state seek damages or penalties.[272] Exceptions to this principle against »prior restraints« are obscenity, some national-security threats and imminent danger of violence. Most of the other restrictions listed above are interpreted very narrowly and are difficult to enforce because of the presumption in favor of free speech. The major exception is securities-trading regulations, which control dissemination and use of stock-market-related information. These restrictions recently have become subject to constitutional challenge under the free speech clause of the U.S. Constitution.[273]

All of these restrictions affect information flows into or out of the U.S. Their scope is in continuing flux because of vague statutes and regulations, which are subject to judicial, common-law, case-by-case review. While it is difficult to generalize, the past trend was to limit restrictions on information flows, and this has continued under the current Supreme Court.

The major restriction on international and U.S. domestic information flows lies in the area of national security. Unilateral and cooperative restrictions

272 *E.g.*, Near v. Minnesota, 283 U.S. 697 (1931).
273 *See* Penny Stock Newsletter, Nos. 801–19962, 801–15347 (S.E.C., Dec. 19, 1984).

on the transfer of technological and strategic information to non-allied countries exist in a variety of forms, and their enforcement has received priority in recent years. These regulations center on nuclear information, arms information and dual-use (civilian and military) information. Multinational coordination attempts to harmonize Western efforts.[274]

Concerning the protection of data privacy, there is a frequent but erroneous view that such protections are weak or non-existent in the United States. There is no comprehensive national statute, possibly because of a general U.S. reluctance for centralized legislation. The thrust of U.S. protection is to restrict, through piecemeal legislation, governmental intrusion into personal data by requiring search warrants, notification, opportunity to challenge searches, access by individuals to information about themselves and the right to correct such data. Restrictions on the private collection of data are more lax where the information is not distributed to third parties. Here the underlying assumption is that an individual seeking credit or employment relinquishes some privacy in order to reduce transactions costs. But consumers have access to credit files kept on them, and employers cannot divulge information freely.

Some characteristics of U.S. international communications regulation conflict both with each other and with other industrialized countries' policies. These characteristics are:

(a) withdrawal of the governmental role in establishing channels of communications and encouragement of competition;
(b) freedom of speech (tempered by common-law and regulatory safeguards of special policy concern)
(c) national security;
(d) acceptance of private data collection as an integral part of economic activity; and
(e) support of the commercial activities of U.S. firms internationally.

As befits this multiplicity of goals, there are not enough »degrees of freedom« to structure a consistent and stable policy, nor is every goal achieved in a pure form. Hence, foreign critics easily can point to inconsistencies as a sign of ideological hypocricy or commerical greed. As Ralph Waldo Emerson said, however, »A foolish consistency is the hobgoblin of little men.«[275] It is precisely in the nature of the common law and of a federal state that policies emerge piecemeal, without necessarily being coordinated in time and purpose.

274 *See* discussion in text at note 188 *et seq. supra.*
275 R.W. EMERSON, SELF-RELIANCE.

On the other hand, such a mechanism permits frequent adjustmen
Indeed, U.S. policies on information and telecommunications hav
changed quite rapidly in the past fifteen years, with little major legislatio
Overall, the tendency clearly has been towards withdrawal of the gover
mental role. In the international sphere, the concurrent stress on nation
security has been the major counter-trend.

This is not ideological inconsistency; even most advocates of a minimali
state seek a strong protective role for government in foreign affairs. But
creates practical problems, as well as the need to negotiate with foreig
governments on international communications matters. It keeps the U.S
government active in communications regulation and creates a built-in fric
tion with its allies, which is not likely to disappear in the near future.