International Lawyer

Volume 35 | Number 1 Article 6

2001

Hidden Dangers in the E-Commerce Data Mine: Governmental Customer and Trading Partner Screening Requirements

Peter L. Fitzgerald

Hidden Dangers in the E-Commerce Data Mine: Governmental Customer and Trading Partner Screening Requirements

PETER L. FITZGERALD*

I. Introduction

As spring approaches, the Walmart.com operation in Silicon Valley receives a series of online orders from Rolando Franco. While most of the products are to be delivered to Franco's offices across the country in South River, New Jersey, some of the orders are to be shipped directly to his associates in Europe. A world away in St. Petersburg, Russia, the Baltic State Technical University places an order for some newly announced laptop computers using the Dell Computer website. Meanwhile, back in snowy Quebec, Pierre Boileau decides to go online and subscribe to America Online Canada, the local subsidiary of the well-known U.S.-based Internet services provider. Pursuing any of these hypothetical transactions—whether conducted wholly within the country, partially within the country, or entirely abroad—could result in substantial administrative, civil, and criminal penalties under U.S. laws and regulations. In each case, this exposure arises not because of the nature of the business being conducted, but rather because of who is participating in the transaction.

The late Sam Walton said the secret to Wal-Mart's success was its "ten-foot attitude." He insisted each employee, or associate, make shopping at Wal-Mart a personal experience. During meetings with the employees at his stores Sam would say, "I want you to promise that whenever you come within 10 feet of a customer, you will look him in the eye, greet him, and ask if you can help him."[1] It is difficult to apply this personal approach to the

 Peter L. Fitzgerald is an Associate Professor of Law, Stetson University College of Law, St. Petersburg, Florida; B.A. William and Mary 1973; J.D. University of California—Hastings College of Law 1976; LL.M. (European Legal Studies) University of Exeter, United Kingdom, 1981. Professor Fitzgerald teaches an E-Commerce Seminar, International Law, International Business Transactions, and International Trade Regulation. Prior to joining the Stetson faculty, Professor Fitzgerald was a member of the IBM Legal Department and law clerk to the Honorable Patrick E. Higginbotham, U.S. District Court, Northern District of Texas.

1. Walmart.com, *Sam's Way: About Walmart.com*, *at* http://www.walmart.com/cservice/aw_samsway.gsp (visited Dec. 12, 2000).

world of e-commerce, and Sam's associates at Walmart.com ask themselves daily how to apply the "ten foot attitude" to a website.[2] They declare that the answer starts,

> [W]e figure, with striving to build a site that is easy for customers to use. We work every day to bring you a better shopping experience. Our online store will always be a work in progress, but one thing won't change: our commitment to keeping our customers' needs at the top of our priority list.[3]

Making e-commerce sites easy to use and meeting online users' needs depends in large part upon knowing as much as possible about who uses a particular site and what they want.

Data mining—gathering, collating, and organizing information concerning one's customers and trading partners—is of fundamental importance to all forms of e-commerce, whether on the business-to-business or business-to-consumer level.[4] In addition to the usual types of information exchanged during the course of any ordinary commercial transaction, online commerce is becoming particularly dependent upon the personalization of the offerings or services provided in order to distinguish one e-business from another. This is seen, for example, in the "welcome" screens employed by Amazon.com and a number of other sites that greet returning customers by name and highlight products or services relating to their past transactions.

This drive towards increasing personalization creates substantial pressure to use whatever technology is available to obtain more and more information from users and visitors to e-business sites, but gathering this information also creates new exposures. While most e-businesses are aware of the privacy issues these technologies and activities create,[5] a potentially more explosive, and much less appreciated, exposure lies hidden in the various blacklists employed in the federal government's trade controls and economic sanctions programs. These exposures are especially insidious, as they generally derive from laws and regulations that both predate the advent of most e-commerce technology and that were not generally crafted with e-commerce transactions in mind. Nevertheless, given the global

2. *Id.*

3. *Id.*

4. *See, e.g.*, Jonathan Berry, *Database Marketing—A Potent New Tool for Selling*, BUS. WK., Sept. 5, 1994, at 56; Laurie Hays, *Using Computers to Divine Who Might Buy a Gas Grill*, WALL ST. J., Aug. 16, 1994, at B1. The terminology that has developed around this area can be confusing, with fine distinctions sometimes being implied between the software and technology being employed to gather information (e.g., data mining tools), the application of those tools to extract information or infer relationships from computerized records that are not necessarily readily apparent (e.g., database mining), and the process of transforming that information into business decisions (e.g., database marketing). *See* Kurt Thearling, *From Data Mining to Database Marketing*, White Papers, *at* http://www3.shore.net/~kht/text/wp9502/wp9502.htm (visited Dec. 12, 2000). For an overview of the types of tools and techniques available for data mining, see generally A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395 (1996).

5. The impact of data mining upon privacy has generated a vigorous debate both within the United States and internationally. *See, e.g.*, Edward C. Baig *et al.*, *Privacy: The Internet Wants Your Personal Info. What's in It for You?*, BUS. WK., Apr. 5, 1999, at 84; Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: A Work in Progress*, 23 NOVA L. REV. 549 (1999); Deirdre Mulligan, Center for Democracy & Technology, *Public Workshop on Online Profiling: Testimony of the Center for Democracy and Technology Before the Federal Trade Commission* (Nov. 30, 1999), *at* http://www.cdt.org/testimony/ftc/991130mulligan.shtml (visited Dec. 12, 2000); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (2000).

reach of online operations, these laws and regulations do apply to e-commerce transactions and violations can result in potentially disastrous consequences.

Consider, for example, Walmart.com's hypothetical dealings with Rolando Franco. Franco was named[6] to the U.S. Commerce Department's Denied Persons List (DPL)[7] because he violated[8] the Export Administration Regulations (EAR)[9] promulgated under the Export Administration Act (EAA).[10] The State Department maintains a similar blacklist of those who violate the International Traffic in Arms Regulations (ITAR),[11] promulgated under the Arms Export Control Act (AECA),[12] which is known as the Debarred List.[13] If Walmart.com conducts business with parties named on these blacklists, like Franco, it risks violating the U.S. trade control regulations itself,[14] even without being directly involved in an export.[15]

If Dell Computer knowingly sends its products to the Baltic State Technical University, it, too, risks violating the U.S. export controls.[16] The University appears on a blacklist of foreign entities of concern with regard to their involvement in weapons proliferation ac-

6. *See* 60 Fed. Reg. 29,550 (June 5, 1995); 57 Fed. Reg. 33,936 (July 31, 1992).

7. 15 C.F.R. pt. 764, Supp. 2 (2000). The DPL is also available at http://www.bxa.doc.gov/dpl/2_denial.htm. *See also infra* notes 42-49 and accompanying text.

8. In 1992, Rolando Franco was found guilty of violating U.S. export control laws for attempting to divert U.S. computer components to the Soviet Union. He received a two year suspended jail sentence, three years probation, and a $6,000 fine. Franco's export privileges were also denied for five years. However, in 1994, Franco was again arrested and found guilty of violating the terms of the 1992 denial order by making numerous overseas shipments. He was fined $3,000 and served five months imprisonment that was followed by three years supervised release. In addition, his export privileges were denied for an additional ten years. *See* Bureau of Export Administration, *Tip from an Alert Manufacturer Helps Commerce Export Enforcement Uncover Violation by a Denied Party, at* http://www.bxa/doc.gov/Enforcement/CaseSummaries/franco.htm (visited Dec. 12, 2000); *New Jersey Man Sentenced for Violating Export Denial Terms*, EXPORT CONTROL NEWS, Dec. 30, 1994, *available at* LEXIS, Nexis News Library, News Group File.

9. 15 C.F.R. §§ 730-74 (2000).

10. 50 U.S.C. app. §§ 2401-20 (1994). The EAA, by its own terms, must be renewed periodically. The EAA expired in 1994, and the EAR promulgated under the EAA was administered under temporary extensions pursuant to the president's authority under the IEEPA for many years. *See* Continuation of Export Control Regulations, Exec. Order No. 12,924, 59 Fed. Reg. 43,437 (Aug. 19, 1994); Exec. Order No. 12,981, 60 Fed. Reg. 62,981 (Dec. 5, 1995); Continuation of Emergency Regarding Export Control Regulations, 61 Fed. Reg. 42,527 (Aug. 14, 1996); Amendment to Executive Order No. 12,981, Exec. Order No. 13,020, 61 Fed. Reg. 54,079 (Oct. 12, 1996); Continuation of Emergency Regarding Export Control Regulations, 62 Fed. Reg. 43,629 (Aug. 13, 1997); Continuation of Emergency Regarding Export Control Regulations, 63 Fed. Reg. 44,121 (Aug. 13, 1998); Continuation of Emergency Regarding Export Control Regulations, 64 Fed. Reg. 44,101 (Aug. 10, 1996); and Continuation of Emergency Regarding Export Control Regulations, 65 Fed. Reg. 48,347 (Aug. 3, 2000). On November 13, 2000 President Clinton signed H.R. 5239, the Export Administration Modification and Clarification Act of 2000, which reinstated and extended the EAA until August 20, 2001. *See* Statement by the President (Nov. 13, 2000), *available at* http://www.bxa.doc.gov/press/2000/HR%205239.html (visited Dec. 12, 2000); *Congress Passes "Baby" EAA*, EXPORT PRACTITIONER, Nov. 2000, at 11.

11. 22 C.F.R. §§ 120-28 (2000).

12. 22 U.S.C. §§ 2778-99 (1994).

13. Announcement of actions with regard to debarred parties periodically appear in the Federal Register. Additionally, an unofficial version of the debarred list is available online at http://www.pmdtc.org/debar059.htm.

14. *See* General Prohibition Four (Denial Orders)—Engaging in Actions Prohibited by a Denial Order, 15 C.F.R. § 736.2(b)(4) (2000).

15. *See infra* notes 51-52 and accompanying text.

16. *See* General Prohibition Five—Export or Reexport to Prohibited End-Uses or End-Users (End-Use End-User), 15 C.F.R. § 736.2(b)(5) (2000).

tivities.[17] Unlike the debarred or denied persons blacklists, the parties designated on the Commerce Department's Entities List[18] need not have violated U.S. law themselves—rather they tend to be parties engaged in behavior that is frowned upon by the government but who are beyond the direct reach of U.S. law and jurisdiction. Those who are subject to U.S. jurisdiction, such as Dell Computer, are prohibited from dealing with these blacklisted entities without U.S. government approval.[19]

A willful failure to comply with these trade controls may be punished by criminal penalties of up to ten years imprisonment, and organizational fines of up to $1 million or five times the value of the goods, whichever is greater.[20] Criminal penalties of up to five years' imprisonment and fines of up to $50,000 or five times the value of the goods are available for knowing violations.[21] Civil fines of up to $100,000 may also be imposed without any showing of knowledge or intent to violate the controls.[22]

The scenario involving Pierre Boileau, unlike the previous two examples, does not involve trade with the United States at all. If American Online Canada conducts business with Pierre Boileau, even though that business is conducted in Canada and between Canadian parties, it nevertheless violates the Treasury Department's regulations regarding the Cuban embargo[23] promulgated under the Trading With the Enemy Act (TWEA).[24] The U.S. government considers Pierre Boileau, a Canadian, as a specially designated national (SDN)

17. Additions to Entity List: Russian Entities, 63 Fed. Reg. 40,363 (July 29,1998).

18. Entity List, 15 C.F.R. pt. 744, Supp. No. 4 (2000), *available at* http://www.bxa.doc.gov/Entities/Default.htm (visited Dec. 12, 2000).

19. BXA explains that:

> Since February 1997, the Federal Register has published several Commerce Department rules which added entities to the Entity List, a listing of foreign endusers involved in proliferation activities. . . . These end-users have been determined to present an unacceptable risk of diversion to developing weapons of mass destruction or missles used to deliver those weapons. Publishing this list puts exporters on notice that any products sold to these end-users may present concerns and will require a license from the Bureau of Export Administration . . . Interagency groups involved in the export control process reviewed the activities of the published entities of concern and determined that exports to these entities would create an unacceptable risk of use in or diversion to prohibited proliferation-related activities. Publishing this entities list allows the U.S. government to identify for U.S. businesses some of the organizations and companies that may be involved in proliferation activities. The development of a list of entities of concern arises from the . . . initiative begun in 1990 to stem the spread of missile technology as well as nuclear, chemical, and biological weapons. Under [this initiative] the Commerce Department can impose licensing requirements on exports and reexports of normally uncontrolled goods and technology where there is an unacceptable risk of use in or diversion to activities related to nuclear, chemical, or biological weapons or missile proliferation, *even if the end-user is not primarily weapons-related.*

Bureau of Export Administration, *The Entity List: Background, at* http://www.bxa.doc.gov/Entities/Default.htm (visited Dec. 12, 2000) (emphasis added).

20. 50 U.S.C. app. § 2410(b); 15 C.F.R. § 764.3(b)(2) (2000). The maximum criminal fine for an individual is $250,000. *See also* 22 U.S.C. § 2778(c) (1994); 22 C.F.R. § 127.3 (2000).

21. 50 U.S.C. app. § 2410(a) (1994); 15 C.F.R. § 764.3(b)(1) (2000).

22. 50 U.S.C. app. § 2410(c) (1994); 15 C.F.R. § 764.3(a)(1) (2000). If national security controls are not at issue, the maximum civil fine is $10,000. Civil liability may be imposed without any showing of intent or knowledge. *See* Iran Air v. Kugelman, 996 F.2d 1253 (D.C. Cir. 1993); *see also* 22 U.S.C. § 2778(e) (1994); 22 C.F.R. § 127.10 (2000) (increases the maximum civil fine to $500,000 if munition items are involved).

23. 31 C.F.R. § 515 (2000).

24. 50 U.S.C. app. § 1 (1994).

of Cuba.[25] Dealings with a SDN, whether in the United States or in a foreign country, are treated the same as direct dealings with the targets of the government's various economic sanctions programs.[26] Thus, the United States considers any transactions with Pierre Boileau in Canada as if they were direct dealings with Cuba, triggering the broad prohibitions associated with that embargo program.[27] Moreover, because of the extraterritorial reach of the regulations, America Online's Canadian subsidiary is as obligated to comply with the terms of the embargo as is its Virginia-based parent company, at least from the perspective of U.S. law.[28] Violations of TWEA-based economic sanctions, like those imposed on Cuba, are punishable by imprisonment for up to ten years, and organizational criminal fines of up to $1 million, civil fines up to $55,000, and forfeiture of any property or funds involved in the transaction.[29] Violations of the International Emergency Economic Powers Act (IEEPA), which provides the foundation for many of the newer economic sanctions programs,[30] are similarly punishable by imprisonment for up to ten years, criminal fines of up to $50,000, and civil fines of up to $11,000.[31]

25. List of Specially Designated Nations, 51 Fed. Reg. 44,459 (Dec. 10, 1986). Pierre Bolieau was added to the SDN blacklist associated with the Cuban embargo on January 7, 1981, along with two other individuals, a Jamaican firm, six Panamanian firms, and two U.S. companies, all of whom allegedly were involved in evading the terms of the U.S. embargo of Cuba with their operations in third countries. *See* REUTER N. AM. NEWS, Feb. 11, 1981, *available in* LEXIS, News Library, REUNA File. Interestingly, Bolieau's name—and the names of the other parties on the Cuban SDN blacklist—did not actually appear in the Federal Register until this publication in 1986. There are numerous similar due process problems associated with the Treasury Department's administration of its economic sanctions programs. *See* Peter L. Fitzgerald, *If Property Rights Were Treated Like Human Rights, They Could Never Get Away with This: Blacklisting and Due Process in U.S. Economic Sanctions Programs*, 51 HASTINGS L.J. 73 (1999).

26. The Cuban Asset Control Regulations (CACR) prohibit all dealings with Cuba or Cuban nationals, without any geographic limitation. The broad basic regulatory prohibition states:

> All of the following transactions are prohibited, except as specifically authorized by the Secretary of the Treasury . . . by means of regulations, rulings, instructions, licenses, or otherwise if . . . such transactions are by, or on behalf of, or pursuant to the direction of [Cuba] or any national thereof, or such transactions involve property in which [Cuba] or any national thereof has . . . had any interest of any nature whatsoever, direct or indirect. . . .

31 C.F.R. § 515.201(a) (2000). The CACR then defines "national" to include not only Cuban citizens and business entities, but also any foreign entities that are directly or indirectly owned or controlled by Cuba or Cuban nationals; those who are believed to "act directly or indirectly for the benefit or on behalf of" Cuba or Cuban nationals; and those whom the Secretary of the Treasury deems to be a Cuban national. 31 C.F.R. §§ 515.305, 515.306 (2000). Thus, through the Secretary's power to name SDNs, the basic regulatory prohibition of the CACR may be extended to third parties who are not otherwise identified with Cuba or Cuban citizenship. *See also* American Airways Charters, Inc. v. Regan, 746 F.2d 865, 867 n.2 (U.S. App. D.C. 1984).

27. The CACR impose a sweeping set of prohibitions affecting all transfers of credit; transactions in foreign exchange; bullion, currency, or securities; "transfers, withdrawals, or exportations of, any property or evidences of indebtedness or evidences of ownership of property;" "all transfers outside the United States with regard to any property or property interest subject to the jurisdiction of the United States;" and specifically including the "purchase, transport, import, or [other dealing] with respect to any [Cuban] merchandise." 31 C.F.R. §§ 515.201, 515.204 (2000); *see also* 31 C.F.R. § 515.203 (voids all prohibited transactions).

28. Canada takes a decidedly different view of the legitimacy of the extraterritorial application of U.S. law to Canadian nationals and companies. *See infra* note 120 and accompanying text.

29. 50 U.S.C. app. § 16 (1994); 31 C.F.R. § 515.701 (2000). The maximum criminal fine for an individual is $250,000 or twice the pecuniary gain from the transaction, whichever is greater. *See* 18 U.S.C. § 3571 (1994); 31 C.F.R. § 515.701(b).

30. Unlike the government's trade controls, where all types of goods and services are regulated within a single set of regulations, the Treasury Department typically issues entirely separate, stand-alone regulations for each of its various sanctions programs and embargoes. *See infra* notes 69-97 and accompanying text.

31. 50 U.S.C. § 1705 (1994). IEEPA also provides the legislative foundation for the EAR during periods

Each of these potential violations occurs because a transaction is being conducted with a party that is blacklisted by the Commerce Department's Bureau of Export Administration (BXA), the State Department's Office of Defense Trade Controls (DTC), or the Treasury Department's Office of Foreign Assets Controls (OFAC). Violating the regulatory limitations on dealing with blacklisted parties can lead to substantial fines or criminal penalties.[32] However, the administrative sanctions available to these agencies to enforce their controls are much more commercially significant than any civil or criminal penalty. Simply put, those who engage in impermissible dealings with blacklisted parties may, in turn, find themselves blacklisted.[33] Walmart.com, Dell Computer, America Online, or any other business, could suddenly find their activities effectively curtailed or shut down as a result of dealing with the wrong customer or trading partner.[34] Under the letter of the law, even inadvertent violations of these laws and regulations can actually substantially restrict or stop business altogether.[35]

A. Governmental Blacklists in U.S. Trade Control Programs[36]

BXA and DTC, as the U.S. government's principal trade control agencies,[37] traditionally used blacklisting as a secondary tool to enforce their primary regulatory controls on exporting goods, services, and technology from the United States. Broad, product-oriented regulations aimed at controlling transactions based upon the technical capabilities of the specific products or technologies being exported, or disclosed to foreign nationals within the country, are at the heart of EAR and ITAR. The precise controls applied to specific items in any given transaction are detailed in complex regulatory control lists promulgated by each agency.[38] Almost any item or service that moves internationally will be covered by

when the EAA has lapsed. *See supra* note 10 and accompanying text. Accordingly, EAR specifically provides that penalties shall be appropriately limited to whatever authority is in effect at the time a violation occurs. *See* 15 C.F.R. § 764.3 (2000).

32. *See supra* notes 20-22, 29-31 and accompanying text.

33. *See* 15 C.F.R. § 764.3(a) (2000); 22 C.F.R. §§ 127.7-.8 (2000); *see also, e.g.*, 31 C.F.R. §§ 515.302(a)(3), 515.305, 515.306(a)(2) (2000).

34. *See supra* notes 6-10, 16-19, 24-28 and accompanying text; *infra* notes 47, 50-52, 64-65, 116, 143-45 and accompanying text.

35. *See infra* note 152-56 and accompanying text; *see also* Iran Air v. Kugelman, 996 F.2d 1253 (D.C. Cir. 1993).

36. *See generally* Peter L. Fitzgerald, *Pierre Goes Online: Blacklisting and Secondary Boycotts in U.S. Trade Policy*, 31 Vand. J. Transnat'l L. 1, 28-35 (1998).

37. There is no single agency or department responsible for U.S. trade controls. On the contrary, there are a variety of agencies involved in regulating U.S. exports and foreign trade, usually depending upon the goods or technology being transferred. These include the Department of Agriculture (tobacco seeds and plants), the Drug Enforcement Agency (narcotics and dangerous drugs), the Department of Energy (natural gas, nuclear, and electric power), the Food and Drug Administration (drugs, biologics, and medical devices), the Department of the Interior (endangered fish and wildlife, migratory birds, and Bald and Golden Eagles), the Maritime Administration (large watercraft), the Nuclear Regulatory Commission (nuclear equipment and material), and the Patent Office (technology contained in patent filings). *See* Other U.S. Government Departments and Agencies with Export Control Responsibilities, 15 C.F.R. pt. 730, Supp. 3 (2000). The vast majority of export and trade related matters, however, are the responsibility of the Departments of Commerce and State.

38. DTC controls products, services, and technology, described in the United States Munitions List, 22 C.F.R. § 121 (2000), and BXA controls products, services, and technology described in the Commerce Control List, 15 C.F.R. pt. 774, Supp. 1 (2000).

one or the other of these control lists.[39] Despite the substantial criminal and civil penalties available to punish those who fail to comply with these trade controls,[40] it is the agencies' ability to administratively blacklist violators that has the greatest commercial significance and impact. Blacklisted parties lose the right to export or receive U.S. goods or technology either directly from the United States or from others elsewhere who are subject to U.S. extraterritorial jurisdiction.[41]

The Commerce Department calls its blacklist the DPL[42] because persons or organizations listed in the DPL have been denied[43] the ability to make or receive exports of goods or technology subject to U.S. jurisdiction.[44] Denial Orders are issued by the Under Secretary for Export Administration following proceedings before an administrative law judge.[45] Temporary Denial Orders may also be issued if BXA believes that a violation of its regulations is imminent.[46] Denial is typically employed, however, as a sanction after a violation has occurred.[47] There are currently 304 entries on the DPL, many of which list multiple names or locations.[48] Thirty-four of these entries pertain to parties in the United States, including Rolando Franco.[49]

39. *See* P.L. Fitzgerald, *Prevention of Liability for Export Control Violations, in* BNA/ACCA CORPORATE COMPLIANCE MANUAL, Ch.14, § B(2)(b)(2) (1998).

40. *See supra* notes 20-22 and accompanying text.

41. *See* Standard Terms of Orders Denying Export Privileges, 15 C.F.R. pt. 764, Supp. 1 (2000); 15 C.F.R. §§ 766.24-.25 (2000).

42. 15 C.F.R. pt. 764, Supp. 2 (2000), *available at* http://www.bxa.doc.gov/DPL/denialist.html (visited Dec. 12, 2000). The names of parties being added to the list appear periodically in the Federal Register. This list used to be referred to as the Table of Denial Orders (TDO) but this terminology caused confusion with the term "Temporary Denial Order" used in connection with certain ex parte and other proceedings where export privileges are denied for a renewable six month period. *See id.* § 766.24; *see also infra* note 46.

43. There is a great deal of discretion in determining precisely what privileges will be lost, and for how long. Denial periods ranging up to thirty-five years have been issued. *See* Actions Affecting Export Privileges: Globe Computers et al. of Goran Josberg, 54 Fed. Reg. 9,537 (Mar. 7, 1989); Order Vacating Temporary Denial Order, Goran Josberg, 54 Fed. Reg. 13,715 (Apr. 5, 1989). It was not uncommon to see denial orders of indefinite (i.e., virtually permanent) duration in the 1980s. *See also* Denied Persons List, 15 C.F.R. pt. 764, Supp. 2 (2000), *available at* http://www.bxa.doc.gov/DPL/Default.htm.

44. No one subject to U.S. jurisdiction may engage in an export-related transaction that directly or indirectly benefits a denied party. *See* 15 C.F.R. § 764.3(a)(2) (2000). This includes "ordering, buying, receiving, using, selling, delivering, storing, disposing of, forwarding, transporting, financing, or otherwise servicing . . . any transaction . . . that is subject to the EAR." *Id.*; *see* Standard Terms of Orders Denying Export Privileges, 15 C.F.R. pt. 764, Supp. 1 (2000) at (b)B.

45. *See* Administrative Enforcement Proceedings, 15 C.F.R §§ 766.1-.25 (2000).

46. *See* Temporary Denials, 15 C.F.R. § 766.24 (2000). Export privileges may be suspended, in ex parte proceedings, with only a suspicion that a violation has or will occur. *See, e.g.*, Action Affecting Export Privileges: Delft Instruments N.V., 56 Fed. Reg. 8,321-02 (Feb. 28, 1991). These temporary denial orders may not exceed 180 days in duration, but may be renewed indefinitely.

47. The violation that triggers the denial order does not necessarily have to be a violation of the EAA. BXA has the ability to issue a denial order for violations of any trade-related regulation or a statute such as AECA or IEEPA. Thus, a Commerce denial order could be issued as a collateral sanction for an ITAR violation, for example. *See* 15 C.F.R. § 766.25 (2000). Convictions in the United States or abroad can support this type of denial, and the parties may be collaterally estopped from challenging the facts in any subsequent proceedings. *See, e.g.*, Spawr Optical Research, Inc. v. Baldrige, 649 F. Supp. 1366 (D.D.C. 1986); Action Affecting Export Privileges: Japan Aviation Electronics Industry, 57 Fed. Reg. 9,533-03 (Mar. 19, 1992); In re Export Privileges; Ahlberg, 55 Fed. Reg. 8,504 (Mar. 8, 1990). This type of denial order may not exceed ten years in duration.

48. *See* Bureau of Export Administration, *The List of Denied Persons, at* http://www.bxa.doc.gov/dpl/2_denial.htm (visited Oct. 22, 2000).

49. *See id.*

If Walmart.com contracts to deliver goods to Franco's associates in Europe, it is engaged in an export-related transaction with a denied party. Walmart.com accordingly risks having its own export privileges denied. If that were to occur, Walmart.com would lose its ability to "order, buy, sell, use, receive, deliver, store, dispose of, service, transport finance, or forward" U.S.-origin goods or technology in any export-related transaction.[50] The proposed deliveries to Franco's New Jersey offices would appear to be entirely domestic, outside the ambit of the government's export controls, and therefore free from this risk. However, if Walmart.com has any "reason to know" the goods are not going to remain in the United States, it might still be sanctioned for acting with knowledge of a violation because Franco—as a blacklisted party—is known to be precluded from involvement in any legitimate export-related transactions.[51] Thus, these export-related controls can also impact what might otherwise be considered as domestic business dealings. It also highlights that, given the global nature of e-commerce, almost any transaction has the potential to be export-related and subject to the Commerce Department's regulatory controls.[52]

The process at the State Department for imposing administrative sanctions under ITAR has a similar effect, but is handled slightly differently and results in debarring persons or organizations from exporting or receiving goods or technology regulated by ITAR.[53] The Director of DTC may order parties debarred following administrative hearings[54] or upon conviction of violating any of the trade-related laws,[55] including the EAA, IEEPA, and TWEA.[56] When it is "reasonably necessary to protect world peace or the security or foreign policy of the United States," the DTC also has the ability to temporarily suspend ITAR privileges.[57] Debarment remains, however, like the Commerce denial order, primarily a

50. *See supra* note 44 and accompanying text.

51. 15 C.F.R. § 764.2(e) (2000), which states:

> No person may order, buy, remove, conceal, store, use, sell, loan, dispose of, transfer, transport, finance, forward, or otherwise service, in whole or in part, any item exported or to be exported from the United States, or that is otherwise subject to the EAR, with knowledge that a violation of the EEA, the EAR, or any order, license, or authorization issued thereunder, has occurred, is about to occur, or is intended to occur in connection with the item.

See also Causing aiding or abetting a violation, 15 C.F.R. § 764.2(b); Coverage of more than exports § 730.5 (2000).

52. If an impermissible export-related transaction occurs, with a denied party like Rolando Franco for example, the question would then be whether the e-business was in a position to demonstrate a negative proposition to government investigators—that it did not have "reason to know" it was involved in an export-related transaction—in order to avoid liability under 15 C.F.R. § 764.2(e) (2000). *See also infra* note 157 and accompanying text (addressing the notion of "deemed exports").

53. DTC's debarment authority is embodied in 22 C.F.R. § 127.7 (2000). The typical duration for a debarment is three years. *See id.* § 127.7(a).

54. This is referred to as administrative debarment. *See id.* §§ 127.7(b)(2), 128.10. Administrative debarment orders are effective until rescinded.

55. This is referred to as statutory debarment. *See id.* § 127.7(c). It is roughly analogous to Commerce's collateral sanction provision. 15 C.F.R. § 766.25 (2000); *see supra* note 48. The standard duration for a statutory debarment is three years, but exporting privileges are not automatically reinstated. The statutorily debarred party may be required to apply for reinstatement. *See* 22 C.F.R. § 127.10(b)(2) (2000).

56. *See* 22 C.F.R. §§ 120.27, 127.7 (2000).

57. *Id.* § 127.8. This interim suspension cannot exceed sixty days unless other proceedings are instituted. *See id.* § 127.8(a).

sanction for violating the regulatory requirements of the State Department's trade controls.[58] Ninety-nine parties are currently blacklisted on the Debarred List.[59]

The Enhanced Proliferation Control Initiative (EPCI), announced by President Bush in 1990, greatly expanded the role of blacklisting in U.S. trade controls and also marked a fundamental shift in focus of the traditional export control system.[60] Export licensing controls on specific products were de-emphasized in favor of a much greater focus on controlling the behavior of parties subject to U.S. jurisdiction and their dealings with their customers and trading partners. The EPCI nonproliferation initiative added new obligations to the product-oriented trade control system that focus upon what exporters and vendors "know" about the parties with whom they are dealing, and what these parties will do with the products they acquire.[61] The EPCI regulations make the export of virtually any item a licensable transaction, if it involves a "bad" customer or a "bad" end-use by an otherwise acceptable customer.[62] Since presumably exporters will know more about what will be done with the goods and services they sell than any licensing official could ever know, the government effectively shifted the decision about what was a permissible or impermissible transaction on to the exporters themselves. Thus, it is the exporters' knowledge of their customer and their customers' activities that triggers EPCI licensing controls, not the government's decision to place an item on the control list.

The government created a new form of blacklisting to augment these EPCI nonproliferation controls on transactions with suspect end-uses or end-users. By naming a party like the Baltic State Technical University to the Entities List, the government affirmatively conveys the knowledge that the blacklisted individual or organization is involved in the weapons proliferation activities required to trigger the controls.[63] Accordingly, shipping Dell Computers to the blacklisted University requires a government license approval, even if exporting the same computers to some other customer would not.[64] If the necessary approval is not obtained in advance, Dell risks being administratively added to the DPL

58. It should be noted that the same term, "debarment," is also used to refer to companies who have lost their contracting rights with the federal government. *See* 48 C.F.R. § 9.400 (2000). This in and of itself is grounds for being debarred by DTC. *See* 22 C.F.R. § 126.7(a)(5) (2000).

59. Office of Defense Trade Controls, *List of Debarred Parties*, *at* http://www.pmdtc.org/debar059.htm (visited Oct. 30, 2000).

60. *See* Exec. Order No. 12,735, 55 Fed. Reg. 48,587 (Nov. 16, 1990).

61. EPCI also imposed a series of product-specific controls on the actual weapons of mass destruction. *See, for example*, the Commerce controls on chemical precursors that are useful in constructing chemical weapons, 15 C.F.R. § 742.2(a)(2) (2000); Biological agents and viroids, *id.* § 742.2(a)(1); chemical/biological weapons production equipment, *id.* § 742.2(a)(3); missile related equipment and technology, *id.* § 742.5; specified nuclear related items, *id.* § 742.3; the Energy Department controls on nuclear power generation equipment, 10 C.F.R. § 110 (2000); and the State Department controls on actual weaponry such as toxicological agents, United States Munitions List, 22 C.F.R. § 121.1 (2000); Category XIV, and its Missile Technology Control Regime Annex, *id.* § 121.6.

62. This is neatly stated in *General Prohibition Five—Export or Reexport to Prohibited End-Uses or End-Users* stating: "You may not, without a license, knowingly export or reexport any item subject to the EAR to an end user or end use that is prohibited by part 744 of the EAR." 15 C.F.R. § 736.2(b)(5) (2000).

63. Additionally, the government sometimes designates an entire country or area as presenting a high risk for proliferation-related activities, rather than identifying particular persons or organizations, thereby triggering the controls on a large scale. *See, for example*, the destinations of concern for the Missile Technology Control Regime for country group D:4, 15 C.F.R. § 740 supp. 1 (2000), the destinations of concern for chemical and biological weapons proliferation for country group D:3, *id.*, and the Nuclear Nonproliferation Special Country List for country group D:2, *id.* While significant from a trade control perspective, this type of designation is not the sort of particularized blacklisting with which this article is concerned.

64. *See id.* §§ 736.2(b)(4)-(5), 744.1(c).

for its violation—denying Dell access to U.S. goods and technology for any export-related transactions—with disastrous consequences to its business.[65]

In contrast to those listed on the Debarred List or the DPL, however, parties named on the Entities List may not have engaged in any illegal conduct themselves. To the contrary, the activities that cause the U.S. government concern might well be entirely legal where they are performed and even actively encouraged by the local governments. These individuals and organizations are not sanctioned for violating U.S. regulations they are blacklisted solely because their activities are contrary to the U.S. government's policies regarding the potential spread of technologies associated with weapons of mass destruction.[66] There are currently 118 major entries on the Entities List, along with several hundred related companies or parties.[67]

This use of blacklisting under the EPCI reflects the U.S. government's desire to extend the reach of its trade controls to influence or coerce behavior of those beyond the direct reach of its jurisdiction. Accordingly, blacklisting by the government's trade control agencies has progressed from simply being one of several tools used to ensure compliance with their traditional requirements and punish those who violate their rules, to being a significant part of entirely new controls being formulated by policy makers to address new concerns. In doing so the BXA actually imported some of the techniques developed by OFAC in its financial and economic sanctions programs into the traditionally commodity-oriented world of trade controls.

B. Governmental Blacklists in U.S. Economic Sanctions Programs[68]

Since the end of World War II, the United States has imposed economic sanctions under the authority of the TWEA[69] targeted at China (1950-1971),[70] North Korea (1950-present),[71] Cuba (1963-present),[72] North Vietnam (1964-1994),[73] South Vietnam (1975-

65. *See supra* notes 42-47 and accompanying text.

66. *See* Fitzgerald, *supra* note 36, at 33-35.

67. 15 C.F.R. pt. 744, Supp. No. 4 (2000); *see also* Bureau of Export Administration, *The Entity List, at* http://www.bxa.doc.gov/Entities/Default.htm (visited Dec. 12, 2000).

68. *See generally* Fitzgerald, *supra* note 25, at 90-98.

69. 50 U.S.C. app. § 1 (1994).

70. *See* Foreign Asset Control Regulations, 15 Fed. Reg. 9,040 (Dec. 19, 1950). The embargo was effectively lifted in 1971 in connection with President Nixon's visit to China, although residual controls remained in place until outstanding claims were settled in 1980. *See* Relaxation of Controls, 36 Fed. Reg. 8,584 (Mar. 7, 1971); Relaxation of Controls, 36 Fed. Reg. 11,441 (June 12, 1971); Unblocking of Assets, 45 Fed. Reg. 7,224, (Jan. 31, 1980). *See generally* Gary Clyde Hufbauer et al., Economic Sanctions Reconsidered: Supplemental Case Histories, 100-09 (2d ed. 1990).

71. *See* Foreign Asset Control Regulations, 15 Fed. Reg. 9,040 (Dec. 19, 1950); 31 C.F.R. § 500 (2000). *See generally* Hufbauer, *supra* note 70, at 110-14. On September 17, 1999, the president announced that the sanctions on North Korea would be loosened in the near future. *See* Office of Foreign Assets Controls, *What's New, Appendix A, at* http://www.ustreas.gov/ofac/t11edit.txt (visited Sept. 20, 1999). On June 19, 2000, 31 C.F.R. §§ 500.533 and 500.586 were amended to relinquish OFAC's control over exports to North Korea and to authorize certain limited transaction in accordance with President Clinton's September 17, 1999, announcement. *See* 65 Fed. Reg. 38,165 (June 19, 2000).

72. Cuban Assets Control Regulations, 31 C.F.R. § 515 (2000). A variety of controls were applied to Cuba beginning in 1960 as a result of the nationalization and expropriation of various properties. Initially, these took the form of restrictions on various exports to and imports from Cuba. The full embargo was imposed following the Cuban missile crisis. *See* Cuban Assets Control Regulations, 28 Fed. Reg. 6,974 (July 9, 1963). *See generally* Hufbauer, *supra* note 70, at 194-204.

73. *See* OFAC Statement of Organization, 29 Fed. Reg. 6,025 (May 5, 1964). The Vietnamese embargo was prospectively lifted in 1994 by Prospective Lifting of Vietnam Embargo, 59 Fed. Reg. 5,696 (Feb. 7, 1994),

1994),[74] and Cambodia (1975-1992).[75] More recently, the IEEPA[76] has provided the primary legislative basis[77] for economic sanctions directed against Iran (1979-present),[78] South Africa (1985-1991),[79] Namibia (1985-1990),[80] Nicaragua (1985-1990),[81] Libya

and completely removed upon settlement of outstanding claims the following year by Unblocking of Vietnamese Assets, 60 Fed. Reg. 12,885 (Mar. 9, 1995). *See generally* HUFBAUER, *supra* note 70, at 133-41.

74. *See supra* note 73. The embargo of North Vietnam was extended to the entire country with the fall of South Vietnam in 1975. *See* Blocking Extended to South Vietnam, 40 Fed. Reg. 19,202 (May 2, 1975).

75. *See* Blocking Controls on Cambodia, 40 Fed. Reg. 17,262 (Apr. 18, 1975). The embargo of Cambodia was prospectively lifted in 1992 by 57 Fed. Reg. 1,872-01 (Jan. 16, 1992), and completely removed in 1994 by Unblocking of Cambodian Assets, 59 Fed. Reg. 60,558 (Nov. 25, 1994). *See generally* HUFBAUER, *supra* note 70, at 412-16.

76. 50 U.S.C. § 1701 (1994).

77. Other statutes have also supported the imposition of economic sanctions. For example, the United Nations Participation Act of 1945, 22 U.S.C. § 287c (1994), mandates the imposition of sanctions in accordance with decisions of the Security Council under article 41 of the U.N. Charter. This was used to impose financial and trade restrictions on Rhodesia when Ian Smith's white-minority government unilaterally declared its independence from the United Kingdom in 1965 thereby thwarting steps towards self-determination in Southern Rhodesia. The Rhodesian Sanctions, 31 C.F.R. § 530 (1972), were prospectively lifted upon the accession of majority rule and the creation of Zimbabwe in 1979 by Exec. Order No. 12,183, 44 Fed. Reg. 74,787 (Dec. 16, 1979), and entirely removed in 1992 by 57 Fed. Reg. 1,386 (Jan. 14, 1992). *See generally* HUFBAUER, *supra* note 70, at 285-93. Since the time of the Rhodesian sanctions, the more common practice has been to predicate the imposition of sanctions on multiple pieces of legislation. For example, both IEEPA and the UN Participation Act were used for the programs aimed at Iraq and Kuwait. *See infra* notes 84-85; Haiti, *infra* note 86; the former Yugoslavia, *infra* note 87; and Angola, *infra* note 88. IEEPA and the International Security Development and Cooperation Act of 1985, 22 U.S.C. § 2349aa-9 (1994), together support the sanctions on Libya, *see infra* note 82, and the second round of sanctions aimed at Iran, *see infra* note 78; and the Comprehensive Anti-Apartheid Act of 1986 bolstered the IEEPA based sanctions on South Africa, *infra* note 79. The sanctions programs targeted at the Terrorism List Governments, *infra* note 94, and Foreign Terrorist Organizations, *infra* note 95, are predicated solely upon the Antiterrorism and Effective Death Penalty Act of 1996, rather than jointly with IEEPA. The only IEEPA-based terrorist sanctions are those aimed at organizations threatening the Middle East peace process. *See infra* note 93.

78. *See* Iranian Assets Control Regulations (IACR), 44 Fed. Reg. 65,956 (Nov. 15, 1979); 31 C.F.R. § 535 (2000). Most of the IACR controls were prospectively lifted in 1981. *See* Exec. Order No. 12,283, 46 Fed. Reg. 7,927 (Jan. 18, 1981); 31 C.F.R. § 535.579 (2000). Iran is also subject to further sanctions under the Iranian Transaction Regulations, (ITR), 31 C.F.R. § 560 (2000), which now have greater impact than the IACR. *See generally* GARY CLYDE HUFBAUER ET AL., ECONOMIC SANCTIONS RECONSIDERED: HISTORY AND CURRENT POLICY 153-62 (2d ed. 1990).

79. *See* Exec. Order No. 12,532, 50 Fed. Reg. 36,861 (Sept. 9, 1985). The South African Transaction Regulations (SATR), 31 C.F.R. § 545 (1986), were initially imposed in an effort to head off more sweeping sanctions then being proposed by Congress. The 1985 controls were substantially modified and broadened the following year, in accordance with the Congressionally-mandated program of sanctions found in the Comprehensive Anti-Apartheid Act (CAAA) of 1986, Pub. L. No. 99-440, 10 Stat. 1086 (1986). *See also* Exec. Order No. 12,571, 51 Fed. Reg. 39,505 (Oct. 27, 1986); 51 Fed. Reg. 41,906 (Nov. 19, 1986); 51 Fed. Reg. 46,853 (Nov. 19, 1986). The SATR were prospectively lifted in 1991, 56 Fed. Reg. 32,056 (July 12, 1991), and the last remaining restrictions affecting dealings in gold coins were removed in 1995. *See* Foreign Funds Control Regulations, 60 Fed. Reg. 33,725 (June 29, 1995). *See generally* HUFBAUER, *supra* note 78, at 221-48.

80. Namibia, as part of South Africa, was initially caught in the sanctions that were aimed at dealings with the government of South Africa. It was removed from the scope of the SATR in March 1990 following Namibian independence. *See* SATR, 55 Fed. Reg. 10,618 (Mar. 22, 1990).

81. *See* Exec. Order No. 12,513, 50 Fed. Reg. 18,629 (May 1, 1985). The Nicaraguan Transaction Control Regulations (NTCR), 50 Fed. Reg. 19,890 (May 10, 1985), 31 C.F.R. § 540 (1986), were imposed as part of the Reagan Administration's opposition to the Sandinista Government of President Daniel Ortega. They were lifted prospectively following the election of the Chamorro Government in 1990, 55 Fed. Reg. 28,613 (July 12, 1990), and removed entirely in 1995, 60 Fed. Reg. 33,725 (June 29, 1995). *See generally* HUFBAUER, *supra* note 78, at 175-91.

(1986-present),[82] Panama (1988-1990),[83] Iraq (1990-present),[84] Kuwait (1990-1991),[85] Haiti (1991-1994),[86] the former Yugoslavia (1992-1996, 1998-present),[87] Angola (1993-

82. After a series of terrorist incidents, President Reagan invoked IEEPA to impose a broad trade and financial embargo of Libya. Additional authority for the President's actions was predicated upon the International Security and Development Cooperation Act of 1985, 22 U.S.C. §§ 2349aa-8,-9 (1994), which would be used the following year to support the ITR, *supra* note 78, as well as the Federal Aviation Act, 49 U.S.C. § 40,106 (1994). Two Executive Orders were issued in quick succession in January of 1986, Exec. Order No. 12,543, 51 Fed. Reg. 875 (Jan. 7, 1986) and Exec. Order No. 12,544, 51 Fed. Reg. 1235 (Jan. 8, 1986), which provided the basis for the Libyan Sanctions Regulations, 31 C.F.R. § 550 (2000). Additional restrictions on investing more than $40 million in the development of Libyan petroleum resources in any twelve-month period were imposed with the Iran and Libya Sanctions Act of 1996. *See* Pub. L. 104-72, 110 Stat. 541 (1996) (codified at 50 U.S.C. § 1701, note); HUFBAUER, *supra* note 78, at 140-52.

83. *See* Exec. Order No. 12,635, 53 Fed. Reg. 12,134 (Apr. 8, 1988). The Panamanian Transaction Regulations (PTR) were imposed as part of the Reagan Administration's efforts to isolate and undermine the regime headed by General Manuel Noriega because of involvement with drug trafficking. Panamanian Transactions Regulations, 53 Fed. Reg. 20,566 (June 3, 1988); 31 C.F.R.§ 565 (1988). The PTR were lifted prospectively in 1990 following the U.S. incursion that removed General Noriega from power, 55 Fed. Reg. 3,560 (Feb. 1, 1990), and removed entirely in 1995, 60 Fed. Reg. 33,725-02 (June 29, 1995). *See generally* HUFBAUER, *supra* note 78, at 249-67.

84. When Iraq invaded Kuwait on August 2, 1990, President Bush issued two Executive Orders, one restricting imports and exports to Iraq and blocking Iraqi government property, Exec. Order No. 12,722, 55 Fed. Reg. 31,803 (Aug. 2, 1990), and another blocking Kuwaiti government property as a protective measure to limit looting by Iraq, Exec. Order 12,723, 55 Fed. Reg. 31,805 (Aug. 2, 1990). The U.S. sanctions were brought completely into line with the related U.N. actions by Executive Order Number 12,724 with regard to Iraq, see 55 Fed. Reg. 33,089 (Aug. 9, 1990), and Number 12,725 with regard to Kuwait, see 55 Fed. Reg. 33,091 (Aug. 9, 1990), thereby grounding the controls both in IEEPA and the UN Participation Act, 22 U.S.C. § 287c. The Iraqi Sanctions Regulations, 56 Fed. Reg. 2,112 (Jan. 18, 1991); 31 C.F.R. § 575 (2000), and the separate but related Kuwaiti Assets Control Regulations, 55 Fed. Reg. 49,856 (Nov. 30, 1990); 31 C.F.R. § 570 (1991), utilize the full range of sanctions tools available to the government in a manner not seen since the TWEA-based FACR and CACR. *See* MICHAEL P. MALLOY, ECONOMIC SANCTIONS AND U.S. TRADE § 9A.2.1 (Supp. 1996). Following the liberation of Kuwait, the KACR were prospectively lifted in 1991, 56 Fed. Reg. 12,450-01 (Mar. 26, 1991), and entirely removed in 1995 by 60 Fed. Reg. 33,725-02 (June 29, 1995). The ISR remain in effect.

85. *See supra* note 84.

86. *See* Exec. Order No. 12,775, 56 Fed. Reg. 50,641 (Oct. 4, 1991); *see also* Exec. Order No. 12,779, 56 Fed. Reg. 55,975 (Oct. 28, 1991). The OFAC Haitian Transaction Regulations, 31 C.F.R. § 580 (1993), which embodied the controls created by the Executive Orders, were issued in March 1992. *See* 57 Fed. Reg. 10,820 (Mar. 31, 1992). When the democratically-elected President Aristide returned to Haiti, the sanctions were first suspended, see Exec. Order No. 12,932, 59 Fed. Reg. 52,403 (Oct. 14, 1994); 59 Fed. Reg. 51,066 (Oct. 6, 1994), and then finally removed in June 1995. *See* 60 Fed. Reg. 33,725 (June 29, 1995).

87. Exec. Order No. 12,808, 57 Fed. Reg. 23,299 (May 30, 1992), was issued following the breakup of Yugoslavia, blocking property of the governments of Serbia and Montenegro (the "Federal Republic of Yugoslavia" or FRY) when their troops seized territory within Croatia and Bosnia-Herzegovina. Exec. Order No. 12,810, 57 Fed. Reg. 24,347 (June 5, 1992), imposed additional controls to limit trade, and Exec. Order No. 12,831, 58 Fed. Reg. 5,253 (Jan. 15, 1993), which expanded the blocking measures to companies and FRY-controlled entities, brought the U.S. sanctions in line with the U.N. measures. *See* Exec. Order No. 12,846, 58 Fed. Reg. 25,771 (Apr. 25, 1993); *see also* Exec. Order No. 12,934, 59 Fed. Reg. 54,117 (Oct. 25, 1994). The blocking measures directed at Serbia and Montenegro were prospectively lifted in January 1996 as a result of the Dayton Peace Accords, 61 Fed. Reg. 1282 (Jan. 19, 1996); 31 C.F.R. § 585.525 (2000)), but were not similarly lifted for the Serbian-controlled areas of Bosnia until May. 61 Fed. Reg. 24,697 (May 16, 1996); 31 C.F.R. § 585.527 (2000), when the Serb forces withdrew. Sanctions were then re-imposed in 1998 because of Serbian actions in Kosovo. *See* Exec. Order No. 13,088, 63 Fed. Reg. 32,109 (June 9, 1998); 31 C.F.R. § 586 (2000). Following the recent elections, a new licensing policy was adopted in October 2000. *See* Office of Foreign Assets Control, *Statement of Licensing Policy Relating to the Federal Republic of Yugoslavia (Serbia and Montenegro)*, *available at* http://www.ustreas.gov/ofac/bulletin.txt (visited Dec. 12, 2000).

present),[88] Colombia (1995-present),[89] Burma (1997-present),[90] Sudan (1997-present),[91] and Afghanistan (1999-present).[92] Additionally, the U.S. government recently created several more programs that are not necessarily tied to any one specific country, imposing economic sanctions on Middle Eastern terrorists (1995-present),[93] governments that support terrorism (1996-present),[94] foreign terrorist organizations (1997-present),[95] those engaged in the proliferation of weapons of mass destruction (1998-present),[96] and most recently, those engaged in narcotics trafficking (2000-present).[97]

88. Sanctions were initially imposed only on dealings with National Union for the Total Independence of Angola (UNITA), and later expanded. *See* Exec. Order No. 12,865, 58 Fed. Reg. 51,005 (Sept. 26, 1993); Exec. Order No. 13,069, 62 Fed. Reg. 65,989 (Dec. 12, 1997); Exec. Order No. 13,098, 63 Fed. Reg. 44,471 (Aug. 19, 1998). The UNITA (Angola) Sanctions Regulations (UASR) essentially block assets of those affiliated with UNITA and impose an arms embargo and prohibit actions that facilitate the sale of arms or petroleum products to UNITA or Angola. *See* 58 Fed. Reg. 64,904 (Dec. 10, 1993). However, Executive Order Number 13,098 required so many changes to the details of the regulations that the UASR were entirely reissued in August 1999. *See* 64 Fed. Reg. 43,924 (Aug. 12, 1999); 31 C.F.R. § 590 (2000).

89. *See* Exec. Order No. 12,978, 60 Fed. Reg. 54,579 (Oct. 21, 1995). The IEEPA-based Narcotics Trafficking Sanctions Regulations (NTSR) was created in March 1997. *See* 31 C.F.R. § 536 (2000). These sanctions are primarily targeted at the Cali Cartel, unlike the broader scope of the recent Kingpin Act sanctions. *See infra* note 97 and accompanying text.

90. The Government of Burma, or Myanmar, was sanctioned in May 1997 for its "large-scale repression of the democratic opposition" by the imposition of a prohibition on any new investment in the country with the Burmese Sanctions Regulations (BSR). *See* Exec. Order No. 13,047, 62 Fed. Reg. 28,301 (May 20, 1997); *see also* 63 Fed. Reg. 27,846 (May 21, 1998); Burmese Sanctions Regulations, 31 C.F.R. § 537 (2000).

91. The government of Sudan was sanctioned in November 1997 for its support of terrorism, efforts to destabilize its neighbors, and for human-rights violations within Sudan. *See* Exec. Order No. 13,067, 62 Fed. Reg. 59,989 (Nov. 3, 1997). The Sudanese Sanctions Regulations (SSR) are found at 31 C.F.R § 538 (2000).

92. Sanctions were imposed on dealing with the Taliban in Afghanistan on July 6, 1999. *See* Exec. Order No. 13,129, 64 Fed. Reg. 36,759 (July 4, 1999); Taliban (Afghanistan) Sanctions Regulations (TASR), 66 Fed. Reg. 2,726-41 (Jan. 11, 2001) (to be codified at 31 C.F.R. § 545).

93. In January 1995, sanctions were imposed that prohibit dealings with designated terrorists and terrorist organizations deemed to pose a threat to the Middle East peace process. Exec. Order No. 12,947, 60 Fed. Reg. 5,079 (Jan. 23, 1995). The Terrorism Sanctions Regulations (TSR) were created in February 1996. 61 Fed. Reg. 3,805 (1996), 31 C.F.R. § 595 (2000). The sanctions programs targeted at the Terrorism List Governments, see *infra* note 94, and Foreign Terrorist Organizations, see *infra* note 95, are predicated upon the Antiterrorism and Effective Death Penalty Act of 1996, rather than IEEPA.

94. The Terrorism List Governments Sanctions Regulations (TLGSR), 31 C.F.R. § 596 (2000), and the Foreign Terrorist Organizations Sanctions Regulations (FTOSR), 31 C.F.R. § 597 (2000), are unusual among the recent sanctions programs in that they are not predicated upon IEEPA. The TLGSR were issued under the authority of section 321 of the Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, §§ 302-03, 110 Stat. 1214, 1248-53 (1996), and prohibit unlicensed financial dealings with any government designated by the Secretary of State as supporting terrorism pursuant to section 6(j) of the Export Administration Act, 50 U.S.C. app. § 2405 (1994). This currently affects dealings with Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. *See* 31 C.F.R. § 596.201 (2000). All, except Syria, however, are countries that are already affected by other OFAC sanctions programs.

95. The Foreign Terrorist Organization Sanctions Regulations (FTOSR), 31 C.F.R.§ 597 (2000), like the TLGSR, 31 C.F.R. § 596 (2000), are not predicated upon IEEPA. The FTOSR were issued under the authority of sections 302-03 of the Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. 104-132 at §§ 302-03, 110 Stat. at 1248-52 (1996), and prohibit providing material support or resources to designated terrorist organizations and also require blocking the assets of such organizations.

96. Certain persons engaged in weapons proliferation are subject to an import ban. Initially established in 1998 by Executive Order Number 13,094, 63 Fed. Reg. 40,803 (July 23, 1998), the ban was implemented with the Weapons of Mass Destruction Trade Control Regulations (WMDTCR), 31 C.F.R. § 539 (2000).

97. Although the Foreign Narcotics Kingpin Act was enacted in late 1999, 21 U.S.C. § 1902, Pub. L. No. 106-120, §§ 801-11, Intelligence Authorization Act for Fiscal Year 2000, 113 Stat. 1606, 1626-36 (1999), it

Apart from the various Asian sanctions, which were administered with a single common set of regulations,[98] the government created entirely new and separate stand-alone regulations for each of these various sanctions programs.[99] Nevertheless, virtually every one of these programs employs some sort of blacklist tool.[100] The OFAC blacklists were traditionally used to expand the scope of the sanctions beyond a particular target destination, to reach third parties and corporate cloaks operating outside the sanctioned country.[101] OFAC effectively deems these blacklisted parties to be agents, for all purposes, or nationals of the sanctioned target. Therefore, dealings with blacklisted parties are the same as direct dealings with the sanctioned destination.[102] Thus, for example, in declaring Pierre Boileau to be a "specially designated national" of Cuba, OFAC is attempting to bring indirect dealings with a Cuban intermediary within the ambit of its prohibitions on direct dealings with Cuba.[103]

The terminology associated with each programs' blacklist vary however, as the government slightly restructures the basic sanctions mechanisms each time it drafts a new program. A confusing array of different terms, such as "specially designated,"[104] "controlled,"[105] "blocked,"[106] or "governmental"[107] persons or entities, is employed in conjunction with the blacklists used for the various programs. The purpose of the blacklist within each program, however, remains unaltered—to extend the reach of the sanctions beyond just the geography associated with a target country to reach transactions involving specific individuals or organizations wherever they may be located.

In several of the newer programs, specific parties or organizations are blacklisted arguably without any direct connection to any particular state or geography whatsoever.[108] In the narco-trafficking, terrorist, and weapons proliferation programs, blacklisting is no longer employed as a secondary tool to reach the activities of corporate cloaks or third parties that might enable a targeted country to avoid the effects of the sanctions. Rather, in these programs, blacklisting is now employed as the primary tool for achieving the government's objectives. The government's objectives have also shifted—from isolating the sanctioned territory as a prelude or alternative to war—to demonstrating political leadership or claiming the moral high ground for political purposes, with considerably less concern for whether the sanctions will actually affect the actions of their intended target. That is, blacklisting is increasingly employed not for foreign policy purposes but in an attempt to address some of the more intractable political problems facing policy makers today, such as human rights

was not until June 1, 2000, that the president used the statute's authority to issue his initial blacklist designations. *See* Office of Foreign Assets Control, *What You Need to Know About U.S. Sanctions Against Drug Traffickers, available at* http://www.ustreas.gov/ofac/t11drugs.pdf (visited Aug. 11, 2000). The controls were implemented with the Foreign Narcotics Kingpin Sanctions Regulations (FNKSR), 65 Fed. Reg. 41,334 (July 5, 2000) (to be codified at 31 C.F.R. § 598).

98. The embargoes of China, Vietnam, and Cambodia were all administered by OFAC under the FACR, as is the current embargo of North Korea. *See supra* notes 70-71, 73-75 and accompanying text.

99. *See supra* notes 72, 78-97 and accompanying text.

100. Only the Burma program lacks a clear blacklist tool as part of its sanctions. *See supra* note 90.

101. *See* Fitzgerald, *supra* note 25, at 83.

102. *See id.*

103. *See id.*; *see also supra* notes 26-27 and accompanying text.

104. *See* Fitzgerald, *supra* note 25, at 98-99

105. *See id.* at 99-102.

106. *See id.* at 100-03.

107. *See id.* at 103-06.

108. *See supra* notes 93-97; *see also* Fitzgerald, *supra* note 36, at 27-28.

violations, terrorism, and matters of outright illegality, such as narco-trafficking.[109] There are currently over 4,800 parties blacklisted under one or more of OFAC's various programs.[110]

C. Application of Blacklists Abroad: Foreign Branches and Subsidiaries[111]

Seeking to influence the behavior of others beyond the reach of U.S. jurisdiction, through either leadership or coercion, is one of the basic functions of both the various OFAC blacklists and the BXA Entities List. The government seeks to influence the decisions of those beyond its reach by controlling the behavior of those within the United States and, in an effort to bring as much pressure to bear as possible, U.S. affiliated parties abroad as well. This raises the question of whether parties outside the United States can be required to adhere to U.S. economic sanctions or trade controls, which may have no counterpart in the local laws where they are operating.

Clearly, U.S. nationals and companies are fully obligated to follow U.S. laws and regulations, whether operating in the United States or abroad.[112] More significantly, however, the United States sometimes regards foreign companies or juridical entities as being subject to requirements of U.S. sanctions programs. OFAC's older, TWEA-based sanctions programs on Cuba and North Korea, in particular, are specifically designed to reach to the farthest possible limits[113] of U.S. legislative or prescriptive jurisdic-

109. *See* Fitzgerald, *supra* note 36, at 27-28.

110. The most recent publication of the consolidated OFAC blacklist on OFAC's website lists over 4,800 separate entries, many with multiple aliases or addresses. Of these, approximately 474 individuals or entities are identified as Cuban Specially Designated Nationals (SDN) and vessels; 662 as Libyan SDNs; seven as North Korean SDNs; 410 as Iraqi SDNs and vessels; 141 are blocked as affiliated with the Sudanese Government; 17 are blocked as affiliated with the Taliban; 26 are blocked as affiliated with UNITA in Angola; 1,117 are blocked as affiliated with the Federal Republic of Yugoslavia under the Kosovo sanctions; 156 are Specially Designated Terrorists (SDT) and 134 are Foreign Terrorist Organizations (FTO) [and 87 of those bear a dual SDT-FTO designation]; 659 are Colombian narcotics traffickers (SDNTs); and 56 are designated as SDNTKs under the Drug Kingpin Act sanctions; additionally, 20 Iranian controlled banks are listed, along with 859 SDNs under the FRY (S&M) sanctions and 87 SRBHs under the Bosnian sanctions even though those programs are currently suspended. *See* Office of Foreign Assets Control, *Specially Designated Nationals and Blocked Persons* (Dec. 7, 2000), *available at* http://www.ustreas.gov/ofac/t11sdn.pdf. This does not include the Designated Foreign Parties (DFP) sanctioned under the WMDTCR and identified in 31 C.F.R. § 539, app. I (2000), or the Terrorism List Governments sanctioned under the TLGSR and identified in 31 C.F.R. § 596.201 (2000). *See supra* notes 94-96, and accompanying text.

111. *See generally* Fitzgerald, *supra* note 36, at 35-41, 61-70.

112. International law, as reflected in the Restatement of Foreign Relations Law, generally recognizes four bases for a state's "jurisdiction to prescribe," all of which are subject to a reasonableness limitation. These overlapping bases are: the territorial principle (a state may proscribe activity occurring within its boundaries); the effects principle (a state may proscribe activity having an effect within its territory); the nationality principle (a state may proscribe activities of its nationals, wherever located); and the security principle (a state may proscribe activities affecting its national security). Regulating the activity of citizens, residents, or companies formed under a state's laws would be a classic application of the nationality principle supporting jurisdiction to proscribe. *See* Restatement (Third) of Foreign Relations Law of the United States §§ 402-03 (1987).

113. For example, the basic prohibitions in the CACR extend to all dealings, direct or indirect, between Cuba, Cuban nationals, or Cuban SDNs, and "any person (including a banking institution) subject to the jurisdiction of the United States." 31 C.F.R. §§ 515.201(a)(1), (b)(1) (2000). The prohibitions also extend to "any property or property interest subject to the jurisdiction of the United States" in which Cuba, Cuban Nationals, or Cuban SDNs have or had "any interest of any nature whatsoever, direct or indirect." *Id.* at §§ 515.201(b)(2), 500.201(b). The basic prohibitions in the FACR are similar to the CACR. *Compare* 31 C.F.R. §§ 515.201(a), (b), *with* 31 C.F.R. §§ 500.201(a), (b).

tion.[114] By definition, foreign subsidiaries of U.S. companies, or those that are controlled in fact by U.S. nationals or companies, are considered to be "persons subject to the jurisdiction of the United States" and obligated to comply with U.S. sanctions despite being established abroad under foreign laws.[115] Thus, under U.S. law, America Online's subsidiary in Canada is obligated to follow the terms of the U.S. embargo of Cuba.[116]

Given the wartime origins of TWEA and the circumstances that were historically associated with the use of economic sanctions, broadly requiring U.S.-affiliated parties outside the country to support and follow such sanctions, makes sense and is a necessary corollary to an effective set of controls.[117] In fact, the regulatory definition that brings controlled foreign subsidiaries within the scope of "persons subject to the jurisdiction of the United States"[118] is directly traceable to a Treasury Department notice issued during the early months of World War II.[119] Nevertheless, the legitimate, reasonable use of such a broad claim of regulatory power was recognized as being confined to unusual circumstances.

Blacklisting is very easy to employ and very amenable to targeting specific parties abroad who might otherwise be beyond the reach of U.S. processes, which makes it an attractive tool for policy makers and regulators. The government merely needs to add individuals and organizations to a list in order to have control and be seen as acting on an issue. The risk is that overuse of extraterritorial sanctions generates conflict with other governments who perceive the U.S. rules as impinging on their own jurisdiction and sovereign interests. This is particularly likely to occur when multilateral agreement on the object of the control is lacking.[120]

---

114. The *Restatement of the Foreign Relations Law* conceptually distinguishes, under international law, between a state's power to legislate or proscribe—the "authority of a state to make its substantive laws applicable to particular persons or in particular circumstances"—and its ability actually to enforce those laws. *See* RESTATEMENT OF FOREIGN RELATIONS LAW, *supra* note 112, at § 401. The state's jurisdiction to proscribe is subject only to a reasonableness limitation. *See id.* § 403.

115. The term "person subject to the jurisdiction of the United States" is defined in the CACR to include (1) U.S. citizens and residents; (2) "person[s] within the United States" (which itself is defined in 31 C.F.R. § 515.330 (2000)); (3) corporations organized under the laws of the United States; and (4) "any corporation, partnership, or association, *wherever organized or doing business, that is owned or controlled by*" U.S. citizens, residents, or corporations. 31 C.F.R. § 515.329 (a) (d) (2000) (emphasis added). The same definition appears in the FACR. *See id.* § 500.329.

116. Canada has a different view and opposes the extraterritorial application of U.S. law to Canadian nationals and companies. *See infra* note 120 and accompanying text.

117. *See supra* note 101 and accompanying text; *see also* Fitzgerald, *supra* note 25, at 98-99.

118. TWEA's broad grant of authority to the president to take action with regard to "any person, or with respect to any property, subject to the jurisdiction of the United States" is not further defined within the statute. 50 U.S.C. app. § 5(b)(1)(B) (1994).

119. U.S. Treasury Pub. Circular No. 18, 7 Fed. Reg. 2,503 (Apr. 1, 1942).

120. Naturally, this can present conflict of laws issues, especially if there are local laws or policies that take a different view of the policy objective behind the U.S. sanctions. A number of jurisdictions, such as Canada, Mexico, the United Kingdom, and the European Union, oppose the extraterritorial application of U.S. sanctions on Cuba to their nationals and companies. *See* Fitzgerald, *supra* note 36, at 61-70. Canada, for example, directs Canadian nationals and companies to refrain from cooperating with the U.S. embargo of Cuba and further requires that they also report any and all communications requesting their cooperation or support for the embargo to the Canadian Attorney General. This is embodied in Canada's Foreign Extraterritorial Measures Act of 1985 (FEMA), R.S.C., ch. F-29, §§ 1-11 (1985) (Can.), *reprinted in* 24 I.L.M. 794 [hereinafter FEMA]. As the U.S. policy toward Cuba was tightened, first with the Cuban Democracy Act, and then with the LIBERTAD or Helms-Burton Act, so too FEMA was amended to counter the tougher U.S. policies. FEMA was substantially amended by Bill C-54, which was passed in late 1996, and became effective on January

An increased U.S. sensitivity to the strength and legitimacy of the objections of foreign governments to the assertion of jurisdiction over non-U.S. companies, perhaps albeit com-

1, 1997. *See* An Act to Amend the Foreign Extraterritorial Measures Act, Bill C-54 (1996) (Can.), *reprinted in* 36 I.L.M. 111, at 115-24 (1997). The only Order currently in effect under FEMA specifically evokes its provisions with regard to the U.S. Helms-Burton Act. *See* Schedule to FEMA, 36 I.L.M. at 124 (1997). This is an amended version of the original Order issued in 1992, which triggered FEMA with regard to the Cuban Democracy Act, 22 U.S.C. §§ 6001-10 (1994). *See generally* 24 I.L.M. 794 (1985). Both Orders are predicated upon a Canadian belief that the extraterritorial application of these U.S. laws "adversely affect significant Canadian [trading] interests . . . or . . . infringe[s] Canadian sovereignty." FEMA, § 5. Violations are punishable with fines of up to Can. $1.5 million and terms of imprisonment of up to five years. *See id.* § 7(1)(a). FEMA goes beyond simply prohibiting compliance with extraterritorial laws from other jurisdictions. It is also a "blocking measure," designed to insulate Canadian nationals and companies from foreign attempts to enforce their extraterritorial requirements or penalize their violation. In an effort to limit the clear conflict of law issues that such blocking measures create, FEMA only applies to three types of situations. First, it applies to particular foreign trade laws that are designated as being "contrary to international law or comity." 36 I.L.M at 118. These designations are accomplished by an Order issued by the Canadian Attorney General, after consultation with the Minister of Foreign Affairs, which amends a Schedule of foreign trade laws to which FEMA applies. The Helms-Burton (LIBERTAD) Act is the only trade law that currently appears in the FEMA schedule. *See* FEMA, § 2.1. Second, it applies to situations where a foreign state or tribunal takes actions that adversely affect Canadian interests in international trade and commerce. The Canadian interests in trade or commerce that are adversely affected must be, at least in part, within Canada. *See generally* FEMA, §§ 3, 5, 8. Third, it applies to situations where a foreign state or tribunal takes actions that adversely affect Canadian sovereignty. *See id.* The basic prohibition on Canadian residents, nationals, and companies complying with designated foreign trade laws or measures is found in a provision that states that the Canadian Attorney General may "prohibit any person in Canada from complying with such measures, or with any directives, instructions, "intimations of policy" or other communications relating to such measures from a person who is in a position to direct or influence the policies of the person in Canada." *Id.* § 5(1)(b). A variety of different blocking techniques are then employed to augment the basic prohibition on complying with offensive foreign laws. First, there is the reporting requirement, which presumably permits the Canadian government to both monitor attempts to compel enforcement of extraterritorial measures within Canada, and to intervene on a state-to-state level, if necessary. The reporting requirement states that the Canadian Attorney General may "require any person in Canada to give notice to [the Attorney General] of such measures, or of any directives, instructions, intimations of policy or other communications relating to such measures from a person who is in a position to direct or influence the policies of the person in Canada." *Id.* § 5(1)(a). The reporting requirement, like the basic prohibition, is quite broadly worded, reaching even intimations of policy, which may be conveyed by a corporate parent or affiliate, for example. *Id.* Second, in order to frustrate the enforcement of extraterritorial requirements, Canadian citizens or residents may be prohibited from producing, disclosing, or identifying records or information sought by foreign tribunals. In appropriate cases, Canadian courts are even empowered to order the seizure of records in Canada to prevent their disclosure. *See id.* § 4. Third, recognition and enforcement of any foreign judgments that are rendered regarding offensive extraterritorial measures may be prohibited, or their awards reduced. *See id.* § 8(1)(b). This section is applicable primarily to antitrust awards, and designated trade laws set forth in the FEMA schedule. It is also bolstered by another section, which specifically prohibits the enforcement in Canada of any awards made under the U.S. Helms-Burton (LIBERTAD) Act, irrespective of whether Helms-Burton appears on the FEMA schedule at the time. *See id.* § 7.1, 36 I.L.M. at 121. Finally, Canadian residents, citizens, or companies are given the right to "clawback" any awards that foreign parties may have recovered elsewhere in a new cause of action. That is, the Canadian party who loses in a foreign forum may sue the foreign party for the amount of the judgment the foreign party obtained, the expenses incurred in both the foreign action and the Canadian clawback suit, and for any consequential losses or damages suffered by the Canadian party because of the foreign judgment. *See* FEMA § 9. The Canadian award resulting from a clawback action may itself be executed not only against the foreign party, but also against the property of any person or entity, which owns or controls, or is part of a group that owns or controls, the foreign party who obtained the impugned foreign judgment. Thus, this permits the clawback award to be executed against any parent company property located within Canadian jurisdiction, or the property of other members of a holding corporation or group. *See id.* § 9(2).

bined with declining U.S. political and economic hegemony, led the United States to back away from the expansive approach it claimed in the TWEA-based programs as new economic sanctions began to be established in the late 1970s and 1980s.[121] By that time, Congress was also concerned that the Korean War era national emergency[122] was too stale to confer extraordinary powers upon the president.[123] Upon investigation,[124] Congress determined that not one, but four, ongoing emergencies delegated broad, extraordinary powers to the president,[125] which Congress then attempted to curtail with new legislation.[126] One result of this effort was the passage of IEEPA,[127] which removed the national emergency authority from TWEA entirely,[128] except for the then-existing programs,[129] confining TWEA once again to being a wartime grant of authority.[130]

Rather than limiting the president in practice, separate emergencies declared under IEEPA supported the imposition of more economic sanctions programs in the past twenty years than were created in the seventy years prior to the amendment of TWEA in 1977.[131] However, while the statutory language continues to broadly empower the president to act with regard to any property or persons "subject to the jurisdiction of the United States,"[132]

121. *See supra* notes 79-83 and accompanying text.

122. The emergency was President Truman's declaration used to support the imposition of economic sanctions on China at the time of the Korean War. Proclamation No. 2,914, 15 Fed. Reg. 9,092 (Dec. 16, 1950). President Truman's declaration remains the basis for the FACR and CACR in effect today. *See* Presidential Determination No. 96-43, 61 Fed. Reg. 46,529 (Aug. 27, 1996).

123. The courts, however, have rejected arguments that a stale declaration of an emergency is insufficient to trigger the delegation of extraordinary power to the president, leaving it to Congress to speak on the matter. *See* Welch v. Kennedy, 319 F. Supp. 945, 947-48 (D.D.C. 1970).

124. The Senate Special Committee on the Termination of the National Emergency was created in January 1973. S. Res. 9, 93d Cong. (1973). Various investigations into the use of presidential emergency power proceeded through 1976, as one outgrowth of the realignment of executive and legislative power in the aftermath of both Watergate and Vietnam. *See* House Subcomm. on International Trade and Commerce, Committee on International Relations, Trading with the Enemy: Legislative and Executive Documents Concerning Regulations of International Transactions in Time of Declared National Emergency, 94th Cong. (1976).

125. These included President Roosevelt's Bank Holiday emergency, Proclamation No. 2039, 48 Stat. 1691 (Mar. 6, 1933); President Truman's Korean Conflict emergency, Proclamation No. 2,914, 15 Fed. Reg. 9,029 (Dec. 16, 1950); President Nixon's emergency relating to work stoppage by Postal Service employees, Proclamation No. 3972, 3 C.F.R. § 473 (1970); and President Nixon's balance of payments emergency, which was used to support supplemental duties on imports, Proclamation No. 4,074, 3 C.F.R. § 60 (1971).

126. The initial result was the passage of the National Emergencies Act of 1976, 50 U.S.C. §§ 1601, 1621, 1622, 1631, 1641, 1651 (1994), which terminated all presidential powers granted by virtue of past declarations of emergencies, but which exempted, *inter alia*, emergencies declared under TWEA. *See* 50 U.S.C. § 1651(a)(1) (1994).

127. 50 U.S.C. §§ 1701-06 (1994).

128. *See* Pub. L. No. 95-223, § 101(a), 91 Stat. 1625 (1977) (striking the "during any other period of national emergency declared by the President" language from TWEA § 5(b); 50 U.S.C. App. § 5, Historical Notes (1994)).

129. Pub. L. No. 95-223, § 101(b), 91 Stat. 1625 (1977), authorized the continuation of the then existing programs until 1978, and the president's ability to annually renew them from 1978 forward. *See* 50 U.S.C. App. § 5, Historical Notes (1994); Presidential Determination No. 96-43, 61 Fed. Reg. 46,529 (Aug. 27, 1996).

130. Other than the procedural mechanisms for triggering their application, the actual grants of authority to the president under TWEA and IEEPA are very similar. TWEA does differ from IEEPA in authorizing the wartime expropriation or vesting of enemy property in the government, as well as broad powers to regulate domestic transactions, and the ability to seize bullion and records. *Compare* 50 U.S.C. App. § 5(b)(1) (1994), *with* 50 U.S.C. § 1702(a) (1994).

131. *Compare supra* notes 78-97, *with supra* notes 70-75 and accompanying text.

132. *See* 50 U.S.C. § 1702(B) (1994).

the actual sanctions imposed under IEEPA have generally taken a more limited approach. Rather than seeking to reach the farthest limits authorized in prescribing the behavior of U.S.-affiliated foreign companies, most of the IEEPA economic sanctions only impose obligations upon U.S. persons.[133] The distinction is that the term U.S. person typically excludes foreign controlled subsidiaries of U.S. companies, although it does include overseas branches (entities that lack any status as a foreign juridical person) within its ambit.[134]

The United States's ability and willingness to ameliorate the extraterritorial reach of its economic sanctions following the passage of IEEPA related to two factors. First, a more limited political objective underlies several of the more recent sanctions, particularly in those programs focused on targets in this hemisphere (e.g., Nicaragua, Panama, Haiti, Colombian narco-traffickers).[135] Second, many of the targets that otherwise might have been subjected to more expansive sanctions were also the subject of sanctions programs by other countries, acting pursuant to directives from the U.N. Security Council[136] (e.g., South Africa and Namibia, Iraq and Kuwait, the former Yugoslavia, Angola, and to a lesser degree, Libya and Iran).[137] Where there is substantial multilateral cooperation on sanctioning a particular target country, there is less practical need for broad extraterritorial controls by any one country such as the United States, and perhaps less justification as well.

In the trade control area, the broad authority granted in the EAA[138] was used to extend the regulations to control transfers abroad of either U.S.-origin items or foreign products that are the "direct products" of U.S.-origin technology, irrespective of who is involved in the transaction.[139] In addition to these product-oriented provisions, the EAR imported

133. The definition of "U.S. persons" is essentially the same in OFAC's IEEPA-based economic sanctions and in the Commerce Department's special trade controls regulating the activities of "U.S. persons" that might contribute to the proliferation of weapons of mass destruction by others in third countries under the EAR. *See* 15 C.F.R. § 744.9(b) (2000). Nonetheless, the definition of U.S. persons used in the IEEPA-based economic sanctions and the EAR's nonproliferation controls should not be confused with the same term as used in the Export Administration Act Amendments of 1977, which introduced a number of prohibitions regarding U.S. participation in the Arab League's boycott of Israel. The definition of "U.S. person" used in the antiboycott law includes controlled-in-fact foreign subsidiaries of U.S. companies and is therefore substantially the same as "persons subject to U.S. jurisdiction" under the OFAC economic sanctions programs. *See* Export Administration Amendments of 1977, Pub. L. No. 95-52, 91 Stat. 235; 50 U.S.C. App. § 2407 (1994), 15 C.F.R. § 760.1 (2000). This only serves to highlight that when dealing with the various U.S. trade control programs even common terms can have arcane implications, which are not consistently applied from program to program.

134. *See, e.g.*, 31 C.F.R. § 536.316 (NTSR); § 537.314 (BSR); § 538.315 (SSR); § 550.308 (LSR); § 560.314 (ITR); § 570.321 (KACR); § 575.321 (IACR); § 585.317 (FRYSR); § 586.319 (KSR); § 590.309 (UASR); § 595.315 (TSR); § 597.319 (FTOSR) (2000); and the analogous provision of the FNKSR, 65 Fed. Reg. 41,334, 41,339 (2000) (to be codified at C.F.R. § 598.318).

135. *See supra* notes 81, 83, 86, 89 and accompanying text.

136. It should be noted that even where the UN has called for sanctions, the U.S. sanctions programs are often more stringent or go beyond the action sought by the UN, as with the South African, Iranian, and Libyan sanctions, for example. In other cases, the U.S. sanctions preceded action by the UN, as was the case with the sanctions on Iraq/Kuwait and on the former Yugoslavia.

137. Also note that the UN Participation Act provides a coordinate basis for the U.S. sanctions in each of these cases. *See supra* notes 78, 80, 83-85, 87-88 and accompanying text. It would not be correct, however, to assume that IEEPA is no longer used as the sole basis for sanctions. The blocking of terrorist assets in January 1995, under Executive Order 12,947, 60 Fed. Reg. 5,079 (Jan. 23, 1995) and the addition of new restrictions on contracts to develop Iranian petroleum resources under Executive Order 12,957, 60 Fed. Reg. 14,615 (Mar. 15, 1995) in 1995 were ordered solely on the president's authority under IEEPA.

138. *See, e.g.*, 50 U.S.C. App. §§ 2404-05.

139. *See, e.g.*, 15 C.F.R. § 730.5 (2000).

OFAC's "U.S. person" approach in the mid-1990s to restrict U.S. involvement with weapons proliferation activities abroad as part of the EPCI program,[140] irrespective of what is involved in the transaction.[141] Thus, two levels of control are actually created under the EAR with regard to transactions abroad with blacklisted parties. Transactions with those named on either the DPL or the Entities List involving most items subject to the EAR are prohibited—even when conducted by foreign persons—simply because they concern U.S.-origin items or the products of U.S. technology.[142] Accordingly, U.S. origin Dell Computers may neither be directly exported, nor retransferred abroad (re-exported) to the Baltic State Technical University.[143] In addition, U.S. nationals, residents, or companies—including their overseas branches—are subject to still further restrictions on performing "any contract, license, or employment" with those blacklisted on the Entity List due to their involvement in weapons proliferation activities.[144] Thus, Dell's foreign subsidiaries might theoretically be able to deal with the Baltic State Technical University, so long as no U.S. nationals, products, or technology are involved. However, this might be quite difficult in practice, depending upon the involvement or level of support provided by the U.S. parent company to the operations of its overseas subsidiaries, because of the broad prohibitions restricting the ability of Dell in the United States to knowingly participate in or facilitate proscribed activities by those designated on the Entities List.[145]

II. Governmental Blacklists and Screening Obligations

Given these requirements, it's striking that there is no regulatory obligation to actually check transactions, customers, or trading partners against the government's blacklists.[146] No penalties are imposed for failing to institute a screening process, so long as no impermissible transactions occur. Additionally, as a practical matter, relatively few, if any, transactions will occur with blacklisted parties for most businesses. Nevertheless, with the government blacklisting more than 5,000 individuals, companies, or organizations around the world, there is a substantial risk in ignoring the possibility that an impermissible transaction might occur.

Conducting some form of screening actually serves two purposes for any business. First, it helps to identify problematic transactions from among the larger background of entirely permissible dealings. Second, in the event that an impermissible transaction does occur, it

140. *See supra* notes 16-19 and accompanying text.

141. *See, e.g.*, 15 C.F.R. §§ 730.5(d), 736.2(7), 744.6, 744.9 (2000).

142. *See id.* §§ 736.2(b)(4), (5); 744.1(c). Note that the U.S. government permission to proceed with these types of transactions usually must be in the form of an actual license approval. The license exceptions that are set forth in the regulations (*see id.* § 732) are typically unavailable when dealing with denied parties or those named on the Entity List. *See id.* §§ 736.2(b)(4), 744.1(c).

143. *See id.*

144. *See id.* §§ 744.1(c), 744.6.

145. *See id.* §§ 744.6, 744.10. Questions might also be raised in this sort of a transaction—depending on how the overseas transaction actually arose—regarding whether Dell in the United States was involved in an attempt to impermissibly evade the EAR controls. *See id.* § 764.2(h). However, it is perhaps also likely that Dell's overseas subsidiaries deal in products that are "subject to the EAR" in any event, which would bring this hypothetical transaction within the scope of the type of control discussed at notes 142-143, *supra*, and accompanying text.

146. Screening is, however, required for holders of "special comprehensive licenses" under the EAR. *See id.* § 752.

helps to document efforts at good faith compliance and negate or at least mitigate any possible penalties.[147] Accordingly, the government strongly encourages screening in its compliance guidance.[148] However, most of this guidance, and presumably most of the companies who are screening their customers and vendors, are primarily concerned with traditional export transactions. The government's controls and most internal business compliance systems were crafted against a background of cross-border transfers of tangible items, often financed as a documentary sale or letter of credit transaction that depended upon the involvement of numerous third parties and, most of all, took time to complete.[149] In contrast, e-commerce enables much faster transactions, in both tangible and intangible goods and services, with a broader range of both payment mechanisms and parties. The government's controls generally do not reflect the newer e-commerce business models. Perhaps as a result, the general awareness of the government's requirements, and the level of compliance among most e-commerce companies appear to be quite low.

Screening, as typically employed in most internal business compliance programs, involves matching customer and vendor or trading partner account information with the various blacklist entries, often through the use of software designed for that purpose.[150] Although it might be possible to distinguish between those regulatory controls that limit their extraterritorial effect to "U.S. persons" and those that apply more broadly, many businesses simply run an automated screen against all the names on the combined blacklist, and wait until there is a match before examining the scope of the actual control to be applied in a particular case. Periodic re-screening of the customer/vendor database becomes necessary whenever there is a change in either the parties with whom the business deals or in one of the blacklists. As this may be awkward or difficult to predict, many businesses further incorporate blacklist screening into their transaction-by-transaction order processing system. A number of companies have grown up in recent years to assist those businesses that do not choose to establish their own screening compliance programs.[151]

In general, businesses subject to U.S. jurisdiction are strictly liable for any impermissible dealings with blacklisted parties, and may face civil and administrative penalties for even inadvertent violations.[152] Lack of knowledge that the other party to a transaction is black-

147. This may be particularly important both to convincing a government agency to exercise its prosecutorial discretion, or at least to secure some benefit under the U.S. Sentencing Guidelines in the event of a conviction. *See* Fitzgerald, *supra* note 39, Ch. 14.

148. *See, e.g.*, Bureau of Export Administration, *Export Management System Guidelines, Element 1: Denied Persons Screen, available at* http://www.bxa.doc.gov/PDF/Screen1.pdf (visited Dec. 12, 2000); Office of Foreign Assets Controls, *Foreign Assets Control Regulations for the Financial Community, available at* http://www.ustreas.gov/ofac/t11facbk.pdf (visited Dec. 12, 2000); Office of Foreign Assets Controls, *Export Compliance; Don't Neglect OFAC (Part 2), available at* http://www.ustreas.gov/ofac/sia_2.pdf (visited Dec. 12, 2000).

149. *See* Fitzgerald, *supra* note 36, at 94.

150. *See* Bureau of Export Administration, *Export Management System FAQs Denied Persons List Screening, available at* http://www.bxa.doc.gov/Compliance/EMSFAQs.html (visited Dec. 12, 2000).

151. *See, e.g.*, OCR-Inc.com, *Compliant Trade: Knowing Your Partner in the Marketplace, available at* http://www.ocr-inc.com/ (visited Dec. 12, 2000); MSR The e-Customs Company, *About Visual Compliance Online, available at* http://www.visualexporter.com/compliancemetasystem/about.cfm (visited Dec. 12, 2000); VASTERA, *Why Leading Manufacturers and Distributors use the EMS 2000 Solution from Vastera, available at* http://www.vastera.com/pressroom/white_paper3.htm (visited Dec. 12, 2000).

152. With regard to BXA's trade controls, see General Prohibition Four: Engaging in Actions Prohibited by a Denial Order, 15 C.F.R. § 736.2(b)(4) (2000); Standard Terms of Orders Denying Export Privileges, *id.* pt. 764 Supp. No. 1; and Administrative Sanctions *id.* § 764.3(a). With regard to DTC's trade controls, see 22 C.F.R. § 127.10 (2000). *See also supra* note 21 and accompanying text. With regard to OFAC embargoes, *see*

listed is significant only when impermissible dealings with those on the Entities List are at issue, when arguing whether an ostensibly domestic transaction is export-related,[153] or when criminal penalties are involved.[154] Otherwise, a business's level of knowledge, like the presence of an internal controls system aimed at preventing impermissible transactions, is more properly a factor to be considered when exercising prosecutorial discretion or mitigating penalties in a particular case, rather than something that negates the violation altogether.[155]

While new business models involving online—or even fully automated—transactions do permit a greater degree of anonymity regarding one's customers and trading partners, they do not insulate e-businesses from the exposures associated with dealing with blacklisted parties. Although anonymous online transactions might be unlikely to come to the attention of government enforcement officials, truly anonymous e-commerce transactions remain rare—especially if payment is to be provided for the goods or services obtained online. Entirely apart from the matter of payment, data mining—acquiring, collating, and analyzing information regarding customers and trading partners—is an increasingly critical part of establishing the distinguishing elements of any e-business operation. Thus, during the ordinary course of their operations, most e-businesses will acquire sufficient information concerning the identity of their customers and trading partners to trigger these governmental controls.

The application of the traditional strict liability approach to online transactions with blacklisted parties can be seen, for example, in the way OFAC regards automated payment processing systems—online systems that are intended to process transactions completely, without any human intervention whatsoever. For many years OFAC was especially lenient with financial institutions when blacklisted parties slipped through the software ordinarily used to interdict their handling of impermissible transactions in their automated processes. In 1995, however, the agency announced that

> It has been determined that it is no longer appropriate to treat fully-automated financial transactions that violate economic sanctions prohibitions as being beyond a financial institution's knowledge or intent . . . [OFAC] will no longer treat the fully-automated processing of violative transactions as a full defense in civil penalty proceedings.[156]

Of the three principal agencies generating these blacklists, BXA is arguably the most attuned to the demands and requirements of e-commerce. It has attempted to grapple with a number of the problems presented by online transactions in its "deemed export" rules for domestic transfers of technology,[157] de minimis provisions for the extraterritorial application

for example, 31 C.F.R. § 515.701(a)(3) (2000) (civil penalty authority under Cuban embargo). *See also supra* notes 27-28 and accompanying text.

153. *See supra* notes 51-52 and accompanying text.

154. See General Prohibition Five: Export or Reexport to Prohibited End-Uses or End-Users, 15 C.F.R. § 736.2(b)(5) (2000), which states "(y)ou may not, without a license, *knowingly* export or reexport any item subject to the EAR to an end-user . . . that is prohibited by part 744 of the EAR" (emphasis added). *See also supra* notes 20-21, 29-31, 62-65 and accompanying text.

155. See, for example, 15 C.F.R.§ 764.5(e)(4) (2000), which includes whether the impermissible act was intentional or inadvertent as a consideration when evaluating what administrative sanctions to impose following a voluntary disclosure of a violation.

156. *See* Compliance with 31 CFR Chapter V with Respect to Fully-Automated Financial Transactions, 60 Fed. Reg. 34,141 (June 30, 1995).

157. Any release of technology or software source code to a non-permanent-resident foreign national is deemed to be an export to that individual's home country. *See* 15 C.F.R. § 734.2(b)(2)(ii) (2000); *see also* Bureau

of its controls to goods and technology transferred abroad,[158] and in the rules formulated to deal specifically with online transfers of encryption technology and software.[159] OFAC is arguably at the other end of the spectrum, having traditionally focused primarily on financial dealings by major institutions that take some time to be executed. Although OFAC is making increased use of the Internet to distribute its materials and blacklists,[160] it has largely failed to provide guidance on how to adapt its requirements to the pace and demands of e-commerce.[161] DTC is somewhere in between, but perhaps unlike the other two agencies, is less likely to see its controls on munitions items to be a major concern for most online businesses. The level of sophistication reflected in the agencies' own controls is perhaps some indication of how amenable they might be to entertaining the discretion to excuse or mitigate an inadvertent violation by an online business.

BXA, and to a lesser degree DTC, have brought numerous, well-publicized prosecutions for violations of their trade controls.[162] Although several have involved high tech businesses, none of the published prosecutions were brought solely for failure to screen an online transaction against the blacklists.[163] OFAC's enforcement actions, at least outside of the financial community, are much less well-publicized.[164] There is a perception that a substantial gap exists between the letter of the law and OFAC's enforcement actions, particularly with regard to retail cash sales and small non-banking transactions with blacklisted parties.[165] The retail sale of a single McDonald's hamburger to Pierre Boileau, for example, presumably does not merit the resources required for a prosecution, even though there is no formal de minimis threshold in the OFAC regulations. There is also a perception that political considerations influence OFAC's prosecutorial discretion. Despite some strong public statements by the agency, Chelsea Clinton's high school classmates were not prosecuted following a very public, unauthorized trip to Cuba.[166] When Bobby Fischer disregarded similar warnings regarding playing a championship chess match against Boris Spas-

---

of Export Administration, *Deemed Export Questions and Answers*, *available at* http://www.bxa.doc.gov/DeemedExports/DeemedExportsFAQs.html (visited Dec. 12, 2000).

158. 15 C.F.R. § 734.4(c); pt. 734, Supp. No. 2 (2000).

159. *See, for example*, 15 C.F.R. § 734.2(b)(9) (2000), addressing the need to screen for IP addresses and foreign government end-user domain names when transferring encryption software or technology over the Internet. *See also* Internet Posting and Sales in Bureau of Export Administration, *Commercial Encryption Export Controls; Questions and Answers* (Oct. 19, 2000), *at* http://www.bxa.doc.gov/Encryption/Oct2KQsandAs.html (visited Dec. 12, 2000).

160. *See, e.g.*, Office of Foreign Assets Control, *at* http://www.ustreas.gov/ofac/ (visited Nov. 17, 2000); *see also* Fitzgerald, *supra* note 25, at 127-29.

161. For example, OFAC declined to respond to a letter and a proposal submitted by IBM on June 10, 1996, regarding guidance on how Internet service providers should address the possibility that online transactions might occur with blacklisted parties without their knowledge or participation. *See* Fitzgerald, *supra* note 251, at 116, n.231.

162. *See, e.g.*, Bureau of Export Administration, *Don't Let This Happen to You!!!*, *at* http://www.bxa.doc.gov/Enforcement/CaseSummaries/DontLetThisHappen2u.pdf (visited Dec. 12, 2000).

163. *See id.*

164. There are only eight readily available press releases regarding OFAC enforcement actions over the past decade. *See* Office of Foreign Assets Control, *Press Releases and Miscellaneous Documents*, *available at* http://fedbbs.access.gpo.gov/libs/fac_misc.htm (visited Dec. 12, 2000).

165. *See* Fitzgerald, *supra* note 36, at 95.

166. *See* Richard Leiby, *A Vacation at Club Red: Kids Plan to Flout the Cuba Ban for Some Socialism and Socializing*, WASH. POST, June 3, 1995, at H01; Lois Romano, *Cuba Missive Crisis*, WASH. POST, June 21, 1995, at D03.

sky in Yugoslavia, however, he was indicted and is now a fugitive from the United States.[167] Nevertheless, the lack of a significant record of public prosecutions should not be surprising, given the adverse political and public relations consequences that would flow from being prosecuted for dealing with embargoed destinations, or blacklisted terrorists, weapons proliferators, or narco-traffickers. One would expect that most enforcement actions are settled or resolved at the earliest possible stages and there are apparently a large number of cases, principally involving financial institutions that are settled upon payment of civil penalties.[168]

III. Conclusion

Large, sophisticated e-businesses like Walmart.com, Dell Computer, and America Online will of course take steps to ensure their compliance with the U.S. government's controls and blacklists. Their extensive customer and trading partner databases will be screened, in some fashion, against the government's various blacklists. While the fines and criminal penalties possible for any violations are significant, it is the fear that unseen bureaucrats might administratively add their names to one of these blacklists that provides the real motivation to institute a screening process. The possibility that a Walmart.com, a Dell Computer, or an America Online might be denied access to U.S. goods, technology, or contractual partners is too great a risk to be assumed as a cost of doing business.

Smaller e-businesses, and especially start-ups, might be tempted to take comfort that there appear to be relatively few high profile enforcement actions involving impermissible dealings with blacklisted parties, and conclude that the risks associated with not screening the information they mine from their online operations are low. However, this reflects a failure to fully appreciate the impact of the administrative sanctions available to these agencies to enforce their controls. Moreover, relying upon prosecutorial discretion in the event an impermissible transaction does in fact occur is not always the most prudent business controls system. Ignoring these blacklists is especially risky when the politics associated with the underlying governmental control programs are often highly volatile and the public relations consequences of being seen to be in violation are potentially disastrous.

Additionally, the probability that any particular e-business will find itself inadvertently dealing with a blacklisted party has dramatically increased over the last decade. New regulatory programs are proliferating, and the government shows an increasing proclivity to resort to the blacklisting tool for a host of issues well removed from the traditional core concerns of foreign policy and trade controls. Trusting that the government will refrain from prosecuting or blacklisting companies for small or innocent violations may have worked for some purely domestic businesses in the old economy. Ignoring the government's blacklists in the new economy, however, must be considered as increasingly suspect. In the world of global e-commerce, screening customer and trading partner information against the government's blacklists must become an integral part of an e-business's online data mining operations.

167. *See* Jeffrey Young, *U.S. to Chess Great Fischer: No Move*, UPI NEWS, Aug. 14, 1992, *available in* Lexis ALLNWS database; *see also Where is Bobby Fischer?*, *at* http://www.anusha.com/fugitive.htm (visited Aug. 16, 2000).

168. *See, e.g.*, Office of Foreign Assets Control, *OFAC Compliance: A Perspective for Community Banks*, *at* http://www.ustreas.gov/ofac/aba2.pdf (visited Dec. 12, 2000). There are numerous due process concerns associated with blacklisting, particularly as it is used by OFAC. *See also* Fitzgerald, *supra* note 25; Peter L. Fitzgerald, *Drug Kingpins and Blacklisting: Compliance Issues with U.S. Economic Sanctions*, 4 & 5 J. MONEY LAUNDERING CONTROL (forthcoming 2001).