WILMERHALE

Forgotten Issues in the U.S. Presidential Contest

2000-12-01

In all the drama of divining voters' intentions by squinting at ballots and repeated challenges in state and federal courts, it is easy to overlook the significance of the outcome of the U.S. Presidential contest for law enforcement outside the United States. For much of the past decade, the U.S. government has been working hard to extend the reach of its criminal laws to actions occurring entirely outside the territorial limits of the U.S., when those actions may cause harm to U.S. economic interests. This is a departure from traditional criminal law enforcement, which has generally been confined to events taking place within the borders of a country, and it is a development that has generally not been followed by other Western countries.

In 1996, Congress enacted the Economic Espionage Act (18 USC §§ 1831-1839) which makes it a crime, prosecutable in a U.S. court, to misappropriate a trade secret belonging to a U.S. company anywhere in the world. The Act defines "trade secret" very broadly to include:

> "all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (a) the owner thereof has taken reasonable measures to keep such information secret; and (b) the information derives economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public. . .". (§ 1839(3)).

Attorney Advertising

The penalties under the Act are twice the usual penalty for U.S. criminal offenses, and are increased again to three times the usual penalty if a "foreign instrumentality" (i.e., "any agency, bureau, ministry, component, institution, association or any legal, commercial, or business organization, corporation, firm or entity that is substantially owned, controlled, sponsored, commanded, managed or documented by a foreign government" (§ 1939(1)) is involved. Thus, the attempt to obtain information in England about a secret process being developed by a joint venture between a U.S. and an English company, by a group which is financed by the government of France, is now a U.S. crime punishable by imprisonment for 15 years and a fine of $10,000,000. Under recently negotiated mutual assistance treaties, the potential offense can be investigated in England and France by U.S. FBI agents, with the active help of English and French law enforcement agencies. When Congress enacted the Economic Espionage Act in 1996, it placed a five year moratorium on prosecutions without the specific prior review and approval of the U.S. Attorney General. That moratorium will expire in October 2001. Attorney General Janet Reno has approved only a handful of prosecutions in the last four years, but the FBI has announced that it has over 800 cases under active investigation, and U.S. Attorneys in high technology areas, like Boston and San Francisco, have publicly stated that the preparation of cases under the Economic Espionage Act is a top priority of their offices. It may be assumed, therefore, that several significant cases, many involving non-U.S. citizens, will be brought under the Act after the moratorium expires next fall.

In 1994, Congress passed the present version of the Computer Fraud and Abuse Act (18 USC § 1038). That statute prohibits anyone, no matter where he or she is located, from obtaining unauthorized access and gaining information from any computer "which is used in interstate or foreign commerce or communications". It is not necessary that the information obtained be a trade secret. Thus, a person working from a laptop in Frankfurt, who hacks into a computer system located at a U.S. company's offices in London, has committed a U.S. crime and can be prosecuted in a U.S. court, even though neither he nor any part of the transaction for which

he is charged crossed into U.S. territory. The FBI will also investigate that offense, including interviewing non-U.S. citizens and reviewing their documents in Frankfurt, with the help of German law enforcement authorities, and in London with the help of English authorities.

In addition, U.S. regulatory agencies have been increasingly concerned over the last five years about threats to the U.S. economy from actions occurring entirely outside the U.S. The SEC has pondered the extent to which it can and should investigate fraudulent stock offerings on the Internet and non-fraudulent but essentially unregulated stock offerings to U.S. citizens from foreign countries. See 1997 WL 276278 (SEC). The Treasury Department has established a Financial Crimes Enforcement Network (FinCEN) in Virginia, at which a large computer center processes information submitted by U.S. financial institutions, looking for patterns in international currency transfers which might signal money laundering. And the U.S. Customs Service has raised the investigation of currency smuggling to a top priority, with a particular emphasis on connections with Eastern Europe.

Over the last decade, U.S. law enforcement agencies have quietly negotiated mutual assistance treaties with at least 34 countries, including most of the European Union members. These mutual assistance treaties are designed to allow quicker, more informal assistance by other countries' law enforcement agencies in the investigation of violations of these statutes outside the U.S. On a few occasions recently, these efforts have been noticed, for example when the FBI and local police arrested a young man in Wales for hacking into a U.S. computer and when it was disclosed that the FBI had developed a software program (known internally by the code name "Carnivore") to tap into Internet transmissions anywhere in the world. The FBI has a center with over 100 agents working just in the area of computer crimes, and the SEC has created a team of lawyers and investigators who regularly surf the Net looking for potentially fraudulent securities offerings. In each of the 93 U.S. Attorneys' offices in the U.S., there is at least one attorney who specializes in computer-based crimes, and there is a section within the Criminal Division of the Department of Justice in Washington

devoted exclusively to assisting U.S. Attorneys to investigate and prosecute computer-based crimes wherever they occur. On the whole, this has been a quiet revolution in U.S. law enforcement. It has drawn little notice, and, as the Clinton administration is coming to an end, each of the law enforcement agencies and local federal prosecutors offices is waiting to see what will happen when the new administration comes in.

That change is about to come, and as this is being written, it appears likely that the Republicans will re-take the White House. Whatever their relationship with an evenly divided Congress, the Republicans will then again control the law enforcement and foreign policy apparatus of the U.S. George W. Bush has surrounded himself with a team that can be expected to focus a good deal of attention and energy on protecting the U.S. economy from what it perceives as threats from overseas, in particular by vigorously enforcing the Economic Espionage Act, the Computer Fraud and Abuse Act, and those sections of the U.S. Code which prohibit undeclared overseas transport of currency and fraudulent use of the Internet. U.S. law enforcement agencies -- like the FBI, Customs, and the IRS -- have the tools in place. Most European governments have already declared their willingness to assist those agencies to conduct their investigations on the ground in Europe. These forces only await the command of a strong U.S. executive with a priority of protecting U.S. economic interests in the new world economy. Mr. Bush may be expected to be such a President, and it should not be long before the evidence of his interest in U.S. overseas law enforcement becomes apparent in Europe.

Richard Wiebusch

richard.wiebusch@haledorr.com

This publication is not intended as legal advice. Readers should not act upon information contained in this publication without professional legal counseling.

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome. © 2004-2024 Wilmer Cutler Pickering Hale and Dorr LLP