WILMERHALE

The Hidden Dangers of International Cooperation

2000-12-01

Much has been written of late on the problem of cross border fraud and the value of mutual legal assistance treaties to fight it. But little attention has been directed to the trade-offs that such a system requires in the protection of basic human and individual rights. Like many good ideas, international mutual assistance in the investigation and prosecution of white collar crime carries with it the seeds of serious problems.

The present-day concern about cross border fraud, or international white collar crime, is based on a realistic assessment of the effects of globalization. Widespread reliance on computer systems to store and process information and to handle every transaction from the manufacture of soft drinks to the deployment of armies, coupled with the globalization of business, news and travel, and free world-wide access to the Internet, have turned the mere possibility of cross border crime into a probability. This, in turn, has required law enforcement agencies in several countries to increase their levels of mutual assistance in the investigation, apprehension and prosecution of responsible parties. It is clear that the first targets of concern -- stock fraud, money laundering, tax evasion, and cyberterrorism -- deserve special attention. However, law enforcement agencies operating outside their borders do not always place a high priority on protecting individual rights and, while law enforcement agencies in different countries may cooperate with each other, their legislatures often do not, with the result that the agents of one country may be enforcing standards in another country that are not otherwise imposed on the citizens of that country. In order for a system of cooperation in

international law enforcement to work, some country must set the standards that all will follow and some provision must be made for the protection of individual rights. At present, the United States is setting the standard for international white collar crime enforcement, but no one seems to be paying attention to the threat to individual rights.

That the U.S. is setting the standard for the definition of white collar crime around the world may be shown by a few examples. For over two decades, the U.S., through the Foreign Corrupt Practices Act, has prohibited its citizens from paying bribes to foreign officials in order to obtain contracts, even in situations where the payment of such a bribe is expected in the local culture and not prohibited by local law. The same statute has also required companies listed on U.S. stock exchanges to disclose such bribes on their financial statements. As international stock offerings have increased in number and the threat of Internet stock purchases on less regulated exchanges has become a concern to the SEC, the U.S. has taken steps to enforce this standard against companies that are neither U.S. citizens nor based in the U.S. In one recent case, the SEC charged an Italian company with violation of the Foreign Corrupt Practices Act when it failed to disclose on its financial statements that it had made a legal payment to an Italian official to obtain a contract in Italy. The Italian company's only connection with the U.S., and the sole legal basis for the SEC to assert this position, was that ADRs relating to the company's stock were traded on the New York Stock Exchange. A year ago, a joint Home office/Department of Trade working group in Britain announced that it would recommend that the UK not make it a crime for UK companies to bribe foreign officials to obtain contracts. Two months later, the government reversed itself and announced that it would pass such a law. The Financial Times reported that the change followed "strong lobbying by the U.S. Treasury Department that was 'appalled' by British inaction over the issue."

A second example may be found in the investigation of crimes on the Internet. A few years ago, the FBI developed, in secret, a software program that allowed it to monitor Internet

communications anywhere in the world. During the same period, the U.S. Government was seeking to compel private companies to surrender software encryption keys, first as a condition for exporting their software and later as a protection against cyberterrorism. On May 24, 2000, the British government proposed a Regulation of Investigatory Powers (RIP) bill that would require companies to turn over their encryption keys to British law enforcement agencies so that they could read Internet transmissions in secret. General opposition from business groups quickly followed. A week later, the government defended the proposal by saying that the power it sought would only be used to tap into the Internet through ISP's - precisely what the FBI had been doing secretly for two years. Despite continued opposition from industry and academics, the RIP bill passed, but with a requirement that the Home Secretary review and approve in advance any Internet tapping operations by British law enforcement. In July, the existence of the FBI's web tapping software (code named "Carnivore") became public and touched off severe criticism in the U.S. Congress. The FBI defended its use of that software by saying that it always obtained the approval of a federal judge before putting it to work.

Why is the U.S. so aggressive in projecting its standards of commercial conduct overseas? Because it is concerned in general that the Internet and globalization have made the U.S. economy more vulnerable, and the U.S. Congress believes that the threat of criminal prosecution will deter attacks by foreign nationals. Britain is following the U.S. lead because the Internet and globalization link the Western economies more tightly than ever before, and injury to one is felt by all.

That this is not merely a phenomenon of the "special relationship" between the U.S. and Great Britain is illustrated by a third example. The U.S. has long sought to prevent secret international transfers of currency that "launder" the proceeds of crime and help evade taxation. The Treasury Department has a well-established program of incentives for international banks to cooperate with U.S. law enforcement in their efforts to prevent money

laundering. But the U.S. can only do so much by itself. On June 23, 2000, the Financial Action Task Force (FATF), an arm of the Organization for Economic Cooperation and Development (OECD) which is, in turn, a body that promotes U.S. and EU interests, announced a "blacklist" of countries around the world that it regarded as "non-cooperative" in the international fight against money laundering. The FATF requested its constituent countries to pay particular attention to financial activities passing through the countries on the blacklist and said that it would take "unspecified countermeasures" against the listed countries if they did not quickly mend their ways. Several countries on the blacklist immediately fell into line. Four days after publication of the blacklist, Cayman Island officials left home to attend an OECD sponsored seminar on money laundering in Paris. A week after publication of the blacklist, the Israeli government announced that it would enact legislation against money laundering. On the same day, Panama proposed to allow its Financial Intelligence Unit to cooperate with law enforcement agencies in other countries. On October 18, the first joint meeting of EU finance and home affairs ministers agreed to establish penalties for the remaining countries that did not respond positively to the FATF blacklist. Clearly, the U.S. and Europe have found a way to cooperate in bringing much greater pressure on smaller countries to stop money laundering and tax evasion and to assist U.S. and European law enforcement in gathering evidence for criminal prosecutions.

While no one will argue that money laundering, stock fraud and tax evasion should not be stopped or that the effort to stop these crimes will not be facilitated by international agreement on one standard of conduct and the procedures for enforcing it, little consideration seems to have been given to how the rights of individual citizens in these countries will be protected as law enforcement agencies from the U.S., EU, OECD, and every other country they pressure into "mutual assistance" begin to work together to investigate and prosecute economic crimes. One may fairly ask what is being done at any level to protect individual rights when the U.S. or UK government monitors Internet traffic in France or Japan using web-tapping software applied to an ISP in Panama City.

Under the mutual legal assistance treaties now in place between the U.S. and UK, FBI agents are permitted to work, side by side, with Scotland Yard and local police in England and Wales to obtain evidence to use in a U.S. court against a citizen of Britain. In fact, last year, when a Welsh boy was arrested for orchestrating a denial of service attack on computer systems in the U.S., FBI agents actually joined local Welsh police in making the arrest at the boy's home in Wales. We can assume that much more activity by U.S. law enforcement agents is occurring on the ground in Britain and throughout Europe than we are aware of. We may be inclined to take comfort in the idea that, if U.S. law enforcement agents are accompanied by local authorities when operating in other countries, they are at least bound to respect the limits on police action that are imposed by the laws where they are acting. But U.S. courts, while refusing to admit evidence obtained in the U.S. by law enforcement agencies in violation of an individual's rights, will accept evidence obtained legally in another country, even if the standards that apply to law enforcement in that country would not be acceptable in the U.S. A recent example occurred in the trial of Nigerian nationals in New York City, for bombing the U.S. embassy in Nigeria. The defendants moved to suppress confessions they had made in Nigeria to FBI agents, who were working with the local police investigating the bombing. The defendants claimed, and the FBI did not deny, that they were abused and threatened by the FBI in order to obtain confessions. Had those tactics been employed on U.S. soil by the FBI, the confessions would have been inadmissible. But the Court ruled that, since they occurred on Nigerian soil and those tactics were permitted to law enforcement in Nigeria, the resulting confessions could be admitted in a U.S. court. Thus, one real danger of international cooperation in the fight against white collar crime is that U.S. law enforcement agencies will be able to obtain evidence in "cooperating" countries, in accordance with whatever rules pertain in those countries, then use it against citizens of those or other countries in a prosecution in the U.S. for violation of U.S. criminal laws. Who can say what may happen when the FBI requests the Panama Financial Intelligence Unit to use the FBI's web-tapping software to monitor Internet traffic between Britain and the U.S.? And if Europeans feel no

threat from the U.S. prosecuting Nigerians in a U.S. court for violating U.S. criminal laws when they bombed the U.S. embassy, how will they feel when the U.S. prosecutes citizens of EU countries for acts which take place in the EU and are perfectly legal where they occur?

International cooperation in law enforcement is a good idea, but, like many good ideas, it can lead to unintended and unfortunate results. International standards of financial conduct, transparency and cooperation should be set, but along with them needs to be international agreement on the nature and protection of individual and human rights, so that the cure does not become more of a threat than the disease.

Richard Wiebusch
richard.wiebusch@haledorr.com