Executive Memorandum

Published by The Heritage Foundation

No. 992
February 14, 2006

EU Privacy Directive Could Prohibit Information Sharing with U.S. Law Enforcement

Alane Kochems

In October 2005, the European Commission released a proposed Framework Decision to protect personal data used in criminal matters. The proposed directive's goals include (1) improving cooperation among European Union countries, especially in preventing and combating terrorism; (2) ensuring that EU states respect fundamental privacy rights; and (3) ensuring smooth data exchanges between states. These are laudable goals that, if realized, could be helpful in combating terrorism and other transnational crimes, such as drug and human trafficking and financial fraud. However, Article 15 of the Framework Decision includes provisions that would impede intelligence, police, and judicial cooperation both among EU states and with non-EU states.

- The proposed EU privacy directive would prohibit EU members from sharing information with U.S. law enforcement.
- President Bush should work with the EU to prevent the directive from hindering the war on terrorism.

Article 15 outlines requirements for sharing data with third-party states, such as the United States. This is problematic because the EU views U.S. privacy protections as inadequate; thus, the directive would likely prohibit cooperation and information sharing with the United States. Impeding such data exchanges would make fighting the war on terrorism even more difficult. The U.S. government should work with the EU to ensure that passage of the directive does not prohibit intelligence sharing between the United States and EU states.

Past EU Privacy Directives. The proposed directive is not the first EU effort to standardize privacy protections within the EU. The EU considers the privacy of personal data as a fundamental right, and its privacy regulations outline common rules for both public and private entities within the EU that hold or transmit personal data. The 1995 EU Data Protection Directive prohibits the transfer of personal data to a non-EU state unless that state is certified as having adequate privacy protections. This directive relies on comprehensive legislation that requires, for instance, the establishment of government data protection agencies and registration of databases with those agencies. The EU does not believe that the United States meets these personal data privacy protection requirements.

Since the United States takes a more segmented approach to privacy protection—relying on a mix of legislation, regulation, and self-policing—it developed the U.S. Safe Harbor Privacy Principles as a way for U.S. companies to comply with the Data Protection Directive. Safe Harbor principles require

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/em992.cfm

Produced by the Douglas and Sarah Allison
Center for Foreign Policy Studies
of the
Kathryn and Shelby Cullom Davis
Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

(1) notice of the purposes for which the information is collected; (2) a choice to opt out of having information disclosed to a third party; (3) restriction of third-party data transfers to those that subscribe to Safe Harbor principles, the EU directive, or another adequate certification; (4) provision for a person to review personal information held about oneself so that inaccurate information can be changed, corrected, or deleted; (5) reasonable security precautions to protect information from loss, misuse, unauthorized access, disclosure, or alteration; and (6) data integrity, meaning that the information must be reliable for its intended purpose. Under this program, which the EU approved in 2000, enrolled U.S. companies that subscribe to Safe Harbor principles are deemed to meet EU privacy standards, allowing them to avoid both delays in business dealings and prosecution under EU privacy laws.

The Latest EU Privacy Directive. Article 15 of the Framework Decision addresses the transfer of personal data from one EU state to competent authorities in a third-party country (or international body) in cases in which the data were originally provided by another EU state for law enforcement or judicial cooperation in a criminal matter. A data transfer must also meet four additional criteria: First, a law must clearly authorize or require the transfer. Second, the data transfer must (1) be necessary for the same reason that the data were originally provided by the originating EU state; (2) aid in prevention, investigation, detection, or prosecution of criminal offenses; or (3) prevent a threat to public security or a person. Third, the EU state that originally provided the data must authorize the data transfer to the receiving third-party country. Fourth, the receiving country must have an adequate level of data protection.

Member states will assess the receiving country's level of data protection processes based on the individual circumstances of each transfer or type of transfer. Specifically, the assessment will consider the type of data, the purpose and method of the transfer, the originating country and recipient country, the applicable laws in the recipient country, the professional and security rules in the recipient country, and the presence of sufficient safeguards.

EU member states and the European Commission would be required to exchange information on whether third-party international bodies and countries are meeting the data protection standards. If a third party does not meet the privacy standards, EU members would be required to take precautions to prevent transfer of personal data to it. The only exception to these rules would be a circumstance in which the personal data transfer is absolutely required to protect a member state's critical interests or to prevent an imminent, serious danger to public security or to a specific person or group.

What Should Be Done. As the London and Madrid bombings and the latest Osama bin Laden tape demonstrate, terrorist groups remain active and dangerous. Only by sharing intelligence and cooperating can the countries of the world prevent attacks and deal with the perpetrators. If enacted, Article 15 will block much of the possible information sharing between the United States and its European allies; the Bush Administration should work with the EU to ensure that it does not undermine the war on terrorism.

If Article 15 is enacted, the Bush Administration should work with the EU to create a program like Safe Harbor that allows law enforcement to sidestep the Article 15 provisions. The program's principles might allow data transfers to a third party only if (1) the third party subscribes to Safe Harbor principles, the EU directives, or another adequate certification; (2) reasonable security cautions are in place to protect information from loss, misuse, unauthorized access, disclosure, or alteration; and (3) the data used in prosecution or prevention of crime are reliable for their intended purposes.

Conclusion. As written, Article 15 would prevent EU member states from sharing information with U.S. law enforcement agencies, impeding the ability of the U.S. to receive information needed to prosecute the war on terrorism. The President needs to ensure that EU privacy concerns do not hinder the war on terrorism. If necessary, the Administration should create a program for intelligence agencies and law enforcement like Safe Harbor to facilitate the flow of information from EU members to U.S. law enforcement.

—Alane Kochems is a Policy Analyst for National Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.