wiley

NEWSLETTER

Encryption: Administration Opens The Door To Domestic Regulation As Congress Debates Privacy, Commercial And Security Concerns

October 2, 1997

The debate over U.S. encryption policy is becoming increasingly polarized. Privacy advocates and promoters of electronic commerce see the strong encryption of personal and financial data as essential to both personal privacy and the integrity of digital transactions. Law enforcement and national security officials argue that they need rapid access to encrypted messages, without the knowledge of either sender or recipient, to prevent or solve crimes and defend vital U.S. interests. Since the "clipper clip proposal" of the early 1990s, which would have mandated Government access to all encrypted computer communications as a condition to dealing with the Government, the debate has raged, without compromise. The result has been a regime without limits on the the domestic use of strong encryption products, but strict controls on the export of even relatively weak encryption technology. The debate has intensified as Congress has stepped in to consider competing bills and the Clinton Administration has advanced proposals that would substantially alter the status quo.

In December 1996, jurisdiction over non-military encryption products was transferred from the State Department to the Commerce Department. Commerce promulgated regulations permitting the export of up to 56-bit key length DES encryption products on the condition that the exporter agree to establish, by the end of 1998, an acceptable method for allowing government access, on request, to information encrypted using the exporter's products ("key recovery").

In August 1997, a Federal district court in California held certain aspects of the Commerce Department's licensing plan to be an unconstitutional prior restraint on speech. However, the regulations remain in force pending appeal of that order.

Opponents of the Commerce Department's approach have been active in Congress and, throughout the early months of this session, mustered surprising support for two bills—the pro-industry, privacy oriented "Promotion of Commerce On-Line in the Digital Era" Act (the "Pro-CODE Act") in the Senate, and the similarly oriented "Security and Freedom Through Encryption" Act (the "SAFE Act") in the House of Representatives. Both bills sought to limit the government's ability to impose restrictions on the export of strong encryption technology.

Recently, however, Congressional efforts to ease export controls have met determined resistance. In the Senate, the Pro-CODE bill was sidelined in favor of a compromise measure, S.909, sponsored by Senators McCain and Kerry. The McCain-Kerry bill would only modestly relax the current controls on U.S. encryption exports and would create substantial incentives for a domestic key recovery system. The bill was ordered to be reported favorably by a narrow vote of the Commerce Committee, and has only limited support. It is not expected to move this year.

On the House side, the SAFE bill was referred to five separate committees—Commerce, Intelligence, International Relations, Judiciary, and National Security—with widely divergent results. The International Relations and Judiciary Committees reported the bill without amendment. However, the Intelligence and National Security Committees, in response to testimony and public statements by FBI officials, including Director Freeh, made major changes to SAFE, adopting amendments that radically changed its potential effect on both the export and domestic use of encryption products. Instead of lifting export controls, the Intelligence and National Security versions of the bill would condition all export of encryption products on the potential to harm national security. The President would annually set the maximum level of encryption strength that could be exported.

The Intelligence Committee's draft would also institute mandatory key recovery for domestic encryption. Manufacturers and retailers of encryption technology would be required to include in their products features that would permit immediate access to the plaintext of encrypted information without the knowledge or cooperation of the party using the product. Furthermore, the amendment would compel network service providers to ensure that encryption products offered on their systems also allow immediate decryption without the knowledge or cooperation of the encrypting party.

On September 25, after a last-minute lobbying campaign by industry and privacy advocates, the House Commerce Committee rejected the strict export control and domestic key recovery amendments adopted by the Intelligence and National Security Committees, instead reporting the bill with two new amendments. The first would prohibit mandatory key escrow, but also would create a "National Electronic Technologies Center" to serve as a resource for law enforcement authorities on encryption matters. The second would direct the Secretary of Commerce to research and report on "domestic and foreign impediments to trade in encryption products and services," and establish mechanisms to seek removal of those impediments.

All five House committees have completed their review of the SAFE bill and have reported sharply conflicting versions. The House Rules Committee will decide which version or versions of the bill to send to the floor for final action. Rules Committee Chairman Solomon has stated that he opposes any encryption bill that does not provide for mandatory plaintext access by law enforcement authorities, something opposed by many of the bill's original sponsors. In view of the ongoing stand-off between industry and law enforcement, it appears unlikely that the House will pass legislation this year. It remains to be seen how the apparently growing support for mandatory domestic key recovery within the Clinton Administration will affect the Commerce Department's regulation of exports.