Denning, D. E., "Key Concerns," Information Security, Vol. 4, No. 11, November 2001, p. 120.

Speaking to the Senate on September 13 and 19, Senator Judd Gregg (R-NH) called for a new encryption regime that would give the law enforcement and intelligence communities the capability needed to monitor terrorist communications. Under the proposed regime, government officials could get access to encryption keys for encryption products built in America or imported into the country "under a strict structure which is legal and judicially controlled." The plan would be developed through cooperation internationally and with the manufacturing and inventive communities.

Senator Gregg's proposal raised alarms throughout the Internet about the possibility of mandatory key escrow. The Computer and Communications Industry Associate voiced strong opposition to the proposal, as did other industry and Congressional leaders and public interest groups. Indeed, there seems to be little support. The Bush Administration has not publicly endorsed the concept, and did not propose any changes to encryption policy as part of its anti-terrorism package. Further, it did not extend the charter of the President's Export Council Subcommittee on Encryption (PECSENC), which expired September 30, suggesting that the Administration considered the major encryption issues to be resolved. As of October 15, Gregg has taken no further action or introduced any bills.

Considering the widespread opposition to the Clinton Administration's various key escrow proposals, any move to regulate encryption domestically would almost certainly fail without first establishing a broad base of support. For this to happen, proponents would need to make the case, something that previous efforts failed to do. Specifically, they would need to establish four conditions:

1. *Necessity* – that encryption has significantly thwarted counter-terrorist efforts to date or that it will significantly thwart them in the future. We have heard that the Al Qaeda network has used encryption and steganography, but do not know to what extent this is hampering investigations and intelligence collection. We do know that law enforcement agencies have successfully handled many criminal cases involving encryption using a variety of means, including acquiring the keys, breaking the codes, and obtaining the plaintext or evidence through other means.
2. *Effectiveness* – that terrorists, particularly transnational terrorists, would use products endorsed by the U.S. government and its allies. One of the reasons so few people supported the Clipper chip and its descendents is that they could not imagine criminals and terrorists using it. Indeed, a recent report claimed bin Laden was using a steganographic system developed in-house by his own computer expert. However, other terrorists have used or are using commercial products from the West.
3. *Safety* – that a method could be developed and widely deployed without introducing unacceptable risks to privacy and the security of legitimate communications. Any method that permits government access is potentially

exploitable by other parties, even if the risks are extremely low. A report from a group of well-known cryptographers arguing that a key escrow infrastructure would threaten security certainly did not help the Clinton Administration's key escrow initiative.

4. *International support* – that the international community would get on board and work with the United States towards a common solution. The United States has no monopoly on either the encryption industry or on encryption expertise, so terrorists could readily acquire products elsewhere, including downloading them from the Internet. Further, international support is needed so that the solution does not seriously harm the ability of American companies to compete in the global market. The Clipper proposals never won a broad base of support internationally.

The private sector here and abroad lobbied hard against the Clipper chip, encryption export controls, and bills proposing domestic regulations. They will do so again unless they are convinced the approach makes sense and is in their best interests. Even with the threat of additional terrorist attacks looming over our heads, people will not support encryption controls unless they are convinced that controls are necessary and would be effective, safe, and internationally supported.

--

Dorothy E. Denning (denning@georgetown.edu) is the Callahan Family Professor of Computer Science and Director of the Georgetown Institute for Information Assurance at Georgetown University, and a member of *Information Security*'s Editorial Advisory Board. She has testified before Congress on encryption issues and was a member of the PECSENC.