Online Ethics Center
FOR ENGINEERING AND SCIENCE

Encryption Issues (Sample Scenarios from the CSTB)

Rights and Responsibilities of Participants in Networked Communities

Author(s)

Anonymous

Year

1994

Description

One of 5 scenarios that discuss computers and internet privacy, sampled from a publication of the Computer Science and Telecommunications Board (CSTB).

Body

A university is connected to the Internet. Under a joint effort of its alumni relations and industrial liaison program, the university also provides library and Internet access for Company X, a small start-up business founded by university alumni, in return for stock options in Company X. To facilitate private communications, the university provides RSA-based public-key encryption software on its host computers, encourages the software's use, and maintains databases that facilitate the lookup of the public keys of all users using the university as a node. ("RSA" refers to a type of highly secure public-key encryption scheme that is widely available in the U.S. and elsewhere. Software that implements RSA encryption/decryption algorithms may be subject to U.S. export control laws.)

Questions

1. A foreign national in Iraq accesses the university system and downloads the encryption software. Who has violated what law? What obligation does the university have to report the incident? To configure its system to prevent a recurrence?
2. Encrypted messages are sent from Company X, based in the U.S., to a client located in Brussels. The client uses decryption software obtained locally. Any violation?
3. The FBI requests access to the university's records regarding who has requested the public keys of a particular client of Company X. Should the university cooperate? Must the FBI use any particular process to compel disclosure? What standard should apply to such requests? Is the standard different if the request is made to Company X?
4. The FBI determines that a staff member of the university and a client of Company X, unbeknown to these institutions, are using the electronic communications system to plan a terrorist act, The FBI demands access to the private keys that will allow them to monitor encrypted communications between the parties, They have a search warrant, Is it feasible/lawful to comply? May the system providers require registration of private keys for purposes of allowing compliance with such warrants? May the government require such registration?
5. Company X uses the authentication capability of public-key encryption to determine that requests for assistance actually come from its clients. The university, which administers the database of public keys, does a sloppy job, and a prankster obtains the private keys of the officers of Company X. In consequence, a student prankster sends a request for information that appears to be from a client of Company X, but is not. Company X discloses confidential information to the prankster, who then reveals this information publicly. As a result, Company X incurs costs, based on its assumption that the message is genuine. Who is liable to whom?

Notes

This scenario was excerpted from the NRC report entitled Rights and Responsibilities of Participants in Networked Communities (NAP 1994). Each scenario in the report includes additional materials and commentaries on the significant issues.

Rights

Use of Materials on the OEC

Discipline(s)

Computer Sciences
Computer, Math, and Physical Sciences