Electronic Vandalism (Sample Scenario from the CSTB)

Rights and Responsibilities of Participants in Networked Communities

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). A dial-in electronic bulletin board is used for legitimate and harmful activities. Who monitors the bulletin board?

Body

A computer club at a local high school sets up a dial-in bulletin board, using equipment bought for the club by a banker whose son is club president. The bulletin board is set up at the club president's home, and it can exchange messages with other bulletin boards across North America. The banker also has a computer system for working at home and that is tied directly into the club's computer; the bankers computer is used to write a public newsletter for his bank. The telephone number of the bulletin board is distributed through a national magazine, and over time, the following activities are taking place on the bulletin board, though no club members are involved in any of these activities:

- Stolen credit card numbers are posted.
- Hate messages are sent to Canada, where such messages are illegal.
- A program is posted in a public space by Joe, a non-member. Others download

the program and discover that it contains a virus that causes considerable damage.

- A second program is posted that is designed to disrupt network services when run on a computer connected to a national network such as Internet or Prodigy.

Questions

1. What responsibilities do club members have to monitor the activities on their bulletin board? What actions are various parties obligated to take? Actions might include removing virus-laden programs, notifying authorities, and/or enabling authorities to monitor activities. The various parties include the club members, the club president, and the banker who provided the equipment.
2. What is Joe's individual liability for his program posting? Does it depend on whether or not he knew about the damaging potential of the program?
3. What are the rights and responsibilities of law enforcement officials in investigating the criminal activities described above? What jurisdiction applies when an illegal act is committed by a person living in one area and accessing a computer located in another? What if one end of the connection is overseas? How should the execution of a search warrant proceed in collecting evidence from a computer that may have been used in the commission of a crime? If a computer is seized and it contains both information of evidentiary value and information that has been collected for the public newsletter, how should those materials be treated? Under what circumstances can law enforcement authorities seize the banker's computer for evidence?

Consider changes in the answers to these questions if:

- The dial-in bulletin board is replaced by a university-owned computer system tied to the Internet.
- The dial-in bulletin board is replaced by several public forums on a commercial network service provider such as Prodigy.

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

Resource Type

Case Study / Scenario
Mini-case
Open-ended scenario

Parent Collection

Sample Scenarios on Social Issues Surrounding Internet Privacy

Topics

Ethics and Society
Privacy and Surveillance
Public Well-being

Discipline(s)

Computer Sciences
Computer, Math, and Physical Sciences
Information Sciences
Social and Behavioral Sciences