it should be allowed to take place. Discussion of gambling forces public policy makers to deal with issues as diverse as addiction, tribal rights, taxation, senior living, professional and college sports, organized crime, neurobiology, suicide, divorce, and religion."[19] Due to its controversy, gambling is either banned or heavily controlled on local or national levels. The accessibility of the internet and its ability to cross geographic-borders have led to illegal online gambling, often offshore operations.[20] Over the years online gambling, both legal and illegal, has grown exponentially which has led to difficulties in regulation. This enormous growth has even called into question by some the ethical place of gambling online.

Related organizations

The following organizations are of notable interest in cyberethics debates:

- International Federation for Information Processing (IFIP)

- Association for Computing Machinery, Special Interest Group: Computers and Society (SIGCAS)

- Electronic Privacy Information Center (EPIC)

- Electronic Frontier Foundation (EFF)

- International Center for Information Ethics (ICIE)

- Directions and Implications in Advanced Computing (DIAC)

- The Centre for Computing and Social Responsibility (CCSR)

- Cyber-Rights and Cyber-liberties

- *International Journal of Cyber Ethics in Education* (*IJCEE*)[21]

- The Center for Digital Ethics and Policy (CDEP) [22]

Codes of ethics in computing

Four notable examples of ethics codes for IT professionals are listed below:

RFC 1087

In January 1989, the Internet Architecture Board (IAB) in RFC 1087, titled "Ethics and the Internet," defines an activity as unethical and unacceptable if it:

1. Seeks to gain unauthorized access to the resources of the Internet.

2. Disrupts the intended use of the internet.

3. Wastes resources (people, capacity, computer) through such actions.

4. Destroys the integrity of computer-based information, or

5. Compromises the privacy of users.[23]

The Code of Fair Information Practices

The Code of Fair Information Practices[24] is based on five principles outlining the requirements for records keeping systems. This requirement was implemented in 1973 by the U.S. Department of Health, Education and Welfare.

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for a person to find out what information about the person is in a record and how it is used.

3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.[25]

Ten Commandments of Computer Ethics

The ethical values as defined in 1992 by the Computer Ethics Institute; a nonprofit organization whose mission is to advance technology by ethical means, lists these rules as a guide to computer ethics:

1. Thou shalt not use a computer to harm other people.

2. Thou shalt not interfere with other people's computer work.

3. Thou shalt not snoop around in other people's computer files.

4. Thou shalt not use a computer to steal.

5. Thou shalt not use a computer to bear false witness.

6. Thou shalt not copy or use proprietary software for which you have not paid.

7. Thou shalt not use other people's computer resources without authorization or proper compensation.

8. Thou shalt not appropriate other people's intellectual output.

9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.

10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.[26]

(ISC)² Code of Ethics

(ISC)², a professional association which seeks to inspire a safe and secure cyber world,[27] has further defined its own code of ethics. The code is based on four canons, under a general preamble.

Code of Ethics Preamble:

The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

Canon One: Protect society, the common good, necessary public trust and confidence, and the infrastructure.

Canon Two: Act honorably, honestly, justly, responsibly, and legally.

Canon Three: Provide diligent and competent service to principles.

Canon Four: Advance and protect the profession.[28]

See also

- Computer crime

- Computer ethics

- Cyberpeace

- Data care

- Digital rights

- E-democracy

- Ethics of technology

- Information privacy law

- International Freedom of Expression Exchange