



Chapter 5

Copyright, Piracy, Privacy, And Security Issues: Acceptable Or Unacceptable Actions For End Users?

Jennifer Kreie and Timothy Paul Cronan
University of Arkansas

End user acceptable/unacceptable behavior related to computer information systems has caused significant losses to business and society. Some measures have been suggested to prevent losses or discourage unethical behavior. One approach is to identify factors that might better explain acceptable/unacceptable actions. In this study, we examined models of ethical behavior and selected factors from these models that might influence decision-making. We conducted an empirical study to determine perceptions of acceptable or unacceptable behavior and which factors were significant in influencing a person's judgment of acceptable/unacceptable behavior. Identifying the factors that influence ethical decision-making is one approach suggested by researchers to find ways to discourage unethical behavior and help businesses prevent losses. The results of the study indicate there are significant factors that affected individuals' assessment of what is acceptable behavior. The results also indicate that the factors which were influential were contingent on the characteristics of the ethical dilemma.

Computer-based information systems are ubiquitous in business and are becoming so throughout society. The proper use of computers has been beneficial to businesses, but misuse, and unethical behavior related to

Previously Published in the *Journal of End User Computing*, vol.11, no.2, Copyright © 1999, Idea Group Publishing.

This chapter appears in the book, *Ethical Issues of Information Systems* by Ali Salehnia.
Copyright © 2002, IRM Press, an imprint of Idea Group Inc.

information systems (IS) have caused significant losses to businesses and society. Fortune magazine (February 1997) recently reported on an actual breach of security to illustrate how easily a business' information system could be accessed and misused.

Estimates for the annual cost of computer crime are in the billions. Though organizations have invested in the development and implementation of security measures, computer misuse will likely continue to be a problem throughout the 1990s (Straub and Nance, 1990). From a professional and social perspective, IS professionals are concerned about the problem of illegal and/or unethical use of computers because of the potential harm to society and to the integrity of the IS profession. There has been research in the area of computer misuse and computer ethics in recent years from several perspectives, such as the ethical attitudes of personnel, deterrents to unethical behavior, the various types of unethical behavior, and approaches to teaching ethics in the field of MIS (Zalud, 1984; Saari, 1987; Aiken, 1988; Heide and Hightower, 1988; Cougar, 1989; Oz, 1990; Paradice, 1990; Straub and Nance, 1990; Conner and Rumelt, 1991).

In an effort to prevent or discourage improper and unethical use of computers several measures have been suggested—enhanced security, prompt and fair reporting, tougher sanctions, and codes of conduct for IS professionals (Anderson, et al., 1993; Straub, 1990). It would also be beneficial to identify the ethical issues that pertain to computer use and include ethics in the IS curriculum (Parker, 1980; Cougar, 1984). This would help to make future IS professionals more aware of ethical issues. A better understanding of what factors influence our decision to act in one way or could, perhaps, provide some guidance for discouraging unethical behavior. For example, it would be beneficial to know whether a code of ethics for IS professionals has a significant impact on a person's decisions and behavior.

The current study is part of an ongoing research effort to identify factors which affect the ethical behavior of individuals when these individuals are faced with ethical dilemmas involving different aspects of computing. The purpose of the present study is to examine factors proposed in several models of thical/unethical decision-making, several of which have not been empirically tested, and determine what factors are significant in the judgment of what is acceptable or unacceptable behavior. In the present study, participants were presented with an IS dilemma and a response. Participants were asked to judge the response as "acceptable" or "unacceptable" and to indicate what factors influenced their decision.

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/copyright-piracy-privacy-security-issues/18570

Related Content

Information Privacy in a Surveillance State: A Perspective from Thailand

P. R. Rananand (2007). *Information Technology Ethics: Cultural Perspectives* (pp. 124-137).

www.irma-international.org/chapter/information-privacy-surveillance-state/23659

Ethical Theories and Computer Ethics

Matthew Charlesworth and David Sewry (2009). *Handbook of Research on Technoethics* (pp. 186-204).

www.irma-international.org/chapter/ethical-theories-computer-ethics/21580

Social and Existential Threats to Personal Security in Virtual Communities: "Groups of Death" and "Columbine Communities"

Liudmila Vladimirovna Baeva (2020). *International Journal of Technoethics* (pp. 1-16).

www.irma-international.org/article/social-and-existential-threats-to-personal-security-in-virtual-communities/258844

IT and Globalized Ethics

Robert A. Schultz (2010). *Information Technology and the Ethics of Globalization: Transnational Issues and Implications* (pp. 129-139).

www.irma-international.org/chapter/globalized-ethics/39897

A Theodicy for Artificial Universes: Moral Considerations on Simulation Hypotheses

Stefano Gualeni (2021). *International Journal of Technoethics* (pp. 21-31).

www.irma-international.org/article/a-theodicy-for-artificial-universes/269433