


Predicting and Explaining Cyber Ethics with Ethical Theories

Winfred Yaokumah, University of Ghana, Accra, Ghana

 <https://orcid.org/0000-0001-7756-1832>

ABSTRACT

People face multiple decisions that have ethical dimensions and are often unable to resolve appropriately those ethical dilemmas in the use of the cyberspace. Individuals find it difficult to explain the rationale behind their moral judgments in their interactions and access to digital content. Identifying ethical and moral orientation that prompts acceptable or unacceptable ethical judgments is an important factor in cyber ethics. The goal of this study is to employ three prominent ethical theories to predict and explain cyber ethical judgements in terms of computer ethics, privacy, intellectual property rights, and academic integrity. The study develops conceptual and predictive models to test a set of hypotheses. The results show consequential ethics as the most significant predictor of computer ethics, cyber privacy, and academic integrity. Deontological ethics most significantly predict intellectual property rights but is not a significant predictor of academic integrity.

KEYWORDS

Academic Integrity, Consequentialism, Cyber Ethics, Cyber Security, Deontology, Ethical Theory, Intellectual Property, Piracy, Plagiarism, Privacy, Virtue Ethics

INTRODUCTION

Individuals face ethical dilemmas in various real-life situations and often make ethical judgments based on what they deem to be right or wrong. Ethics is a set of principles by which people live; what they consider as morally right or wrong; their judgments about what ought to be done; and about moral duties and obligations people should perform (Heller, 2012). Digital transformation through the use of information and communication technologies, though improves critical business operations and economic growth, poses ethical challenges to the society (Tiirmaa-Klaar, 2016). In particular, interactions among people and access to digital content in the cyberspace bring ethical concerns (Jamal et al., 2015). Some decisions and choices individuals make in the cyberspace are unethical or illegal (Luppardini, 2009). Often, individuals are unable to resolve ethical dilemmas (Arar et al., 2016). In some cases, people find it difficult to explain the rationale behind their moral judgments in their accessibility and interactions with digital content. It is often hard to conclude what ought to be the most appropriate ethical behaviour. This is because differences exist among individuals in their judgements and even among cultures as to what is right or wrong (Burmeister, 2017).

Ethics in the cyberspace is often referred to as cyber ethics. Cyber ethics is a term used to encompass all forms of applied ethics issues pertaining to technology related human activities (Luppardini, 2009). Cyber ethics tries to determine an appropriate perspective or philosophy in the application of technology to real-life situations (Shapiro & Gross, 2013). Ethical theories are useful when faced with alternative perspectives for evaluating and resolving ethical situations (McDonald,

DOI: 10.4018/IJCWT.2020040103

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

2014). As people face multiple decisions that have ethical dimensions in the cyberspace, it is important to establish what ethical theoretical perspectives and moral convictions that prompt acceptable or unacceptable ethical judgments. Ethical theories enable individuals to defend or oppose a position on a particular ethical issue (Hammersley-Fletcher, 2015) in the cyberspace. According to Amin (2019), providing cyber safety requires four interrelated domains: a) hardware, software, and networks as building blocks of the organization's cyber infrastructure; b) the information domain which includes monitoring, information storage, and visualization; c) the cognitive domain which involves information analysis for decision-making; and d) the social domain where appropriate social and ethical considerations are made.

This current study focuses on the ethical domain of cyber security to predict and explain cyber ethics using ethical theories. Literature suggest that among several ethical theories, consequentialism, deontology (Heller, 2012) and virtue ethics (Audi, 2015) are the most relevant to technological applications. Consequentialism (consequence-based ethics) refers to those moral theories which hold that the consequences (i.e. outcomes) of a particular action form the basis for any valid moral judgment about that action or create a structure for judgment (Sinnott-Armstrong, 2014). Deontological ethics (duty-based ethics) are concerned with what people should do, not with the consequences of their actions (Alexander & Moore, 2015). It focuses on doing the right thing because it is the right thing to do (Alexander & Moore, 2015). Virtue ethical theory (character-based ethics) focuses on the criteria having to do with character development of individuals and the acquisition of good character traits (Hinmann, 2016). This study employs these three prominent ethical theories to predict and explain ethical judgements of individuals in the use of the cyberspace. The question the study attempts to answer is "How do ethical theories predict and explain cyber ethics?" Empirical evidence to predict and explain the effect of ethical theories on cyber ethics is lacking in the literature. As a consequence, full ethics is needed in the field of cyberspace (Dipert, 2016) and more research is required to explore appropriate ethical theories that can foster cyber ethics (Burmeister, 2017).

LITERATURE REVIEW

Ethical Theories

Ethical theories are generally categorized into three: Consequentialism, deontology, and virtue ethics (ethics of character). Consequentialism and deontology answer a question as to "how should I act?" and the virtue ethics answer a question as to "what kind of person ought I to be?" (Hinmann, 2016).

Consequentialism

Consequential ethics contends that people should strive to maximize positive outcomes (Sinnott-Armstrong, 2014). It is based on two principles: (a) whether an act is right or wrong depends only on the results of that act and (b) the more good consequences an act produces, the better or righter that act (Ethics guide, 2014). Consequentialism is categorized into utilitarianism, group consequentialism, and ethical egoism (Hinmann, 2016). For utilitarianism, an action is right if it tends to promote happiness and wrong if it tends to produce reverse of happiness (Driver, 2014; Mill, 1961). With this view, an act is morally permissible if the consequences resulting out of it produces greatest amount of good for the greatest number of persons affected by the act (Sinnott-Armstrong, 2014). Utilitarianism plays a very important part in everyday life because it is simple and appeals to common sense: (a) It seems sensible to base ethics on producing happiness and reducing unhappiness, (b) It seems sensible to base ethics on the consequences of what is done, since people usually take decisions about what to do by considering what results will be produced, and (c) It seems easy to understand and which is based on common sense (Ethics guide, 2014). Another aspect of consequentialism is group consequentialism, which considers consequences of an act on smaller groups such as a nation, a tribe, a family, or

16 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/article/predicting-and-explaining-cyber-ethics-with-ethical-theories/250905

Related Content

International Law and Cyberoperations: French View

Martina Smuclerova (2021). *International Journal of Cyber Warfare and Terrorism* (pp. 1-20).

www.irma-international.org/article/international-law-and-cyberoperations/289383

Social Media Networking and Tactical Intelligence Collection in the Middle East

Karen Howells (2019). *International Journal of Cyber Warfare and Terrorism* (pp. 15-28).

www.irma-international.org/article/social-media-networking-and-tactical-intelligence-collection-in-the-middle-east/231641

A Study of Good-Enough Security in the Context of Rural Business Process Outsourcing

Reena Singhand Hemant Jalota (2018). *Psychological and Behavioral Examinations in Cyber Security* (pp. 239-252).

www.irma-international.org/chapter/a-study-of-good-enough-security-in-the-context-of-rural-business-process-outsourcing/199892

A Classification Framework for Data Mining Applications in Criminal Science and Investigations

Mahima Goyal, Vishal Bhatnagarand Arushi Jain (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 277-293).

www.irma-international.org/chapter/a-classification-framework-for-data-mining-applications-in-criminal-science-and-investigations/251432

Ascertaining Trust Indicators in Social Networking Sites

N. Veerasamyand W. A. Labuschagne (2013). *International Journal of Cyber Warfare and Terrorism* (pp. 22-37).

www.irma-international.org/article/ascertaining-trust-indicators-in-social-networking-sites/101938