THE ETHICAL RESPONSES OF STUDENTS TO UNIVERSITY ICT CODES OF CONDUCT

Salma Banu Nazeer Khan, Deborah Richards, Paul Formosa and Sarah Bankins,

Macquarie University, Australia

ABSTRACT

Governments, organisations, and universities implement cybersecurity laws, regulations, policies, and processes to reduce their cyber risks. In the context of universities, students sign, usually before commencement of enrolment, various agreements including Information and Communication Technology (ICT) codes of conduct. However, individuals can ignore, circumvent, or act contrary to these codes due to a lack of awareness of the possible consequences of such contraventions, but also due to a lack of sensitivity to the ethical principles underpinning such codes. Therefore, there is a need to understand why students and other users are not compliant with ICT codes of conduct and how to change the behaviour of students and other users so that they act ethically and in accordance with ICT codes. We designed a between-subjects experiment involving students' responses to 5 scenario pairs (breach/no breach of ICT code of conduct) following awareness training of ethical principles, or awareness training of acceptable use of IT, or no awareness training (control) to understand the potential value of training. Furthermore, we profile students to capture their moral stance and measure their attitudes towards their university's IT services and resources to understand individual differences that may affect their cybersecurity behaviour.

Keywords: Information Communication Technology Code of Conduct, cyberethical scenarios, AI4People ethical principles, AI ethics, cybersecurity ethics, moral sensitivity, ethics training

1. INTRODUCTION

Information and Communication Technology (ICT) codes of conduct are policies and rules applied in most organisations, including governments and universities. Employees, staff, and students within universities are generally required to agree to abide by these ICT codes of conduct. Recent studies (Wilk, 2016, Neigel et al., 2020) have shown that there is a pressing need to enhance cyber education among students to generate better understanding of cybersecurity ethical principles and to support their digital skills both in their personal and professional lives. In a university context, it is therefore critical to educate students on ethical aspects of cybersecurity to support code compliance (Wilk, 2016). Further, it is well recognised that there is a lack of awareness and knowledge about practicing good cyber hygiene amongst young adult users, which may result in cybersecurity risks (Cain et al., 2018). However, what is not well understood is why students and other users are not compliant with the ICT policies and procedures that have been put in place to protect a university's ICT assets. To address this, we have developed an ongoing research study which is focused on two areas. First, to examine how to create student awareness of the ethical ramifications of violating a university's ICT principles. Second, to investigate the effectiveness of strategies to change the behaviour of students and other users so that they act more ethically and in accordance with ICT codes of conduct.

2. BACKGROUND

2.1 ICT Code of Conduct

ICT are technological resources and applications. Recent developments in ICT "have made possible a transition in information storage, processing and dissemination to help human activities" (Sembok, 2004). However, there is growing concern over digital assets being used inappropriately and potentially illegally, including by students at universities, causing threats to ICT infrastructure and Intellectual Property Rights (IPR) (Sembok, 2004). Unlimited or unrestricted access to the internet is the primary source of this threat. Thus, it is necessary for ICT users to know about the ethical standards and rules that they need to follow to minimise such threats (Pólkowski, 2015). An empirical study conducted by Bia and Kalika (2007) showed that factors such as structure, standard, technology, and size of the organisation are the key causes driving high or low adoption of ICT codes of conduct. Measures to create awareness of and educate users about the importance of ICT codes of conduct are needed. A survey was conducted by Rezaee et al. (2001) to examine the importance and implications of codes of conduct in higher educational institutions. The surveys were mailed to vice-presidents of finance departments of colleges and universities (C&U), as these individuals have knowledge about their institution's code of conduct and ethical policies (Rezaee et al., 2001). They found 70 percent of C&U's had ethical guidelines written in their codes of conduct and 61 percent of the responses indicated their compliance with the guidelines (Rezaee et al., 2001). Further research is needed to examine the awareness and compliance with the code among students and faculty more broadly (Rezaee et al., 2001). A study conducted by Neigel et al. (2020) on cyber hygiene practices by university students showed that human factors, such as individual knowledge and motivation, can influence the practicing of good cyber hygiene. Cyber education awareness thus needs to be provided to students so that they understand and practice good cyber hygiene (Neigel et al., 2020). Furthermore, students need to understand how their organisation's ICT code of conduct creates expectations about their cyber hygiene practices. For example, does the code require them to report phishing attacks or ignore them? An approach we recommend to improve compliance with ICT codes of conduct is to inform students of their expected cyber behaviours under the code and the ethical principles embedded within the policies they are agreeing to abide by. In our study we will use a university's ICT code of conduct policy to explore this issue.

2.2 Ethics and ICT

Despite the continuing advances in computer technology, there remains a lack of adequate and universal guidance on the principles and policies needed to enact ethical computing (Pólkowski, 2015). Some recent examples are the additional use of security surveillance for monitoring staff, and the increasing use of Artificial Intelligence (AI) agents which raises questions around the accessibility and transparency of their actions (Rogerson, 2011). During the current pandemic, government initiatives to develop contact tracing data collection surveillance systems have challenged IT professionals to support society while acting ethically, being transparent, and building the trust necessary for success (Wigan, 2020). Principlist approaches to ethics are common in many areas of applied ethics, especially in bioethics where the four ethical principles of beneficence (benefiting people), non-maleficence (not harming people), autonomy (allowing choice and consent), and justice (being fair and unbiased), first introduced by Beauchamp and Childress (Floridi and Cowls, 2019), have been widely used for many years. Recently this applied ethics framework has been adapted to the context of ethical computing by the AI4People's Unified Framework of Principles for AI in Society ((Floridi et al., 2018) and (Floridi and Cowls, 2019)). In addition to the above four principles, this framework adds the fifth ethical principle of explicability, which is an important addition in the area of ethical computing because computing devices can act as agents in their own right, which raises issues about the accountability and intelligibility of their actions. The importance of the fifth principle has come to the forefront currently with the current interest in machine learning, and particularly deep learning using neural networks that are typically black boxes due to the use of hidden layers. However, providing explanation has been a key element of AI at least since expert systems were introduced in the 1980s, with explicability being a purported advantage due to their ability to answer “why” a question was asked and “how” a conclusion had been reached (Richards, 2003). Similarly, machine learning algorithms that produced decision-trees were also able to explain their reasoning. More recently, explainable virtual agents are able to explain why they have made certain recommendations in order to encourage or persuade the user to take certain actions (Abdulrahman and Richards, 2019). While our study is focused on the ethical use of university computing resources by student users, and not ethical AI specifically, given that we are investigating a closely related area of ethical computing, it is appropriate to draw on this well-established ethical framework for our study.

2.3 Training in Cybersecurity Ethics

Even though many universities have added information ethics into their curriculum, there is still a need for training dedicated to the ethical issues of ICT usage (Pólkowski, 2015). This training needs to include awareness of the ICT code of conduct, good cyber hygiene practices, and how the two are related (e.g. what constitutes a breach and how to manage breaches). It is recommended that universities provide education on computer ethics to students, academics, and other employees, and also raise awareness of past cybercrime breaches (Pólkowski, 2015). Previous research has also shown that there is a need for training students to learn how to address dilemmas relating to ethical and cyber issues, particularly in the case of students studying to be future cybersecurity professionals (Blanken-Webb et al., 2018). A survey conducted by Cain et al. (2018) to assess the knowledge of users on cyber hygiene showed that more effective training on cyber hygiene is required, especially among younger users, to create awareness of best practices for effective cyber hygiene. In recent times, Association for Computing Machinery’s (ACM) Education Board and Council formed the Cyber Education Project (Richards and Ekstrom, 2015) to develop curriculum on cyber science (cyber related areas: cyber security, cyber operation, security coding, etc). However, cyber education is not provided to all students and the ethical concerns relating to cybersecurity decisions are often missing from even Cyber Science curriculums (Mead et al., 2015).

McNamara et al. (2018) conducted a study of the ACM's code of ethics with 63 software engineering students and 105 software developer professionals to measure participant's decision-making responses to 11 ethical vignettes on ethical issues in software development. The authors' study is built on Peslak's (Peslak, 2007) investigation of student's ethical decision making when exposed to ACM's code of ethics. McNamara et al. (2018) found that extensive research and interventions are still required to improve ethical decision making and to help individuals to identify the ethical consequences of their decision.

3. AIMS AND APPROACH

The aim of this research is to understand how students' moral integrity and moral foundations relate to their ethical choices in terms of decisions relevant to compliance with their university's ICT code of conduct. We also explore whether ethical training is beneficial for increasing sensitivity to the ethical principles embedded in ICT codes of conduct and whether this increases compliance with the Code. We will address the following research questions (RQ).

RQ1: How can student/user sensitivity to the ethical principles underlying their behaviour towards usage of IT resources be measured?

RQ2: Can we predict when students/users are most likely to breach certain ICT policies?

RQ3: Does (1) ethics awareness or (2) ICT policy awareness change students' judgements about ICT policy compliance?

To answer RQ1, we will connect a university's ICT code of conduct to underlying ethical principles, by drawing on the five ethical principles in the AI4People framework, and create scenarios that involve ethical dilemmas that both accord with and are in breach of one or more of these five ethical principles. Design of the scenarios are described further in section 3.1.

To answer RQ2, we will capture profiles of the participants to understand their moral stance and measure their attitudes towards their university's IT services and resources. We will look at whether they "care" about their university's ICT resources or feel an obligation to protect their university's reputation from damage as potential moderators between their ethical principles and actions. We want to explore if there are students who care about ethical obligations in general, but who feel apathetic or negatively towards acting ethically in relation to their university's ICT resources in particular scenarios. The data to be collected to profile participants is described further in section 3.2.

To answer RQ3, prior to interacting with the scenarios, participants will be divided into three groups: group one (G1) receives only information about the code of conduct beforehand; group two (G2) receives only information about relevant ethical principles; and group three (G3- control) receives no information. The participants will be randomly and evenly allocated to one of the three groups.

3.1 Scenario Creation

Scenarios are designed to connect the ICT policy of the university to underlying ethical principles. Five scenarios were created to address the five ethical issues outlined in the AI4People framework.

There are five basic ethical principles that are often used when thinking about ethical computing. ICT policies can be designed to ensure that people use computing technologies in ways that are compatible with these five ethical principles. They are:

Beneficence: Computing technology should be beneficial to humanity and it should promote human well-being. It should be used to make our lives better.

Non-maleficence: Computing technology should not be used to intentionally harm humanity. It should not be used to make our lives worse.

Autonomy: Computing technology should be used to promote human autonomy. It should allow humans to decide for themselves how to use that technology in their lives.

Justice: Computing technology should promote fairness, equality, and impartiality. It should not unfairly discriminate, undermine solidarity, or prevent equal access.

Explicability: Computing technology should operate in ways that are intelligible, transparent, and comprehensible, and it should be clear who is accountable and responsible for how it functions.

Each of the five scenarios consists of two versions (scenario-pair), one version with a breach and one version without a breach of the university's ICT code of conduct based on the Schedule of Breaches under "Acceptable Use of IT Resources Policy and Acceptable Use of IT Procedure". Four individuals (three academics and one Masters of Research candidate) were involved in creating and reviewing the scenarios. The team considered which ethical principles were captured in each scenario to ensure that all five principles were covered. Most scenarios captured more than one ethical principle due to the complexities involved. Participants were asked to respond to a 7-point Likert scale (1=strongly disagree, 7=strongly agree) regarding their agreement with the behaviour described in the scenario and to provide a free text response as to "why" they made that choice. An example of a scenario-pair and the ethical principles encapsulated for the breach is provided in Table 1. To avoid introducing bias, students are not shown the ethical principle/s assigned to a scenario.

A student enrols in a web design unit at University. While studying, they are also working for a company that builds commercial websites. Their employer has assigned them a project to build an eCommerce website. The student builds and tests the website on University servers which are accessible to students for their academic studies. The student continues to host the website on University servers when the site goes live to the public.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither disagree nor agree (4)	Somewhat Agree (5)	Agree (6)	Strongly agree (7)	No position / Refused
O	O	O	O	O	O	O	O

*Why*____

A student enrols in a web design unit at University. While studying, they are also working for a company that builds commercial websites. Their lecturer has assigned the student a project to build an eCommerce website. The student builds and tests the website on University servers which are accessible to the students for their academic studies. The student continues to host the website on University server until their lecturer can assess it.

Is using University IT services and resources for this purpose something you agree or disagree with?

Strongly disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither disagree nor agree (4)	Somewhat Agree (5)	Agree (6)	Strongly agree (7)	No position / Refused
O	O	O	O	O	O	O	O

*Why*____

[Ethical relationship - major: Non-maleficence; minor: Justice]

Table 1: A scenario pair for Acceptable Use of IT Resources Policy and Acceptable Use of IT Procedure breach (a) use for any purpose other than an authorised purpose

In the first case we have a scenario with a breach and in the second case we have a scenario without any breach of the ICT code of conduct. The participants will each receive all 10 scenarios, but we have created a fixed order of presentation to ensure the breach and no breach alternatives are spaced at a maximum distance apart and also that breach and no breach cases are interleaved. A participant scoring high (7=strongly agree) on the Likert scale indicates the participant's non-compliance towards their university's ICT code of conduct and associated ethical principles and vice versa for scoring low (1=strongly disagree). This scenario maps on to the university's IT policy that states ICT resources should not be *"use[d]* *for any purpose other than an authorised purpose"* and this relates to the ethical principles of non-maleficence (major) and justice (minor) as unauthorised uses could harm others and violate rights. The free text option allows us to interpret the quantitative score and encourages participants to reflect on their response to uncover their ethical considerations. We anticipate their responses will allow us to determine if they identified the same ethical principle/s in the scenarios that we identified.

3.2 Profiling of Participants

The data on participants' knowledge of cyber hygiene is collected with the Cyber Hygiene Inventory (CHI) scale (Vishwanath et al., 2020) (5-point Likert scale of never to always). Participants ethical integrity is collected by using Schlenker's (2008) Integrity scale (5-point Likert scale of strongly disagree to strongly agree), where higher scores on the scale reflects a stronger commitment to ethical principles and a lower score indicates a higher willingness to breach ethical principles. Next is the Institutionalization of Ethics scale (Singhapakdi and Vitell, 2007) which includes implicit and explicit dimensions of ethics, which measures the implementation of ethics in organisation and evaluates its dimension, reliability, and authenticity. The implicit dimension refers to ethical behaviour that is not expressed directly (i.e., through ethical aspects of organization and its top management). The explicit dimension refers to ethical behaviour expressed formally with no ambiguity (i.e., formal ethical training within the organization). Participants are given only the implicit statements as explicit questions are appropriate for employees but not for students. Using this scale, we measure the student's awareness of the importance of ethics within their university using a 5-point Likert scale of strongly disagree to strongly agree. Next we use the short version (MoralFoundations.Org) of the Moral Foundation Questionnaire (Graham et al., 2011), to produce data on how strongly the students' rate each of the five moral foundations (care/harm, fairness/cheating, loyalty/betrayal, authority/subversion, and sanctity/degradation). The MFQ will provide a broad ethical profile of participants.

4. CONCLUSION AND FUTURE WORK

The outcome of the study will be to understand how user's ethical integrity and moral foundations relate to their ethical choices concerning compliance with ICT codes of conduct. We have recently obtained approval from our university's Human Ethics Committee to conduct an experiment with university students of the Psychology department and students enrolled in our "Introduction to Cyber Security unit". If the student is from the Psychology pool, they will receive 30 minutes of course credit for participation. No compensation or reward can be offered to other participants. Participants will be assigned to one of the three groups, one that receives brief training and a short quiz concerning the university's ICT code of conduct, another that receives brief training on the five ethical principles from the AI4People framework applied to ethical computing, and a control group that receives no training. The scenarios and survey will be deployed online using the Qualtrics Survey Software (QSS). Participants will be randomly and evenly assigned to one of the three groups. Through profiling of the participants, we aim both to shed light on how different cohorts respond to various ICT ethical dilemmas and to assess the value of ethical training to sensitise individuals to ethical principles embedded in ICT codes of conduct. This research could potentially help universities to minimise cybersecurity risks to themselves and society.

5. REFERENCES

ABDULRAHMAN, A. & RICHARDS, D. Modelling Therapeutic Alliance using a User-aware Explainable Embodied Conversational Agent to Promote Treatment Adherence. Proceedings of the 19th ACM International Conference on Intelligent Virtual Agents, 2019. 248-251.

BIA, M. & KALIKA, M. 2007. Adopting an ICT code of conduct. *Journal of Enterprise Information Management,* 20**,** 432-446.

BLANKEN-WEBB, J., PALMER, I., DESHAIES, S.-E., BURBULES, N. C., CAMPBELL, R. H. & BASHIR, M. A Case Study-based Cybersecurity Ethics Curriculum. 2018 (USENIX) Workshop on Advances in Security Education (ASE18), 2018.

CAIN, A. A., EDWARDS, M. E. & STILL, J. D. 2018. An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications,* 42**,** 36-45.

FLORIDI, L. & COWLS, J. 2019. A unified framework of five principles for AI in society. *Harvard Data Science Review*.

FLORIDI, L., COWLS, J., BELTRAMETTI, M., CHATILA, R., CHAZERAND, P., DIGNUM, V., LUETGE, C., MADELIN, R., PAGALLO, U. & ROSSI, F. 2018. AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines,* 28**,** 689-707.

GRAHAM, J., NOSEK, B. A., HAIDT, J., IYER, R., KOLEVA, S. & DITTO, P. H. 2011. Mapping the moral domain. *Journal of personality and social psychology,* 101**,** 366.

MCNAMARA, A., SMITH, J., MURPHY-HILL, E. & Does ACM's code of ethics change ethical decision making in software development? Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 2018. 729.

MEAD, N. R., GIBSON, D. S. & HAWTHORNE, E. K. Cyber Sciences and Software Engineering. 2015 IEEE 28th Conference on Software Engineering Education and Training, 2015. IEEE, 21-23.

MORALFOUNDATIONS.ORG. 2013. Available: https://moralfoundations.org/questionnaires/ [Accessed 31-8-2020].

NEIGEL, A. R., CLAYPOOLE, V. L., WALDFOGLE, G. E., ACHARYA, S. & HANCOCK, G. M. 2020. Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security,* 92**,** 101731.

PESLAK, A. R. 2007. A review of the impact of ACM code of conduct on information technology moral judgment and intent. *Journal of computer information systems,* 47**,** 1-10.

PÓLKOWSKI, Z. Ethical Issues in the Use and implementation of ICT. Sankalpa: Journal of Management & Research, ed. R. Khajuria, R. Banerjee i K. Sinha, 4th International Conference on "Business Ethic for Good Corporate Governance & Sustainability", Gujarat Technological University, Ahmedabad, 2015. 2-5.

REZAEE, Z., ELMORE, R. C. & SZENDI, J. Z. 2001. Ethical behavior in higher educational institutions: The role of the code of conduct. *Journal of business ethics,* 30**,** 171-183.

RICHARDS, D. 2003. Knowledge-based system explanation: The ripple-down rules alternative. *Knowledge and Information Systems,* 5**,** 2-25.

RICHARDS, J. M. & EKSTROM, J. J. The Cyber Education Project and IT IAS Curriculum. Proceedings of the 16th Annual Conference on Information Technology Education, 2015. 173-178.

ROGERSON, S. 2011. Ethics and ICT. *The Oxford Handbook of Management Information Systems*.

SCHLENKER, B. R. 2008. Integrity and character: Implications of principled and expedient ethical ideologies. *Journal of Social and Clinical Psychology,* 27**,** 1078-1125.

SEMBOK, T. Ethics of information communication technology (ICT). Proceedings of the Regional Meeting on Ethics of Science and Technology, 2004. 239-325.

SINGHAPAKDI, A. & VITELL, S. J. 2007. Institutionalization of ethics and its consequences: a survey of marketing professionals. *Journal of the Academy of Marketing science,* 35**,** 284-294.

VISHWANATH, A., NEO, L. S., GOH, P., LEE, S., KHADER, M., ONG, G. & CHIN, J. 2020. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems,* 128**,** 113160.

WIGAN, M. 2020. Rethinking IT Professional Ethics. *Australasian Journal of Information Systems,* 24.

WILK, A. Cyber security education and law. 2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE), 2016. IEEE, 94-103.