My University, My Facilities: Exploring Student Attitudes to Ethical Usage

AUTHOR
Mary Prior and Mike Leigh

ABSTRACT

Context

Over the past decade there have been several studies into the ethical attitudes of IS professionals [Prior et al, 2002, 2005]. Studies have also been undertaken that include the views of university students in the UK [Prior, 2004, Prior et al, 2008] and in the USA [Grozinsky et al, 2008]. Some of survey instruments used in the studies covered a wide range of computer ethics issues, and were originally designed to be administered to IS professionals before subsequently being used with student subjects. Other survey instruments were designed explicitly to be used with students, but covered only a restricted range of ethical issues. This paper reports a study using a survey instrument explicitly targeted at university students of IS/IT, covering a range of ethical issues. It is also distinguished from previous work in being part of a co-ordinated study across three countries: the UK, USA and Canada.

Research Design

The paper will report the results of a study using a combination of questionnaire and structured interviews. A questionnaire was used as an efficient method of ascertaining the views of a large number of students; structured interviews were used to follow up particular issues raised by the questionnaire results, to probe in more depth the reasons for particular responses [Bryman, 2008].

The questionnaire was based on a survey instrument used in previous studies [e.g. Prior et al 2005]. It presents a series of statements to which the respondent indicates the strength of their agreement/disagreement using a five-point Likert Scale. A process of negotiation was used with collaborating partners to arrive at a set of statements tailored for the study subjects: university students. For example, a new set of statements concerning the use of social networking sites was introduced. Finally, the agreed questionnaire was contextualised at each site to take into account local cultural and/or institutional differences.

The profile of respondents differs in some respects between each of the three geographical sites taking part in the collaborative study. This paper reports responses from students at a UK university. Responses were sought from second and final year undergraduate groups and a postgraduate group. Students were studying on a variety of IT-related courses; the majority were under 25, but some mature students were represented, as were both male and female students. They came from a variety of ethnic backgrounds, with the postgraduate group including a larger proportion of students from outside the UK.

After the questionnaires had been administered they were submitted to a collaborating colleague with statistical expertise and process using a statistical package. The results were analysed and interpreted to identify issues worthy of being followed up in greater depth in the structured interviews.

At the time of preparing this abstract, the structured interviews are not complete; however from the work completed to date some comments can be made on the findings.

Findings

Students appear to hold some views that are worthy of further scrutiny. For example nearly 50% of them agree or strongly agree that it is acceptable to make unauthorised copies of software to use for their university work. As many as 67% say it is acceptable to use the university’s facilities for their own non-profit-making activities. Some 20% do not care about the overall objectives or purpose of a systems development project, so long as it provides them with an interesting challenge – another 25% are indifferent.

Behind the overall figures lie some interesting differences. On some issues, there is a clear difference between the 2nd and final year cohorts, with the latter showing evidence of more ethical awareness. On others, it is the responses of the postgraduate group that differ from the undergraduates. It is possible that on the one hand, the final year students have had more time and experience (most of them have worked for a year in industry as a part of their course) to develop their views; in addition, they may have had their attitudes further developed by undertaking a computer ethics module. On the other, there may be cultural factors at work when it comes to the postgraduate students, many of whom are from the Middle East. These are some of the issues to be pursued in the structured interviews.

Conclusion

This paper is part of an ongoing series of studies into the ethical attitudes of IS professionals, and of students of IS/IT. It differs from previous surveys in being specifically targeted at university students, and being a part of a collaborative study.

The findings are considered important as it explores some of the developing attitudes of tomorrow’s IS professionals. If it is desirable to ensure that the IS professionals of the future adopt an ethical approach to their work, it is important to gain an understanding of how that approach may best be formed and enhanced. To what extent does the study of a computer ethics module help in the formation of a professional, ethical approach to IS/IT-related work? This and its sister studies will help to find an answer to that question.

REFERENCES

The Finnish eVoting Experiment: What Went Wrong?

ABSTRACT

In this paper we analyze the validity of claims made in Finland of benefits from an electronic voting (e-voting) system in the context of the recent election there. We also look at the potential harms from an e-voting system and then compare the benefits with the risks. According to our analysis of the discussion in Finland, legal, ethical and technical experts in the field see the benefits to be marginal, whereas discussion in Finland and elsewhere suggests the harms can be fundamental. The main problem with the assertion is that it has been done without carrying the underlying principles of the paper ballot over to the e-voting system.

Justifications given in Finland for the e-voting system have been the following: ‘cost savings’, ‘activating passive voters’, ‘speed and efficiency of the system’, ‘staying in the front line of ICT-using-nations’, and ‘reliability of counting votes’.

The argument was also made that if the banking system can be made secure, why not the voting system? The possibility to ‘Follow the Estonian way’ where Internet and Mobile Voting were introduced was last hinted at, but never really considered as a justification, although the more passive citizens are to be activated, this seems like a logical next step. All these claims are, of course, prima facie plausible. However, most of them do not stand up to close scrutiny: nor are the problems with the stated justifications the only ones with the e-voting system as it was implemented in Finland.

There are problems with the claims, some major, some minor. Cost savings from using the system are questionable at best. Information Systems tend to need updates and modifications from year to year, and according to official reports, at least for now, there have only been extra costs from the system (Valtiovarainministeriö, 2000-2008). Passive voters would still need to show up to the voting location (as there was no Internet or Mobile voting) thus the novelty may have resulted in some new voters, but this is unlikely to last. Clearly, the system is faster in giving results than the traditional paper ballot. However, the time saved reducing the count from approximately 4 hours to 30 minutes at all or major part of voters use the system, is hardly a major advantage if elections are held once every 48 months. ‘Staying in the front line of ICT’ anything can be questioned to be a true value in itself. Some justification for why it would be valuable is if course needed. Reliability of the system is questionable – already problems have been discovered with the user interface of the system, the system itself is a black box (security through obscurity!) and the functioning which is a mystery to all except the designers and auditors of the system. Internet and/or Mobile voting might actually activate currently passive voters, however, the results from other votes in which these have been used show a jump in activity (novelty value of the technology).

The system is, by definition, much more complex to understand than a paper ballot which can be explained to anyone in 15 minutes. By contrast the software, cryptography, etc. involved in an e-voting system cannot (e.g. Mercuri, 2001 on difficulty to explain systems to laypersons).

Finally, there is the possibility of hidden backdoors in the software. A hostile takeover of the system by either national or external parties is thus much more likely than with traditional paper ballot. Some of the major problems with the e-voting system in Finland are

1. The above mentioned tremendous concentration of capital:
2. The migration of capital to the knowledge producing branches (mentioned earlier)
3. The desire to control the fundamental (strategic) branches of production.

As a result of such an overlap, the global process of the production of knowledge is dominated by individuals and organizations (state-owned as well as privatised) who control immense capital and who are clustered together in particular geographic areas (e.g., United States, Russia, parts of Europe).

We return now to the question asked earlier: What could change in the capitalist system as a result of the revolutionary changes in the collective productiveness of labor? The answer to this question is that the result of changes in the collective productiveness of labor is a new division of labor, which is qualitatively different from the old one. Interestingly enough, this answer doesn’t differ much from some of the predictions about the future of capitalism made in the 19th century, for instance, by Karl Marx in his Das Kapital. Obviously, this is not the only change: it is one of the most important ones. The gist of this new global division of labor is that a certain, relatively very small, segment of the global population has control over the entire global production and the production of most advanced technologies. Moreover, this production is physically located in areas controlled and protected by the same segment of the global population. This means that the division of the global population is in control of the most crucial instruments of changes in the global collective productiveness of labor. i.e., it has a key advantage over the rest of humanity. This advantage resulted from the tele-information revolution: thanks to this revolution, the knowledge and technologies used for setting in motion processes – economic, political, and recently also biological – which have the most profound impact on the entire global population are now produced on the territories controlled and protected by a very small segment of the global population. Acknowledging this fact permits for a new interpretation of the concept of Information Society. It frees this concept from its hitherto existing muddiness and lack of substantial content. To present such a new interpretation of the concept of Information Society is one of the main objectives of this paper.
Management of information security is important in any Electronic Government and particularly when confidential and sensitive data is recorded on a daily basis. The term ‘Electronic Government’ (eGov) refers to the use of Information and Communication Technologies (ICT) to improve delivery of government services, facilitate interactions with business and industry, or empower citizens through access to information. Efforts to offer such services to citizens have intensified across many countries. With this, threats such as computer crime become more malicious and non-malicious threats also have increased in number. Consequently, the topic of managing information security is both important and topical in view of the recent statistics reported on breaches of computer crime originating from both outside and within organizations. Although, it is argued that these ‘reported’ cases only represent the tip of a potentially large iceberg (CSU/FBI 2018).

For the last ten years, the Indian government has initiated various eGov projects both at national and state level and the local level. Ministry of Communication and Information Technology introduced National e-Governance Plan (NeGP) to support the growth of eGov within the country. Most recently in 2018, the Indian government implemented a Policy of Open Standards that aims to provide a set of guidelines for the uniform and reliable implementation of eGov. In the efforts to facilitate, promote advice and support the eGov initiatives at State and local level, the Computer Society of India (CSI) publishes various studies on challenges faced by the Indian government. Some of these challenges include: infrastructure resistance to re-designing departmental processes, lack of communication between government departments and developers responsible for eGov (also see, Mahapatra and Sahu 2017).

Given that the India government has also initiated a major push towards offering its services through the Internet, it is clear that potential for information security breaches will also continue to increase. An example reflects India, like any other country already faces information security breaches. The Computer Crime & Abuse Report, for example, highlighted that over 6,265 incidents of computer crime cases affected 660 organizations in India during 2001 and 2002 alone. Reports such as Forensic Accounting Report (2007) point out that even the fast developments in India awareness level about computer crime is very low. To combat such threats, the Indian Government gave effect to a resolution of the General Assembly of the United Nations for adoption of a Model Law on Electronic Commerce. As a result, Information Technology Act 2000 was introduced to regulate and legalize electronic commerce. More recently, the Act was modified to include computer crime such as hacking. However, statistics indicate that very few people have been prosecuted under this Act. Furthermore, the Act has also been criticized for its complexity.

In explaining information security breaches, researchers provide alternative viewpoints. Taking into account the gravity and complex nature of ICT, one strand of studies argue that relying on technical solutions alone to secure any organizations from threats like computer crime is a very ‘narrow’ approach (for example, see Vroom and Solms 2004). Although, technical solutions are equally important, information security in general is much broader in perspective than “Computer Security”. It is for these reasons that information security researchers advocate the need to recognize both technical and social issues (for example, see Dhillon and Backhouse 2001, Siponen 2001, Kesar 2002). While trying to understand the factors that lead to the absence or poorly implemented solutions, researchers believe that it is also important to explore how management within organizations addresses the issue of information security. In this regard, it has been argued that one of the primary reasons for the absence of the complicity towards information security (Hinde 2000). As a result, complicity towards information security can be a major contributing factor for management of threats such as computer crimes. Hence, it can be argued that complicity towards information security combined with inadequate lack of anti- or basic security controls could itself offer little scope for developing effective solutions.

Discussions so far, bring forth three fundamental issues regarding management of information security in the context of eGov. Firstly, most cases of computer crime for various reasons are rarely reported. Although, the extent of damage caused by information security breaches can be gauged by the ‘reported’ cases, as mentioned above, they represent only the tip of the iceberg (Parkar 1998). To further compound the problem of computer crime, most acts do not catch the attention of organizations until it is too late. Secondly, there seems to be lack of studies that take into account government officials’ perceptions and views about information security. Thirdly, there is a general underestimation of the risks associated in an increasingly electronic and connected environment within government.

Against this backdrop, research question addressed in this paper is: “How do government officials responsible for eGov projects perceive and interpret information security policies and procedures?” It makes specific reference to one eGov project implemented at a local level in India. While conducting the case study, it uses the design–ready gap analysis framework based on a multidimensional framework consisting of seven dimensions, namely: Information, Technology, Processes, Objectives and values, Staffing and skills, Management systems and structures, and Other resources (ITPOSMO) proposed by Heeks (2001). While the prime focus of Heeks (2001; 2002) framework is on identifying gaps in the design and development of eGov projects, this paper uses the framework to address the research question stated above. In this paper, both primary and secondary data is used. Primary data involves semi-structured interviews (operational and managerial staff) and surveys. While secondary data includes documents and newspaper articles.

To conclude, this paper contributes in providing significant knowledges for eGov implementation in India in the context of management of information security. This can be beneficial to the efforts directed towards overcoming challenges and issues involved in securing eGov implementation from increasing threats such as computer crime.

REFERENCES
The Problem of Teaching Ethical Theory to Computing Undergraduates

Posted on August 31, 2018 by Eric Gossett

AUTHOR
Suzie Jagger

ABSTRACT
Practitioners have identified that the teaching of ethical theory presents problems for students learning ethics as part of a professional degree programme. This is particularly the case where the course is compulsory rather than optional and is due to the student feeling they did not sign up to learn these philosophical concepts. Thus, there is often a balancing act in judging how much theoretical content to put into a module and differing views on whether ethical theory should be taught at all. This study examines the extent to which students on a first year undergraduate computing course were able to understand and apply ethical theory to help them identify ethical issues, using a step-by-step model.

The study utilises empirical measurement from the perspective of moral development theory by incorporating three scoring methods. An ethical theory score, a moral sensitivity score and a moral judgment score. The ethical theory score should be taught at all. This study examines the extent to which students on a first year undergraduate computing course were able to understand and apply ethical theory to help them identify ethical issues, using a step-by-step model.

The study aims to improve on existing research by evaluating the extent to which ethical theory is taught in computing courses, and how well students are able to understand and apply the concepts. The study uses an existing framework to assess the extent to which ethical theory is taught and evaluated in computing courses. The framework is based on the Moral Development Theory (Kohlberg, 1981) and assesses the extent to which ethical theory is taught and evaluated in computing courses.

The study concludes that there are significant differences between how ethical theory is taught and evaluated in computing courses. The results suggest that there is a need for further research to improve the teaching of ethical theory in computing courses.

REFERENCES


Commonly debated ethics issues include abortion, euthanasia, human cloning, torture, animal rights, corporate fraud, and the... Language History People World Art Education Technology Internet Business Food Beauty Miscellaneous Industry Science Anatomy Health Crafts Cars Home Finance Medicine Fashion Fitness United States Environment Travel Law Hobbies. What are the Most Common Ethics Issues? Related Topics. Issues Ethical, Legal Ethics Issues. Ethic Issues. Computer Ethics Issues: An ethic is driven by a moral, an idea of what is right and wrong, what should and shouldn't be. Ethics are the driving force behind every action and decision a person makes. Weather choosing tactful words to use when speaking to a person who might get offended to ordering dinner, every decision that is made has an ethic as the driving force. As a person grows, learns, and develops, ethical actions may change and evolve in society’s eyes and in the person’s eyes as well. Ethics are a system of moral principles and a branch of philosophy which defines what is good for individuals and society. They infuse debates on topics like abortion, human rights and professional conduct. Approaches to ethics. Philosophers nowadays tend to divide ethical theories into three areas: metaethics, normative ethics and applied ethics.