

WORKING PAPER SERIES

Discipline: Management

Towards a Profound Sense of Professionalism – *Teaching Ethics to IT and Business University Students*

Ghassan al Qaimari
Fujairah College

Stephen D. Samuel
Mittal Steels [IT Services]

Zeenath Khan
University of Wollongong in Dubai

WP 68/2008
June 2008

© University of Wollongong in Dubai, 2008

Towards a Profound Sense of Professionalism – *Teaching Ethics to IT and Business University Students*

Dr. Ghassan al Qaimari
Fujairah College
ghassan@fc.ac.ae

Stephen D. Samuel
Mittal Steels [IT Services]
Stephen.samuel@gmail.com

Zeenath Khan
College of IT
University of Wollongong in Dubai
zeenathkhan@uowdubai.ac.ae

Abstract

The boom in technology has taken over every sector of the private and public life. From hospitals to banks, military to schools and even stores, all indulge in the use of some form of technology. A by-product of this boom has been the immense amount of data that is divulged to strangers every single day. So how do customers of these services know that the people, who are serving them and taking down their personal data at a daily basis, have the sense of professionalism to ensure privacy and security? How do organizations ensure they are hiring the people with the ability to respect and maintain this privacy? In doing so, how do managers of these organizations ensure they do not cross the line themselves while using surveillance technology to monitor their own employees? In this paper, we discuss a survey study that clearly demonstrates how ethics education leads to a profound sense of professionalism, a building block in ensuring employees and managers have the knowledge and understanding to execute confidentiality or scrutiny without compromising privacy or security. We end this paper by identifying topics that, we believe, should be taught in an ethics course to IT and business university students based on the experience of the first author to help shape future employees and managers with a profound sense of professionalism.

Keywords: *IT and Business curricula, computer ethics, cyberethics, privacy, surveillance, corporate ethical and social responsibility.*

About the authors

al-Qaimari is a professor of Computer Science, and the CEO of Fujairah College. Prior to that, he taught at University of Wollongong in Dubai (January04-June06), where he was the Chair of College of IT, and at RMIT University (1995-2003). He obtained his doctorate from Heriot-Watt University, 1994, and received his BSc. in Electrical Engineering and MSc. in Computer Science from the University of Detroit. Professor al-Qaimari is actively involved with major industry players, such as IBM, Telstra and DaimlerChrysler. His research and consulting experience in the area of HCI, Usability and Software Engineering has earned him an international profile.

Samuel has been interested in computers since he was seven. He received his first computer when he was ten and has been programming ever since. He completed his graduation in Computer Science with software specialization and has been involved in developing solutions for multinational corporations in various fields from accounting to press printing to advertising. He is currently working on his dissertation proposal and hopes to carry on his love for computers.

Khan has been teaching at the Australian University of Wollongong in Dubai since 2001 and is currently pursuing her PhD in Community Informatics. She is Bangladeshi but spent most of her adult life in the United Arab Emirates. She is the receiver of the Federal Environmental Award for scientific research in the UAE and has won many other awards for her dedication to the local community and environment. Her passions include reading, writing and singing.

1. Introduction

Human tendency has always been inclined on communicating with each other. This tendency often leads to leaking private information about one person to another for the sake of conversing. With the boom of the technology era, the twenty-first century is facing mankind's highest cases of violations of privacy simply due to the ease in flow of personal information. Every bank, every school, every petrol station, and every mart requests some form of private data from the customer, which invariably ends up in the hands of the wrong-doers. A research study result showed that almost 70% of people have stolen key information from work using office mail or other technologies sometime during their career (BBC News, 2004). Other crimes such as identity theft are also on the rise due to the enhanced technology. In 2003 alone, 10 million U.S. residents were the victim of ID theft, according to the US Federal Trade Commission (Evers, 2005).

In today's high-tech world, issues of data theft are no longer limited to IT and Business professionals. Employees at every tier of an organization are dealing in customers' and company's private information in some form or the other. Human tendency to communicate can not be curbed. What is more, employees seem inclined on committing these crimes for varying reasons, from personal greed to simply passing on information to revenge on the organization from a grieving employee to rooting for a promotion. Research shows 72% of respondents interviewed had no ethical problems stealing information to help them in a new post (BBS News, 2004). In moral terms, 58% thought that it ranked with exaggerating insurance claims (BBC News, 2004).

So what is the solution to this ever-growing problem? Employers will answer: use technology of privacy to protect customers' information, hire employees with strong sense of professionalism, and use technology of surveillance to monitor their performance in the workplace. Their answers would not be that far-fetched. Of course, professionalism in an employee will hinder his/her urge to divulge information. And of course keeping an 'eye' on the employees will ensure they do not share the information with anyone else. But, where do organizations draw the line between protecting their business and the rights and privacy of their own employees?

An American company, AOL suffered 'an estimated \$300,000' when an employee stole '92 million e-mail screen names from the Internet company and [sold] them to a spammer' (Kearney, 2005). In contrast, a nationwide survey of 301 businesses conducted by MacWorld magazine in the USA found that only one third of the companies gave their employees notice of electronic monitoring, and only 18 percent had written policies (ACLU Special Report, 1997). Surveillance technology is progressively becoming intrusive such that new devices called "back scatter" are being introduced that can see through the clothes of the person in front of it, an "electronic strip search" (Maltby, 1998); or that 'a business named HygieneGuard is test-marketing a product that indicates whether employees have washed their hands after going to the restroom' (Eckel, 1997). Where this may not seem such a 'big deal' to companies, the fact that these intrusive levels of surveillance may result in 'antagonizing their workforce and inviting lawsuits' (Tribbey, 1999).

So, how do companies ensure the employees they hire will be professional enough to practice caution while handling customer and company data? Or that their managers will be able to exercise propriety while implementing surveillance technology on their employees without crossing the line and invading their employees' privacy?

We believe part of the answer lies in establishing a need for 'prior-knowledge' in employees and managers in order to grow a profound sense of professionalism at workplaces. To achieve this, focus should be placed on incorporating courses, at the undergraduate as well as the postgraduate levels, in both Business and IT degree programs that deal in various ethical issues related to work-environment, privacy and surveillance into the curricula taught worldwide.

While we are equipping our students (who are the future employees) with the knowledge of every powerful tool - from cryptography to nanotechnology, to simple ones such as databases, email software and such - we should consider equipping them with the ability to understand the consequences of misusing these tools (as mentioned above). In other words, teaching students ethical values is not enough – they should also be trained to (al-Qaimari, Khan, Samuel, 2006):

- 'Identify the privacy, legal and security issues related to the introduction of information and communication technologies. This should begin to develop a desire to continually seek improved solutions, and a desire to initiate, and participate in organisational, social and cultural change;
- Explain technical solutions to security and privacy problems arising from the introduction of technology. This should begin to develop an ability to logically analyse issues, evaluate different options and viewpoints, and an ability to implement decision; and
- Evaluate existing laws and regulations relating to privacy, legal and security issues. This will begin to develop a commitment to continued and independent learning, intellectual development, critical analysis and creativity'.

This paper focuses on a recent research carried out by the authors, which demonstrates the effects of teaching subjects such as Technology and Ethics, IT and Citizens' Right, and Cyberethics that arm students with the required sense of ethics on how to use technology that is at their disposal at a daily basis when they join the workforce.

2. Teaching ethics in academic institutions

Ethics are standards or codes of conduct that define right from wrong and form the basis of civil societies; whereas, 'professionalism includes integrity, courtesy, honesty, and willingness to comply with the highest ethical standards' (Oregon State Bar, 2005) among others. Professionalism is often referred to as an attitude rather than a definition. An employee, who knows how to conduct him/herself with professionalism, is then said to have a strong ethical background. Professionalism without a profound sense of what is ethical and what is not, is then considered to be superficial at the most.

IT and Business professionals world-wide are being trained and geared to face the challenge of the twenty-first century's ever-growing thirst for technology. Cashiers to travel agents, support techs to corporate managers, employees and managers are dealing with and managing data every single day. Data is about people and mismanagement of data infringes on peoples' privacy. So what is privacy? Judge Cooley defined privacy as "...the right to be let alone" (Warren, Brandeis, 2004). In the twenty-first century, this definition has evolved to include what is now called information privacy – 'an interest held by individuals regarding the control, and handling of data about themselves' (Clarke, 1997). When talking about privacy, it is in vein if we do not look at secrecy, security and confidentiality. Often enough,

employees disclose information that is meant to be a 'secret', such as data in relation to any country's defense or military operations. It is not 'private' in nature, but the disclosure of this information is meant to be forbidden (Clarke, 1997). It is information that is secret in nature in corporate environment that is often officially referred to as 'confidential'. Confidentiality is 'a status accorded to information to indicate that it is sensitive for stated reasons, that it must be protected and that it must be controlled' (Clarke, 1997). Of course, cases of secrecy in relations to a country's defence and military may be classified as confidential. There are clear laws world-wide that dictate punishment for infringement of confidentiality. Bodies such as Organization for Economic and Cultural Development (OECD) which refers to itself as 'a club of like-minded countries that ... provides governments a setting in which to discuss, develop and perfect economic and social policy' (OECD, 2005), have produced guidelines that countries adopt at regular basis in order to develop their protection laws. One result of such laws is the growing trends of security at workplaces. Organizations insist on installing security devices because they want to ensure their employees are doing the job without invading the privacy of their customers and employer. Security is 'the nuts and bolts mechanism which may be implemented to ensure privacy, confidentiality and secrecy' (Clarke, 1997). A major part of security is surveillance. 'Surveillance is the collection of data (be this visual, biometric, location or personal data) on a person, object or 'target', with the explicit intention of influencing or managing what that 'target' does or where it goes' (Ball, 2006). Companies implement various techniques to 'keep an eye' on their employees using hidden cameras, telephone taps, undercover workers, email and internet monitoring software.

In the face of growing data theft, surveillance seems to be the obvious way to prevent such face-less crimes. However, reactive responses are not the only ways to combat such unprofessional behavior at workplaces. The acts themselves cost companies billions a year from; Plus,

"studies by the National Workrights Institute have shown that monitoring employees seems to reduce the quality of their work. For instance, monitored customer services representatives were characterized as being "less willing to pursue complex customer questions" than surveillance free representatives. Moreover, employees may feel that they are being deprived of their liberties, and this may lead to litigation or workers' strikes which injure the company and the economy at large. For example, former Delta flight attendant Ellen Simonetti sued the airline after being fired for posting pictures of herself in Delta uniform on her personal website. Another economic pitfall of using surveillance technology is the company cost in purchasing, installing, and maintaining the equipment. In addition, extra company time must be invested in processing all of the information recorded by the equipment. Thus, the practice of employee surveillance can have potentially adverse effects on companies and the entire economy" (Patel, 2006)

In addition,

"as the digital revolution proceeds, computers are permeating everyday life. Consequently, the emergence of software and technology that monitors digital devices could precipitate the loss of societal security. Seized information has the capacity to be used as a weapon, not only by employers, but by governments and terrorists. The continuance of digital surveillance could prognosticate authoritarian government appropriation of personal information [or arm terrorists with vital information]"

(Patel, 2006)

Therefore, it is safe to say that both IT and Business professionals should be able to identify ethical issues related to the management of information, and the use of technology of privacy and the technology of surveillance. But how?

While governments and organizations are spending millions researching into new fields, such as cryptography, surveillance and so on, they are spending barely '0.4% of their estimated budgets to research into their societal and ethical implications' (Treder, 2006). Governments and academic institutes need to focus their efforts on backing student education with ethical awareness in the hope of producing professional employees and managers for the future.

Universities such as the University of Colorado (USA), Indiana University (USA), Oxford University (UK), have introduced and developed research and teaching areas into computer ethics. However, even in many of the leading universities, the number of subjects related to ethics is very limited. Research has shown that of 24 subjects, only one elective offered, in a leading Australian University, for Computer Science students is ethics-related. (Kee, Keat, Nan, Leong, 2004). This is obviously not enough. According to the study, 'Unlike the technical subjects that train a person in a certain set of skills, the study of ethics molds a person's character. Developing one's character take a much longer time compared to learning the necessary facts for a technical subject' (Kee, Keat, Nan, Leong, 2004).

Therefore, there is definitely a need to incorporate courses that increase ethical awareness among students at the academic level. The remaining paper has been divided into two major parts. The first parts details the design, mode, structure and content of proposed subjects based on the first author's experience in teaching the course for four semesters at a university. The second part develops a framework survey that studies the university students and industry employees to test if there is a difference in respondent level of awareness to ethics as a part of professionalism when they are exposed to ethics courses and when they are not, and how they would react to situations with ethical complications. The paper concludes with recommendations to incorporate such subjects in both IT and Business curricula in order to instill a profound sense of professionalism in employees and managers.

3. A course on ethics for IT students

The course should examine the information technology industry, which encompasses telecommunications, computing, broadcasting, and publishing. It should analyze the encroachment of industry activities that use electronic media on: citizens' rights in matters of data surveillance, freedom of access to information and ownership of intellectual property. The extent to which technical solutions to these problems can or cannot be provided should be discussed and alternative non-technical (e.g. administrative or regulatory) solutions should be treated. The curriculum should be contextualized when investigation of the current legal safeguards, their legislative histories and the need for new legislation are covered.

In terms of learning objectives, a student who successfully completes this subject should able to:

- Identify the privacy, legal and security issues related to the introduction of information and communication technologies;
- Explain technical solutions to security and privacy problems arising from the introduction of technology;

- Evaluate existing laws and regulations relating to privacy, legal and security issues.

We suggest from our experience the following topics to be included in a subject about ethics for third year IT students:

- Defining what is meant by privacy in the information age, and related concepts such as confidentiality, secrecy and security.
- Looking at international agreements and organizations, such as the European Directives, and the eight information privacy principles of the Organisation for Economic and Cultural Development (OECD), in addition to its guidelines on data privacy protection and trans-border data flows.
- Categorization of Privacy: Accessibility privacy (or freedom from unwarranted intrusion); Decisional privacy (or freedom from interference in one's personal affairs); and Informational privacy (or control over the flow of personal information).
- Definition of Ethics, Cyberethics and the development of technology (past, present and future), from the era of stand-alone machines, to Minicomputers and PCs, to the Internet, to the present era, which is categorized by convergence of information, entertainment and communication technologies, to the future and areas such as nanotechnology, genetic and genomic research.
- Technology of privacy and technology of surveillance.
- Privacy in the workplace and surveillance technology.
- Professionalism and professional organization such IEEE and ACM, and their code of conducts.
- White collar crimes, which include: computer and Internet fraud; identity theft; insider trading; insurance fraud; and credit card fraud. Prevention methods, detecting computer crime and the laws relating to computer crime should also be discussed.
- The Internet as a "free speech" environment and related issues, such as censorship, harassment, and defamation of characters. The impact of the Internet on "free speech", "legal jurisdictions" and "virtual communities" should also be debated.
- Freedom of Information act, and people in many countries campaign against the introduction of a national ID card.
- Commercialization of the Internet: e-commerce and on-line Shopping, consumer protection and the role of government and industry.
- Intellectual Property Laws, which covers patents, designs, trademarks, copyright, confidential information and trade practices protection.
- Corporate ethical and social responsibility.
- The aftermath of September 11, especially the "patriotic act."

As the proposal is based on the subject having been taught for over four semesters at the University of Wollongong in Dubai, the best mode, from experience, to teach this subject is in workshop mode to encourage student participation. Students should also be encouraged to conduct their own research, and to give presentation related to topics, such as: privacy on the Internet, email in the workplace and employer/employee expectations, public sector privacy, computerization of medical records, surveillance in the workplace, satellite surveillance, data matching - surveillance by stealth, ethical issue in technology (software piracy, digital rights management, audio bugging, data mining, intelligent agents, biometrics, viruses, nanotechnology, etc...), and the aftermath of September 11.

A group project for students might include performing a feasibility study for a particular company that is considering implementing a stored-value consumer

identification card, and documenting the findings in the form of a report. The students should attempt to identify the nature of the business, and then explain reasons for the company's interest in a stored-value card system, i.e. discuss the benefits in the context of the business. Students should attempt to identify: what kind of applications (current and future) the company plans to implement with the stored-value card; the advantages or disadvantages that relate to implementing a "multi-use" card (e.g., identification and transaction); the implications with regard to privacy and surveillance that this system might have on customers; ensure that security measures are kept up to date; and provide a local perspective on the regulations and ethical codes, if any, regarding privacy protection and security of telecommunications that might impact companies business.

The first author taught this subject at the University of Wollongong in Dubai for four semesters. The model has continually been developed using a student-centered approach and based on student evaluations and feedback. To test whether the subject has achieved its desired effect of increasing student awareness of ethics, a questionnaire was given to 50 students taking the subject this semester (Spring 2006). The study is discussed in the following section.

4. Ethics and Professionalism: A survey study

A survey was conducted using questionnaires prepared by the authors to test the hypothesis on whether education in ethics increases awareness among potential employees and managers to allow them to exercise ethical decisions in workplace environments. The study is based on a previous survey carried out by the authors, for more details, please refer to (Khan, al-Qaimari, Samuel, 2006).

Questionnaires were handed out to 50 third-year university students; and 50 employees from local, and multi-national companies were also chosen from various levels of respective organizations; the demographic break-down is illustrated in the table below:

Table 1: Respondent Occupation and years in service

Occupation	1-3 yrs	4-7 yrs	8 and above
Programmer	8	7	2
Manager	0	5	2
System Administrator	2	8	1
Officer	3	1	0
Support Staff	5	6	0

The survey was divided into three sections. The first section collected demographic and other information regarding the respondent such as (for employees and managers) position and number of years at work; and (for students) year and degree enrolled in. The two other sections had a mix of questions from multiple-choice to YES/NO and included Likert items. The second section tested the interviewees on their knowledge of ethics and professionalism, their attributes and definitions with questions such as 'Ethics is a process of rational thinking aimed at establishing what values to hold and when to hold them' or 'Professionalism is the way an individual conducts oneself in certain situations' on a 5-point Likert scale starting at "strongly agree", "agree", "neither agree or disagree", "disagree" to "strongly disagree". The next section tested the respondent's awareness of ethical issues such as "If a

colleague's email is open, it is okay to read his/her emails' and application of their ethical values to various set-situations borrowed from ACE test-bank such as 'You work in the mailroom and suspect a colleague is using the Federal Express service for personal mail. What do you do?' with multiple choices of

- A. You ignore the situation. (x2)
- B. You start using Federal Express for personal mail, too, but only in an emergency. (x1)
- C. You contact ethics. (x4)
- D. You notify your supervisor. (x3) (e-business.com, 2006)

The points at the end of each choice indicated the significance of the answer to the question. There were YES/No questions that asked the respondents (if they were professionals) if they had been exposed to ethical courses during their degree programs and if so, whether it helped curb their sense of professionalism and if not, whether they think it would.

The results of the survey supported the hypothesis that education indeed instills a profound sense of professionalism in both business and IT students, paving the way to ethically enhanced employees and managers in the future. It distinguished those employees (19 out of 50) who had been taught about ethics and clearly showed awareness to differing ethical situations in marked contrast to those employees who had not been exposed to any courses in ethics. This led to the conclusion from the survey results that employees are more inclined to be professional at work places when handling information in relation to privacy and confidentiality when they contain prior-knowledge or education base in ethics subjects; it also highlighted how prior knowledge increased a sense of professionalism when faced with monitoring employees without crossing the line (results were grouped together and summarized in the table below):

Table 2 : Employee response to ethical issues at various tiers

	Ethical issues at work n=50	Ethical Issues at home n=50	Ethics and the use of Internet n=50	Ethics or Aesthetic? n=50	Ethics and copyright n=50
strongly agree	48.29%	38%	28.00%	82%	12%
agree	21.71%	46%	28.00%	18%	16%
neither agree nor disagree	8.57%	10%	16.67%	0	24%
disagree	16.29%	6%	23.33%	0	27%
strongly disagree	5.14%	0	4.00%	0	21%

For students, the results clearly highlighted that when taught the difference between right and wrong, they were able to distinguish situations to real-life simulations; and in fact, their responses to majority of the scenarios had more ethical approach than some of the employees (results were grouped together and summarized in the table below):

Table 3 : Student response to ethical issues at various tiers

	Ethical issues at work n=50	Ethical Issues at home n=50	Ethics and the use of Internet n=50	Ethics or Aesthetic? n=50	Ethics and copyright n=50
strongly agree	68.00	49.00	52.00	55.00	44.00
agree	20.00	32.00	23.00	23.00	27.00
neither agree nor disagree	9.00	8.00	12.00	13.00	1.00
disagree	3.00	1.00	6.00	9.00	16.00
strongly disagree	0.00	10.00	7.00	0.00	12.00

For example, where majority of the students (52%) strongly disagreed to statements such as ‘it is okay to read others’ emails, net surf or use email for personal use’; equal percentage (28%) of employees (specially those who did not have ethical education background) agreed and strongly agreed they would carry out such actions. Other examples include ‘It is okay to tap into employees’ telephone and internet usage to ensure confidentiality is maintained within the organization and for customers’, where students scored a high 68% “strongly disagree” whereas only 48.29% of the employees did. This helped to establish that education in ethics does have a positive effect on the future employees and managers.

When asked in personal interviews (as follow up to the survey) most of the managers agreed that having that one employee with an ethical background helped build a sense of profound professionalism and that these managers often had to return to traditional text books and other literature to decide on the ethical issues of privacy and surveillance when implementing security as protection for customers and the organization.

A clear recommendation can be drawn from the study to academic institutes to re-evaluate their priorities when introducing or revamping their syllabi and to include courses in ethical awareness to work towards instilling a profound sense of professionalism in both IT and business students.

5. Conclusion

As the Information Age grows to its peak, technology is infiltrating every sector of our daily lives. Be it medical or military, private or public, schools or workshops, every day millions of data are being transferred to and fro through various forms of technology. Vital, personal information of individuals across the globe are being ‘stolen’ and maliciously used without their knowledge for purposes of theft, terrorism

and identity theft, among others. Majority of the thefts seem to be caused by employees within organisations at various levels. Companies and governments are retaliating by incorporating surveillance technology and other high-tech security systems to 'spy' on their employees and other service areas. At a time where reactive actions seem to give rise to negative economic and societal effects, there seems to be only one way to reach a balance: reaching the root of the problems and teaching students, both IT and business, and increasing their awareness to the ethical issues in order to grow in them a profound sense of professionalism.

Based on the experience of the first author, and the survey conducted for this and previous studies by the authors, we believe the ethics subjects described in this paper will be valuable additions to any IT or business student's curriculum, because it will enable them to understand the consequences and implications of the use of the technology such as surveillance and security, and the value of privacy and confidentiality. We believe employees with profound sense of professionalism, especially at the level of higher management, will positively affect the organizational culture and responsibility of corporations towards the society and help curb face-less crimes.

5. References

- ACLU Special Report. (1997). "Surveillance Incorporated: American Workers Forfeit Privacy for a Paycheck." Rights to Privacy. Robert Emmet Long, Ed. New York: The H.W. Wilson Co.
- al-Qaimari, G., Khan, Z. R., and Samuel, S. D. (2006). Information Technology Education – should the curricula include a course on ethics? Conference paper to be presented at the IASTED International Conference on Education and Technology (ICET 2006). Canada.
- Ball, K. (2006). Who's watching you work? Surveillance in Business. The Open University. BBC. Available URL: http://www.open2.net/money/briefs_20060526watching.html
- BBC News. (2004). Workplace data theft runs rampant. Available URL: <http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/3486397.stm>
- Clarke, R. 1997, Introduction to Dataveillance and Information Privacy, and definitions of terms, available online <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro>
- e-businesstics.com. (2006). ACE Practice Tests. Business Ethics. 4th Ed. Available URL: http://college.hmco.com/cgi-bin/SaCGI.cgi/ace1app.cgi?FNC=AcePresent__Apresent_html__business_ferrellethics_01
- Eckel, Sara. (1997). "Orwell Didn't Anticipate Big Business New Technologies." Sacramento Bee, p. B7.
- Evers, J. (2005). Separating theft from Reality. CNET Networks. Available URL: http://news.com.com/Separating+myth+from+reality+in+ID+theft/2100-1029_3-5907165.html
- Kearney, C. (2005). Ex-AOL employee sentenced to 15 months in spam case: stole 92M e-mail screen names and sold them to a spammer. Reuters. Computer World. Available URL: <http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,103991,00.html?source=x2105>
- Kee, I. L. S, Keat, W. S, Nan, L. and Leong, C. K. (2004). The Inadequacy of Ethics in Australian Computer Science Education. Proceedings of the Second Australian Undergraduate Students' Computing Conference. 105-112. University of Melbourne. Available URL: <http://www.cs.berkeley.edu/~benr/publications/auscc04/papers/lim-auscc04.pdf>
- Khan, Z. R., al-Qaimari, G. and Samuel, S. D. (2006). Professionalism and ethics – is education the bridge? Chapter submitted in the forthcoming book 'Information Systems and Technology Education: From the University to the Workplace'. Idea Group Inc. UAE
- Maltby, Lewis. (1998). "Privacy—A Rising Concern in the Workplace." The San Diego Union-Tribune, p. B7.

OECD (2005) About OECD. Available URL: www.oecd.org
Oregon State Bar. (2005). Statement of Professionalism. Oregon. Available URL:
<http://www.osbar.org/rulesregs/professionalism.htm>
Patel, S. (2006). War at workplaces. Ohio State University. p 2-3. Available URL:
www.cse.ohio-state.edu/~patelsud/Sudhir_Patel_601_Paper.doc
Treder, M. (2006). Research nano implications! But which ones? Available URL:
http://crnano.typepad.com/crnblog/what_we_believe/index.html
Tribbey, R. (1999). Workplace Privacy: Audio and Video Surveillance. University of Louisville.
USA. Available URL: www.louisville.edu/cbpa/lmc
Warren, S. and Brandeis, L. D. (2004) The Right to Privacy. Law Library. Brandeis School of
Law. University of Louisville. Available URL:
<http://www.louisville.edu/library/law/brandeis/privacy.html>



University of Wollongong in Dubai

UOWD Research Committee

Working Paper Series

Co-ordinator: Dr Melodena Stephens Balakrishnan

Administrative Support: Ms. Shalini Manghat, Mr Ivan Fernandes

WorkingPapers@uowdubai.ac.ae

University of Wollongong in Dubai

P.O. Box 20183

Dubai, UAE

Phone: (+ 971) 04 367 2400

Fax: (+ 971) 04 367 2760

Website: www.uowdubai.ac.ae/research

DISCLAIMER

The views and statements represented in this Working Paper are the views and statements of the author(s) and do not necessarily represent the views of the University of Wollongong in Dubai. The University of Wollongong in Dubai is not responsible for any loss, claim, liability, or damage related to the use of the information contained in this Working Paper, whether from errors or omissions in the content of the Working Paper. Furthermore, the University of Wollongong in Dubai makes no representations, express or implied, as to the accuracy of the information and data contained in this Working Paper, or as to the suitability of the said information and data for any particular purpose.

COPYRIGHT

This Working Paper and the information contained therein are protected by the United Arab Emirates and international copyright laws. The authors grant a non-exclusive licence to the University of Wollongong in Dubai to publish this Working Paper in full in the University of Wollongong in Dubai *Working Paper Series*. Any other usage by third parties is prohibited without the express permission of the authors.