Conference Proceedings of

A*i*CE 2012

Melbourne, 13 February, 2012.

Sixth AUSTRALIAN INSTITUTE OF COMPUTER ETHICS CONFERENCE

Proceedings of

A*i*CE 2012

Edited by
Shona Leitch and Matthew Warren
ISBN 978-0-9872298-1-6

Organised By
Information Security, Privacy & Ethics (iSPER) Group, School of
Information Systems, Faculty of Business and Law, Deakin University.

Welcome

The A*i*CE 2012 conference follows on from the highly successful initial A*I*CE 99 conference and the A*i*CE 2000, A*i*CE 2002, A*i*CE 2005 and A*i*CE 2008 conferences. This conference looks at the continued development of Computer Ethics within Australia, taking into account the current issues that impact Australia such as social media.

Members of the conference organising committee accepted each paper in the proceedings after a careful review; this took the form of a **blind review** by at least **two** members of the conference organising committee. The papers were subsequently reviewed and developed where appropriate; taking into accounts the comments of the reviewers. The aim of this conference is to further the work already achieved within Australia and bring together researchers in the field to discuss the latest issues and their implications upon Australia.

We commend the authors for their hard work and sharing their results, and the reviewers of the conference for producing an excellent program.

A*i*CE 2012 Organising Committee

John Barlow, Australian Catholic University.
Mike Bowern, Australian National University.
Oliver Burmeister, Charles Sturt University.
Shona Leitch, Deakin University.
John Lenarcic, Royal Melbourne Institute of Technology.
Richard Lucas, University of Canberra.
Donald McDermid, Edith Cowan University.
Craig McDonald, University of Canberra.
Matthew Warren, Deakin University. (Conference Chair).
John Weckert, Charles Sturt University.

Contents

Ethical Considerations and Guidelines in Web Analytics and Digital Marketing: A Retail Case Study

R Kenny, J Pierce and G Pye

School of Information Systems, Deakin University, Australia
Email: rjken@deakin.edu.au; justin.pierce@deakin.edu.au; graeme.pye@deakin.edu.au

ABSTRACT: *Within the information economy customers utilise the media that interests them, view the news that affects them and read about the people that inspire them. Web analytics enables an organisation to collect customers' data as they interact with an organisation. Then with analysis of the captured data, organisations can offer a unique online experience, tailored to the customer's individual preferences and create direct marketing campaigns that target individual consumers. This paper discusses the ethical considerations of collecting customer data and highlights how ethical guidelines can better inform organisational behaviour.*

Keywords: web analytics, digital marketing, retail, business ethics

INTRODUCTION

The Australian retail industry contributes AUD $292 billion or approximately 24% of GDP (ARA, 2011; ABS, 2011). During the global financial crisis (GFC) of 2007-2009, Australian retailers were relatively insulated by the Labor Government Stimulus Package, but a stronger Australian dollar caused by continuing global economic concerns in 2011 has intensified Australian retail competition as the industry becomes more globalised by the advent of online retailing (Pierce, 2011). Increased global competition could indicate that some retailers will not be bound by the level of ethics Australian consumers have come to expect.

Since its commercialisation in 1994, the Internet has been an invaluable and multi-faceted tool for retailers, especially in terms of reaching customers and satisfying business needs (Runyan *et al.,* 2009). Not only can businesses broadcast to potential customers across the globe, but they have the ability to analyse user interactions with their website, affording an unprecedented understanding of the needs and wants of their audience (Omidvar *et al.,* 2011). *Web analytics* is the term given to the automated practice that allows organisations to study website performance relative to customer experience to determine whether business objectives are being met (Young, 2008).

As technology advances, businesses conceive of new ways to exploit it (cf. 'the virtuous circle of the "real" new world economy', McNurlin & Sprague, 2006 p.80). Business products and services are designed to exact competitive advantage either through more efficient operations, or establishing a superior and sustainable strategic position and as the rhetoric goes, information is both the best offence and the best defence (Pearlson & Saunders, 2011). The technology tools that support both the business and the consumer often operate by collecting and processing data provided by the consumer, although not always with their direct knowledge or consent (Pollach, 2005).

Web analytics can be used to measure the success of online marketing campaigns and tailor marketing material to suit a specific audience (Fulgoni, 2011). The underlying objective of using web analytics tools is to make improvements to the customer engagement initiatives and the overall website design (Sostre & LeClaire, 2007). By engaging web analytics tools, businesses are more prepared to design better-targeted advertisements and strengthen marketing initiatives (Google, 2011) with the underlying goal of enhancing profitability.

The focus of this research is the ethical implications behind the deployment of web analytics applications and the collection of data through online media resources. The authors discuss current ethical guidelines and frameworks and whether they adequately cover the full range of ethical issues that surround online data collection. The authors also argue that although capability exists to monitor and collect intimate customer data that it is not necessarily the right of commercial enterprise to do so.

It is necessary to determine the ethical viewpoint to identify how businesses intend to use this data. For example, is the data being analysed to improve customer relationship management (CRM)? Is it the sole purpose? Or is it collected without any real goal or direction, or with secondary or ternary purposes? Although these technology tools can benefit both the business and the consumer, the modern enterprise must consider the ethics of collecting and using consumer details for analytical purposes (Dwight, 2010).

There are two themes to this paper, the ethical issues in web analytics and direct marketing, which are linked in terms of what they offer in business opportunities. The paper is organised as follows: to describe the emerging business practice of web analytics and its capabilities before presenting a retail case study. The case study enables consideration of the ethical issues that surround the collection of customer data in an online and retail context, which leads into an ethical discussion with regard to direct marketing; highlighting the currently available ethical guidelines before concluding with future research directions.

CAPABILITIES OF WEB ANALYTICS

Web analytics offer a multitude of possibilities. However, the irony is that organisations do not always know what they don't know (Hassanzadeh *et al.*, 2011). So as the desire to learn more about customers builds, organisations are looking to web analytic providers to assist them to understand their customers, resulting in a growth in the web analytics sector (Sen *et al.*, 2006). Providers offer varying capabilities to help businesses discover more about their website users and enhance their online presence.

Google Analytics and Yahoo Analytics, for example, both enable businesses to track user interactions with their websites. Organisations can view user click-paths, drop off points and even e-commerce reporting such as product views, purchases et cetera (Google, 2011; Yahoo, 2011). Both of these analytics tools provide visual representations of the data, such as click-path conversion funnels that show the pages of the website users are leaving. These visual representations enable easy interpretation of the data and can assist the business in making decisions regarding the layout of the website. Another web analytics tool, eLogic, provides the ability to monitor visits to the website in real time. Some of the data collected by eLogic includes where visitors are coming from, the page they land at, how many visitors are returning and which hours of the day the site draws more traffic (eLogic Web Solutions, 2010).

The types of features offered by analytics providers include: tracking email campaigns, search engine optimisation (SEO), banner advertisements and offline adverts. Businesses can see what actions engage audience interest and what behaviours result in revenue and purchases (Yahoo, 2011). It is also a useful method to identify which marketing campaigns are most effective, which advertising material produces the most traffic or generates the most sales (eLogic Web Solutions, 2010). This then enables the business to identify the strengths and weaknesses in their online marketing campaigns and subsequently enable them to fine-tune future campaigns.

Another useful feature is benchmarking. Google Analytics has the ability to compare website metrics with those within the same industry (Google, 2011). This gives a comparative indication of how successful the website is in terms of industry averages. The tool also allows the setting of targets and to identify whether the website is meeting business expectations. Google appears to have first mover advantage in benchmarking web analytics, although the literature contains many proofs of concept (e.g. Krishnamurthy *et al.*, 2005; Pang *et al.*, 2009; Panian, 2010; Lee *et al.*, 2005; Spangler *et al.*, 2009).

Internal site search can also be monitored using web analytics. Google Analytics provides the ability to view the top site search terms which is useful to find out what users are actually looking for on the website (Google, 2011). This information can help businesses to identify gaps in their website strategy; what information is not readily available and what parts of the website should be more dominant on the homepage.

Yahoo Web Analytics also provides the functionality to identify user demographics. Demographic reports can be used to identify user age groups and gender, or standard reports can be filtered by age or gender (Yahoo, 2011). There is also the capability to report user behaviours such as the types of websites they visit, in order to identify the categories of interest of the websites users (Yahoo, 2011).

Through using these reporting features, businesses will develop a better understanding of their users' behaviours, beliefs, preferences, and interests in order to better target their marketing campaigns to their main audience.

With the proliferation of social media use, some web analytic providers, such as Omniture Analytics (2009), are offering businesses the option to track social networking, video and mobile devices. The ability to view user-generated content on Facebook and Twitter is invaluable in gaining insights with regard to brand sentiment. Omniture Site Catalyst can measure Facebook applications, identify the devices used to access the site, identify the number of times the business is mentioned on Twitter and provide metrics on blogs, consumer reviews and social networking (Omniture, 2009).

HOW CUSTOMER DATA IS COLLECTED

Using web analytics customer data are essentially collected automatically as a function of viewing the web media. Marshall (cited in Murdock, 2006) identifies two ways in which data can be collected by web analytics packages: the log file method and the Javascript method, which are explained as follows, in greater detail.

The Log File Method
This method involves using locally stored tracking files—*cookies*—that automatically record user activities as they interact with the site. This method collects data as requested by the server and are potentially difficult to maintain (Whyte, 2010). Some of the benefits of using the log file method, as indicated by Whyte, include no firewall issues (see the JavaScript method), that completed downloads can be tracked, mobile visitors are tracked by default and filters can be applied at any time. Some disadvantages, however, include no event tracking, all updates and modifications must be managed by a team, robots can skew the data by multiplying the visitor count, excessive disk space is required for storage, one IP address implies one person (proxy servers are ignored) and cached pages are not counted (*ibid*).

The JavaScript Method
Using this method, the business embeds some JavaScript code in the web page and then sends the user activity to a third party web analytics service provider. The JavaScript method, also known as the 'Page Tagging' method has more accurate session tracking allows data collecting and storage for later analysis by a host vendor, tracks client-side events, captures client-side e-commerce data and the host vendor manages all of the stored data (Whyte, 2010). Similar to the log file method, the JavaScript method also has a number of disadvantages, such as: inaccurate set up and tagging of site pages will create inaccurate data, firewalls can skew the data, latency can result in untracked visitors and deleted or rejected cookies can cause inaccurate tracking.

It is clear the JavaScript method is a technical improvement over the log file method and it can be seen that user data (URL origin, device, browser, plug-ins, IP address, operating system etc.) and behaviours (mouse-click latencies, preferences etc.) can be collected seamlessly with ease. With the obvious potential in web analytics, there are a number of questions regarding the ethics of this data gathering approach, the information gleaned from it and the subsequent targeted marketing employed, such as:
- What are the ethical implications of this approach?
- What are the implications for customers?
- What do customers expect in terms of using the information gathered?
- Do customers know what is happening to their information?
- Are customer privacy issues or expectations beginning compromised?

The following case study describes the actions taken by a retailer with a view to aggressively marketing their eCommerce website to increase their online sales by gathering consumer activity information using a web analytics approach.

A RETAIL CASE STUDY

AIM is a large national department store chain retailer that has established numerous retail outlets in metropolitan, regional and rural locations throughout Australia. AIM has predominately focused on

delivering their customer needs as a traditional 'bricks and mortar' retailer and aggressively holds a significant market share over its main local retail competitors. However, times are changing and AIM is aware that with the pervasion of 'online shopping' into the retail marketplace, this is empowering their traditional customer base to choose alternative shopping options and to browse or make purchases online from both national and internationally based competitor retailers. Although initially cautious to adopt a retail presence on the Internet, AIM acknowledges that the Internet and eCommerce is now a viable reality and with their competitors adopting this online technological approach to shopping. Therefore, AIM took the decision to make a significant investment that has resulted in a comprehensive and popular eCommerce website that has delivered steady but slow online sales growth.

AIM is aware that the new online sales paradigm represents a means of continuing to provide strong customer service to local customers and is an opportunity to competitively retail within the wider global marketplace. In seeking to customise their eCommerce website to provide a more personalised eCommerce experience to their customers, AIM considers that the use of a Web Analytics approach would enable them to gather valuable data about the online activities of their customers. This would enable AIM's marketing department to analyse and surmise ways of enhancing and personalising their online customer's shopping experience. AIM already operates a Facebook page through which it interacts with people who are AIM's 'friends.' It also operates a community of practice tool to interact with customers who are incentivised with AIM vouchers in exchange for providing open and honest feedback.

Using web analytics will enable AIM to run reports regarding the number of site visits; track user origin; 'click paths'; locate where on customers leave the website; number of product views; internal product searches, and the number of purchases and orders placed. Using this information AIM can begin to build a profile of their individual repeat customers including, their demographic; click paths; orders; product browsing habits; product searches; the time spent at the website and how often they visit. This information is invaluable to AIM's Marketing department in terms of developing broad advertising strategies and aggressive individual marketing campaigns, particularly for enacting personalised direct marketing promotions to individual customers.

Potential Ethical Issues: The Good, the Bad, and the Ugly

The capabilities of web analytics are impressive, and the commercial advantages to be had are clearly evident in the building and customising of user experience in the online environment. Enterprises that build innovative and superior customer experience focusing on newness will enjoy repeat visits (Grewal *et al.*, 2004). Despite the advantages, however, the use of web analytics in this context raises a number of ethical questions, those most notable regarding:

- security and privacy issues – to both the business and the consumer;
- the issue of informed consent – the extent to which consumers understand how their personal data is being used;
- tracking individual and social networking activity – as an invasion of privacy;
- the perceived quality of open source versus packaged solutions;
- access to industry figures, and;
- the accuracy and permanency of collected data.

The authors use the term 'ethics' to refer to what the business ought to do. It is asserted that the organisations that collect customer data have a duty of care with respect to the following points as a minimum:

- the customer is the owner of information about them;
- the customer should be informed on the information the organisation is collecting and for what purpose the information is being collected;
- the customer should have the option not to participate;
- the customer's information should be protected from third-party access;
- appropriate governance on management and destruction of customer data is established.

Mindful of these assertions, and assuming an organisation is diligent in their application of these ethical principles, we now discuss use of customer data in the form of direct marketing. It follows that armed with personal customer details organisations can offer personalised marketing campaigns directed at the very preferences the customer may have unknowingly divulged to the organisation.

DIRECT MARKETING

Atraight Technologies (2009) define direct marketing as 'all marketing communication techniques which allow to address *[sic.]* directly and individually the addressee with the objective of a more or less immediate answer.' In other words, direct marketing is any marketing communication that is tailored to individually satisfy the needs of a specific audience. Online direct marketing uses the data collected using web analytics tools to segment the audience into more specific groups. This gives businesses the opportunity to provide marketing communications that are relevant to each individual group.

While direct marketing is increasing in popularity, it is important to consider that it may not be suitable for every marketing campaign. Table 1 lists the advantages and disadvantages of direct marketing as they apply to both the business and the consumer.

	Advantages	Disadvantages
For the business	- Cost reduction (Rath, 2009). - Avoids fallout from consumers. - Easy to integrate with a database which also allows data analysis. - Online direct marketing reaches the audience faster than other mediums such as post or television. - Easy to modify marketing campaigns.	- Potential to target the wrong audience. - Restricting the distribution of marketing material lowers the chance of attracting a new audience.
For the consumer	- Reduces unwanted marketing material. - Only informed about promotions that are of interest to the consumer.	- May miss out on wanted marketing material if the defined targeted audience is too narrow.

Table 1: Advantages and Disadvantages of Direct Marketing

In following on from the ethical concerns raised by web analytics, the discussion now moves to marry the two themes together to discuss the ethical guidelines that exist for marketing.

CURRENT ETHICAL GUIDELINES

As web analytics and direct marketing both involve the collection and use of personal and sometimes sensitive information, business has a duty of care to the consumer. Currently, there are a number of guidelines that have been developed help businesses to decide the most appropriate course of action, especially in the current environment where competitive and ethical issues sometimes collide or overlap. The following are examples of current industry standards for ethics.

Best Practice for Digital Marketing
The Australian Direct Marketing Association (ADMA) is an organization developed to inform businesses about responsible and effective direct marketing. ADMA have established a set of "Best Practice for Digital Marketing" guidelines, which covers a number of important areas in relation to online marketing and the collection of data. These guidelines cover (ADMA, 2010):
- Online privacy policies;
- A means for customers to opt-out from having their information passed on to a third party;
- Email marketing;
- Guidelines for responsibility marketing to children.

Marketing Code of Ethics
The Marketing Association of Australia and New Zealand (MAANZ) have a focus on "marketing education and training, marketing information and practical marketing tools for marketing and business development". As a result, MAANZ have designed a Marketing Code of Ethics which covers the following areas (MAANZ, 2010):
- The responsibilities of the marketer;
- Honesty and fairness;
- Rights and duties of parties;
- Product development management;

- Promotions;
- Distribution;
- Pricing;
- Market research;
- Organisational relationships.

In terms of online direct marketing and web analytics, the main areas of focus for the Marketing Code of Ethics is the responsibility of the marketer, honesty and fairness, the rights and duties of parties and market research. However, it is still important for businesses to consider the other areas when venturing into online marketing.

National Privacy Principles

The National Privacy Principles are a part of the Privacy Act 1988 (*Cth*) and are the "base line privacy standards which some private sector organisations need to comply with in relation to personal information they hold" (Australian Government, 2010). A more detailed information guide has also been established to provide the "Office's interpretation" (*ibid*) of the principles. The areas covered in the National Privacy Principles include:

- Collection;
- Use and disclosure;
- Data quality;
- Data security;
- Openness;
- Access and correction;
- Identifiers;
- Anonymity;
- Trans-border data flows;
- Sensitive information.

For online and direct marketing, all of these principles must be adhered to, but there are a few that require special attention; collection, use and disclosure, data security, openness, identifiers and sensitive information.

Synthesis

Overall it appears these guidelines place an onus on the marketer to place the interests of the customer above their own commercial interests. For example the provision of opt-out clauses in the marketing terms allows the customer to participate in the face value of the marketing application without participating in secondary or ternary applications. Where the National Privacy Principles seem to be the more overarching guidelines there is scope to provide specific guidelines for the ethical practice of web analytics. The authors recommend said guidelines to be developed and proposed in future research.

CONCLUSION

In the years 2009-2011, in response to increased competition in Australia many traditional retailers have joined their online competitors by selling goods via the online medium. The so-called multi-channel retailing efforts are becoming more competitive. Examples include the case study, JB Hi-Fi, Myer, David Jones, Harvey Norman and numerous specialty stores. As these traditional stores continue to vie for a share of the customer's wallet it is likely that web analytics will continue to be a differentiating factor in well-designed web experiences and retailers that engender customer loyalty and entice repeat purchases. The continuing high clause of the Australian dollar makes the situation unique to Australia, especially as local retailers claim to be combatting a non-level playing field in that imported purchases under AUD $1000 currently do not attract GST (Pierce, 2011).

In the current online environment where content is key and consumers constantly want newness and the ability to interact socially, the pressure is very much on organisations to offer a truly unique experience. The potential offered by web analytics providers for organisations to fully understand and customise web experiences to their consumers is considerable and often provides the means to offer a customisable experience.

In this paper we have argued that although the potential exists to use customer data to create their unique and personally customised experience, business is duty bound not to overstep the boundaries of

ethical collection and use of consumer data. As Kant's (1997 cited in Quinn, 2006) second formulation of the categorical imperative implies treat others as ends in themselves and never as means to an end. Taking the Kantian view, it therefore holds that organisation's first obligation is to the customer, even at the expense of creating a customisable experience for them.

Future research will continue to examine the ethical issues of online technology use, especially where collection and use of customer data is concerned. Furthermore, the framing of ideas regarding ethical guidelines for web analytics use and direct marketing in terms of formal ethical frameworks is required to test their validity and offer a set of best practice guidelines to industry.

REFERENCES

Atrait Technologies (2009) "Terms Used" [online] http://www.atrait.co.uk/corporate/lexique.php, Accessed: 6 November 2010.

Australian Bureau of Statistics (ABS) (2011) "5206.0 - Australian National Accounts: National Income, Expenditure and Product, Jun 2011" [online] http://www.abs.gov.au/ausstats/abs@.nsf/mf/5206.0, Accessed: 14 November 2011.

Australian Direct Marketing Association (ADMA) (2010) "Best Practice for Digital Marketing" [online] http://www.adma.com.au, Accessed: 13 November 2011.

Australian Retail Association (ARA) (2011) "About ARA" [online] http://www.retail.org.au/index.php/xarpages/ara_home/aras_mission_and_values, Accessed: 14 November 2011.

Australian Government (2010) *Privacy Act 1998*, Canberra, Commonwealth of Australia.

Dwight, L.R. (2010) "Why Businessmen are More Honest that Preachers, Politicians and Professors" *Independent Review*, **14**(3), pp.434-44.

eLogic Web Solutions (2010) "Webstats PRO: Real-Time Web Analytics Solution" [online] http://www.elogicwebsolutions.com/web-analytics.html, Accessed: 8 February 2011.

Fulgoni, M. (2011) "Online in Context" *Journal of Advertising Research*, **51**(1), March 2011, pp.84-6.

Google (2011) "Google Analytics" (Product Description) [online] http://www.google.com/analytics/features.html, Accessed: 8 February 2011.

Grewal, D. Iyer, G.R. & Levy, M. (2004) "Internet Retailing: Enablers, Limiters and Market Consequences" *Journal of Business Research*, **57**(7), pp.703-13.

Hassanzadeh, O. Duan, S. Fokoue, A. Kementsietsidis, A. Srinivas, K. & Ward, M.J. (2011) "Helix: Online Enterprise Data Analytics", *Proceedings of the 20th International Conference Companion on World Wide Web*, Hyperabad, India, 28th March – 1st April 2011.

Kant, I. (1997) *Foundations of the Metaphysics of Morals and What is Enlightenment?* Translated with an introduction by Lewis White Beck, Prentice Hall, Upper Saddle River, NJ, USA.

Krishnamurthy, S. Patel R. & Kaushal, A. (2005) "Online Competition" *Marketing Research*, **17**(4), pp.20-5.

Lee, S-H. Thomas, S.R. & Tucker R.L. (2005) "Web-Based Benchmarking System for the Construction Industry" *Journal of Construction Engineering & Management*, July 2005, **131**(7), pp.790-98.

Marketing Association of Australia and New Zealand (MAANZ) (2010) "Marketing Code of Ethics", [online] http://www.maanz.org, Accessed: 13 November 2011.

McNurlin, B.C. & Sprague, R.H. (2006) *Information Systems Management in Practice*, 7th Ed, Prentice Hall International, New Jersey.

Murdock, K. (2006) "Web Analytics: Data Collection Methods" [online] http://www.practicalecommerce.com/articles/196-Web-Analytics-Data-Collection-Methods, Accessed: 4 November 2010.

Omidvar, M.A. Mirabi, V.R. & Shorkry, N. (2011) "Analysing the Impact of Visitors on Page Views with Google Analytics" *International Journal of Web & Semantic Technology (IJWesT)*, **2**(1), January 2011, pp.14-32.

Omniture (2009) "SiteCatalyst—Actionable Web Analytics" [online] http://www.omniture.com/en/products/online_analytics/sitecatalyst, Accessed: 10 February 2011.

Panian, Z. (2010) "The Path to Web Intelligence Maturity" *World Academy of Science, Engineering & Technology*, June 2010, **66**(1), pp.1618-24.

Pang, M-S. Suh, W. Kim, J. & Lee, H. (2009) "A Benchmarking-Based Requirement Analysis Methodology for Improving Web Sites" *International Journal of Electronic Commerce*, Spring 2009, **13**(3), pp.119-62.

Pearlson, K.E. & Saunders, C.S. (2010) *Managing and Using Information Systems: A Strategic Approach*, 4th edn, John Wiley & Sons Inc, Danvers, MA, USA.

Pierce, J.D. (2011) "Staying Afloat: Retail Price Deflation and the Online Battle" [online] http://www.chifley.edu.au/IndustryArticles/JustinPierce_31Jan11.aspx, *Chifley Business School Industry Article Series*, Accessed: 8 January 2011.

Pollach, I. (2005) "A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent", *Journal of Business Ethics*, **62**(3), pp.221-35.

Quinn, M.J. (2006) *Ethics for the Information Age*, 2nd Ed, Pearson International, Sydney, NSW, Australia.

Rath, S. (2009) "Benefits of Direct Marketing" [online] http://business.ezinemark.com/benefits-of-direct-marketing-16a6ffd5c5a.html, Accessed: 6 November 2010.

Runyan, R. Huddleston, P. & Swinney, J. (2009) "A Model of Small Retailer Innovation Proneness: Early Internet Adoption as a Measure of Innovativeness", *B>Quest*, 2009, pp.1-26

Sen, A. Dacin, P.A. & Pattichis, C. (2006) "Current Trends in Web Data Analysis", *Communications of the ACM*, November 2006, **49**(11), pp.85-91.

Spangler, S. Chen, Y. Proctor, L. Lelescu, A. Behal, A. He, B. Griffin, T.D. Liu, A. Wade, B. & Davis, T. (2009) "COBRA – Mining Web for Corporate Brand and Reputation Analysis" *Web Intelligence & Agent Systems*, September 2009, **7**(3), pp.243-54.

Sostre, P. & LeClaire, L. (2007) *Web Analytics for Dummies*, Wiley, Hoboken, NJ, USA.

Whyte, J. (2010) "Analyze This! Lesson One: Methods Of Data Collection" [online] http://www.searchmarketingstandard.com/analyze-this-lesson-one-methods-data-collection, Accessed: 4 November 2010.

Yahoo (2011) "Yahoo Web Analytics" (Product Description) [online] http://web.analytics.yahoo.com/features, Accessed: 8 February 2011.

Young, L. (2008) "A Social Media Glossary" [online] http://www.capilanou.ca/help/login-page/active-cms/glossary.html, Accessed: 4 November 2010.

You are what you type: Privacy in online social networks

R Kanha Sar[1], Y Al-Saggaf[2] and T Zia[3]

School of computing and mathematics, Charles Sturt University, Australia
[1] *rsar@csu.edu.au,*
[2] *yalsaggaf@csu.edu.au*
[3] *tzia@csu.edu.au*

ABSTRACT: *The increasing popularity of social network system (SNS) sites such as Facebook, Twitter and LinkedIn, has raised concerns about privacy particularly the risk of private information leakages and the secondary use of those information. Users' information is being shared/leaked in a number of ways including the use of tracking technologies (such as HTTP cookies). This paper will provide an analysis of the privacy issues related to OSNs and using a hypothetical scenario it will argue for the SNS users' right to privacy. It is hoped that the analysis will raise awareness about the threats to privacy from the current practice to information leakages and the future possibilities of information leakage.*

Keywords: Privacy, Ethics, Social Network System, Online Social Networks.

INTRODUCTION

Over the past few years, social network sites (SNS) such as Facebook, Twitter, and LinkedIn, have become increasingly popular since they provide new means of communication. Users of these systems are typically required to fill out their online profile with minimum personal information such as name, date of birth, email address and/or profile picture. Then they can share their thoughts, ideas and creativities, form online social communities and keep in touch with people they know from both online and offline.

It is reported by the Digital Criminal (as cited in Irvine, 2009) that nearly two fifths of polled 2,000 social network users posted details of their holiday plans and 41% of them reveal private information (such as date of birth, and workplace) to public or complete strangers. A study of Twitter content has shown that users do write about themselves, their activities and where they are (Humphreys, Gill, & Krishnamurthy, 2010). By having different pieces of identifiable and/or personal information diffused online, and having no clue of who has access to those information, the users expose themselves to various risks ranging from the risk of privacy loss and the associated risks such as harassment, identity theft, and digital dossier.

An example of this would be the story of an Australian Olympic swimmer Stephanie Rice was dumped by sponsor Jaguar over her a Twitter message she wrote and was forced to apologize to those offended by her Tweet when she claimed the South African rugby team were homosexuals (Bymes, 2010). Her gay friend, Matthew Mitchum, defended her saying she meant no harm but nevertheless her message was offensive and thoughtless. A number of conclusions can be drawn from this situation: (a) Rice has no idea of who (in the world) have access to her Tweets, (b) Rice treated Twitter as a private space, and/or (c) Such an incidence would never happen if she said exactly the same thing with her close friend, in a private space (e.g. her home).

Privacy might not be valued to the same degree among users from different countries and cultures, but the users should at least have knowledge about or control over what type of information about them is being collected. Privacy issue in SNS become a concern because large amount of personal information are voluntarily shared and they can be harvested so rapidly and stored for an unknown time period.

In this paper, we discuss different possible information leakages caused by SNS and non-SNS in a number of ways such as the tracking technologies (e.g. cookies). We also present a scenario to illustrate how different bits and pieces of user's information diffused online may be used to build a detailed picture of a person's life - which may affect his/her future job opportunities and/or health insurance –

without that person's knowledge: that is when the privacy issue arises.

SOCIAL NETWORK SITE OVERVIEW

For the purpose of this paper, social network site (SNS) is defined as "web-based services that allow individuals to (a) construct a public or semi-public profile within a bounded system, (b) articulate a list of other users with whom they share a connection, and (c) view and traverse their list of connections and those made by others within the systems" (Boyd & Ellison, 2007).

The first recognizable SNS was launched in 1997. sixdegrees.com allowed users to create and populate their profiles, list their friends and surf the friend lists in 1998. Despite the fact that it attracted million of users, it lasted for only 3 years (Boyd & Ellison, 2007). From 1997 to 2011, a number of SNS like Ryze (www.ryze.com) was launched to help people leverage their business works. While Ryze failed to acquire mass popularity, LinkedIn becomes a very powerful network attracting professional users. Remarkably, Facebook, which was launched in 2004, becomes very popular and successful. It attracted 500 million users in mid 2010 (Zuckerberg, 2010) and continues to grow to more than 800 million in 2011 (Facebook, 2011).

SNS can be grouped into different categories such as business, common interest, dating, face-to-face facilitation, friends, pets, and photo (Social Software Weblog, as cited in (Gross & Acquisti, 2005). Some sites are designed for specific ethnic, political, religious, or sexual orientation categories. With the popularity of smart phones with the Internet access, mobile specific social network site like Foursquare (www.foursquare.com) emerged, and some web-based SNSs like Facebook (Slee, 2007) and LinkedIn (Nash, 2009) also provide mobile access to the sites. The number of users access Facebook from mobile increases from 100 million (Palihapitiya, 2010) in early 2010 to 350 million in 2011 (Facebook, 2011).

PRIVACY

Given the ease of access and the popularity of the SNS, privacy issues have emerged which becomes a major concern among SNS users.

There is no rigid definition of privacy. Different ways of life in different societies give different forms of privacy. Privacy is not about all or nothing; we need to give up our privacy to some extent to live in a society, but we cannot experience a total loss of privacy. Ruth Gavison (1980, as cited in Gibbs, 2008) defines privacy as the limitation of other's access to an individual, and that limitation of access has three key elements: control of information about oneself (Secrecy), freedom from other's attention (Anonymity) and freedom from surveillance and observation (Solitude). Meanwhile, privacy is classified into four distinct types: Physical/Accessibility (involving one's physical space), Decisional (noninterference involving one's choices), Psychological/Mental (non-intrusion/ noninterference involving one's thoughts and one's personal identity), and Informational Privacy (Having control over/limiting access to one's personal information) (Tavani, 2007).

Al-Saggaf and Weckert (2011) point out that our inner thoughts and feelings, our personal relationships, our personal information (particularly about our lives as our health and finance), our own space (e.g. our house, desk, room), and our state of being unobserved should be treated as an individual's business and should be private matters, at least in a sense that those involved want to be able to choose what details they intend to share to which third parties. People might not mind others knowing various things about them, but the control over access to the knowledge is crucial.

Information being shared among SNS and non-SNS sites

Concerns involving technologies that threaten information privacy is not new. However, what makes the difference is \the type of information "being voluntarily shared by the SNS users and being leaked from the SNS to the third party sites without the user's knowledge. In order to join an SNS, the users are typically required to fill in their profile pages with basic and/or personal information such as full name, email address, location, gender and date of birth. Later, they also provide extra information to enrich their profile pages. Those information can be classified into five groups (Krishnamurthy & Wills, 2008) known as: (1) Thumbnail (A brief profile contains at least full name and image), (2)

Greater profile (Additional information including interests and relationship status), (3) List of friends, (4) User generated content (e.g. pictures, video, links and comments), and (5) Comments (Status updates, testimonial and tags). There are at least three ways the user's information are leaked/ become available to the third party organization: privacy setting, tracking technologies and the use of application programming interface (API).

SNS provide privacy setting that allows users to set different privacy levels to whom they decide to share the information to. By default, the user's profile page is publicly available and searchable in the search engines. Some users do not care about changing their privacy setting (Boyd & Hargittai, 2010) while others change the privacy setting for their profile to be viewed by people they know only (Young, 2009). There are two main reasons why the users do not change the default setting online; either they may be uninformed that they can change the default setting or they might not have technological knowledge to change it (Shah, and Kesan, 2003, as cited in Humphreys et al., 2010). By exposing and sharing personal and sensitive information, the users might expose themselves to various real-life and cyber risks such as phishing attack, identity theft and digital dossier.

Another contribution to the information leakage is the tracking technologies such as HTTP cookies, flash cookies and web beacons or web bugs (Angwin, 2010). HTTP cookie is a small piece of information transferred back and forth between servers and clients. It is used by the web-based application to maintain the state in the stateless HTTP protocol (Kristol, 2001). Meanwhile, Flash Cookies were originally used to remember user's preferences such as volume for online videos (Brinkmann, 2007) but they can also be used to re-install regular cookies that a user has deleted, and cannot be controlled through the cookies privacy control in the browser (Schneier, 2009). Web Beacon or Web bugs and Pixels, on the other hand, are pieces of code run on a web page, which can track the user's movement on the page including what is being typed or where the mouse is moving (Angwin, 2010). Different pieces of information (including SNS ID) are being leaked to the third parties from SNS (Krishnamurthy &Wills, 2010a) and non-SNS (Krishnamurthy & Wills, 2009) from the desktop as well as mobile devices (Krishnamurthy & Wills, 2010b) via the use of cookies; which mean a user's online behavior combined with his/her SNS unique ID, and/or mobile phone unique ID, can reveal so much about a person's life. This information sharing or leakages keep increasing without the user's knowledge (Krishnamurthy &Wills, 2009).

The users' information is also being shared via the use of Application Programming Interface (API) among SNS (Ko, Cheek, & Shehab, 2010). The API services allow the third party sites develop social applications without having to build their own social networks. These applications provide interesting contents to users' existing profiles. Through the use of API, SNS allow limited access to the users' information to the third parties. For example, by installing the third party music application called iLike (www.iLike.com), Facebook users can share music with their Facebook friends, and in order to install iLike, users have to give up some certain information to iLike in exchange for the service.

As a result, the user digital dossier can be built at ease with the combination of the user's partial PII, the location information, the mobile device unique identifier and the available large amount of personal data from the API.

DISCUSSION AND ANALYSIS

Let us consider a scenario of a girl named Emilie:
Emilie is a nice and helpful girl. She has just finished her undergraduate degree from a university in Paris. She is updating her profile in LinkedIn and looking for a job. She is also learning English and using Dictionary.com (The site with the most tracking files in a case study by the Wall Street Journal (Angwin, 2010)) as reference for English vocabulary. She is also on Facebook keeping in touch with her friends and relatives. Her activities on Facebook include posting pictures, comments and statuses, using check-in service to reveal her location to her friends, and playing third party game like Farmville (by Zynga). Sadly, she has a friend who is HIV-positive and depressed, and is having problem with drugs and alcohol. In order to provide mental support to her friend, Emilie spends some time searching for information to understand her friend's condition. Meanwhile, she helps her pregnant cousin order the books and vitamin supplements for pregnancy from online stores. Her Internet access is done via both her desktop computer and her mobile phone.

By being part of SNS and non-SNS, Emilie's minimal information being diffused on the internet

include: her online activities, personal information, SNS unique identifier, mobile phone unique identifier, location, interests and preferences. This information is being tracked and recorded by SNS and non-SNS like Dictionary.com.

To find out how privacy concerns are generated by SNS and non-SNS, we analyze Emilie's story based on two ethical theories: utilitarianism and deontology. From a utilitarianism view point, the expected outcome or consequences of an act is very important to determine whether or not that act is morally acceptable while the role of duty and respect for persons are the key to what is morally permissible for a deontologist (Tavani, 2011). Two outcomes can be drawn from the Emilie's story.

Thanks to Facebook default setting which makes users' profile pages publicly available and searchable, Emilie's childhood friends are able to find and reconnect with her based on Emilie's basic personal information including pictures, her hometown and high school. The tracking technologies help to provide the tailored advertisements, and Emilie is able to get the book and vitamin supplements for pregnancy at discounted prices from online stores. Facebook Connect, meanwhile, allows Zynga to provide more interactive and social online games like Marfia wars and Farmville - which allow users to engage more in online games with their existing Facebook friends. The act of sharing and gathering SNS users' information in order to enhance their online experience (e.g. friendship reconnection, relevant ads, and interactive games) appears to be consistent with both Kant's principles of treating people as ends in themselves and the principles of utilitarianism which promote the greatest good for the greatest number.

On the other hand, different pieces of Emilie's information, her interests and preferences are being harvested and tracked without her consent. This information can later be exchanged, transferred, traded, and/or combined. The combination of her online activities, her SNS profiles and her psychological profiles may reveal too much about her, which could be embarrassing or damaging to her future job opportunity. Her job or health insurance applications may be rejected simply because she may be pregnant and she might be involved with HIV, drugs, and alcohol. Almost half of European recruiters seek information on candidates based on their online reputation in various SNS (EurActiv, 2010). What is worse is that not all the information is 100% accurate about Emilie's life. She is neither pregnant, nor HIV-positive, but the cookies are not aware that she did the search for her friend and cousin (YOU ARE WHAT YOU TYPE!). From a deontologist viewpoint, SNS users are not respected as persons and they are treated as means to some ends (the means being users' information while the ends being the income generated from the sales of those information). Their informational privacy is violated since the ability to control what type of information about them is being collected, by whom and for what purpose the information will be used is not given to them. This also results in negativity for online image/reputation and job opportunity for the majority of SNS users - which is not morally permissible according to utilitarianism.

CONCLUSION AND FUTURE RESEARCH

Social network sites (SNSs) offer exciting new opportunities and benefits for interaction and communication, but also raise privacy concerns. SNS default setting, tracking technologies (e.g. traditional cookies, flash cookies and web beacons), and the use of Application Programming Interface (API) among SNSs contribute to the leakages of user's personal information from those SNS to the third party sites, without the user's knowledge. There is no definite answer to who has access to and control over users' information. Large amount of users' personal information are voluntarily shared among SNS or non-SNS. They can be harvested so rapidly and stored for an unknown time period without the user's knowledge. In the event of SNS ownership changes, through merges or bankruptcy, it is not clear what will happen to that information. Different bits of user's information diffused online can be accumulated over time. Through the secondary use of personal information (e.g. data mining technique) from SNS and non-SNS, the user's identity could be combined and revealed.

The users might have different tolerance toward their privacy and/or they might be aware of the collection of bits and pieces of their information, but they may not be aware that the combination of their information can be used to build a detailed profile of their lives. Emilie may voluntarily give her personal and professional information, online game behavior, shopping preferences, and browsing interests to SNS, online game company, online stores and search engine respectively; however, she may not authorize any third party organization to make the secondary use of her information. While analyzing Emilie's story by using ethical theories reveals both positive and negative impacts brought by

cyber-technology, particularly, among SNS and non-SNS. However, to maximize the positive impact, the users should at least have control over the amount and type of information being gathered, how and whether or not it is necessary, and by whom.

Despite the fact that we did not provide concrete solution to the threats to privacy in SNSs, by pointing out the potentials for violating the users' privacy, we hope that this article will raise users' awareness alerting them that they are what they type.

In the future work, we intend to look at the impacts of SNS on privacy from three different angles: technical, social and philosophical. The technical angle will employ a qualitative approach using a case study method of an SNS user to investigate the types of information being leaked/shared among SNS and non-SNS in the HTTP headers and HTTP cookies, and the consequences of the leakages within that case. The social angle will use ethnography method to study the importance of privacy from the perspective of online users, particularly the users of SNS. The finding of these two studies will then be analyzed by using different philosophical theories. The research will shed light on what types of information leakages posing threats to privacy, why privacy is important from social and philosophical viewpoint. It will also provide recommendations to improve the current situation.

REFERENCES

Al-Saggaf, Y., & Weckert, J. (2011). Privacy from a Saudi Arabian perspective. *Journal of Information Ethics*, 20 (1), 34-53.

Angwin, J. (2010, July). The web's new gold mine: Your secrets. *The Wall Street Journal*. Available from: http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html

Boyd, D., & Ellison, N. B. (2007, November). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13 (1-2). Available from http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Boyd, D., & Hargittai, E. (2010, August 2). Facebook privacy settings: Who cares? *First Monday, 15* (8). Available from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086

Brinkmann, M. (2007, May). *Flash cookies explained.* ghacks.net. Available from http://www.ghacks.net/2007/05/04/flash-cookies-explained/

Bymes, H. (2010, September). *Shattered Stephanie rice says sorry over homophobic tweet.* Available from http://www.dailytelegraph.com.au/news/shattered-stephanie-rice-says-sorry-over-homophobic-tweet/story-e6freuy9-1225915930831

EurActiv. (2010, February). *Social networks put careers at risk, survey finds.* EurActiv. Available from http://www.euractiv.com/en/Social-networks-careers-risk

Facebook. (2011, October). *Facebook statistics.* Available from http://www.facebook.com/press/info.php?statistics

Gibbs, M. (2008). Privacy. In D. McDermid (Ed.), *Ethics in ICT: An Australian perspective* (p. 89-123). Malaysia: Pearson Education Australia.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *In Proceedings of the 2005 ACM workshop on privacy in the electronic society* (pp. 71{80). New York, NY, USA: ACM. Available from http://doi.acm.org/10.1145/1102199.1102214

Humphreys, L., Gill, P., & Krishnamurthy, B. (2010, June). *How much is too much? privacy issues on twitter.* Available from http://www.cs.utoronto.ca/~phillipa/papers/ica10.pdf

Irvine, C. (2009, August). *Facebook and twitter users could be targeted by burglars.* The Telegraph. Available from http://www.telegraph.co.uk/technology/twitter/6096677/Facebook-and-Twitter-users-could-be-targeted-by-burglars.html

Ko, M. N., Cheek, G. P., & Shehab, M. (2010, August). Social networks connect services. *Computer: Innovative Technology for Computer Professionals*, 43 (8), 37-43. (IEEE Computer Society)

Krishnamurthy, B., & Wills, C. (2009). Privacy diffusion on the web: a longitudinal perspective. *In Proceedings of the 18th international conference on world wide web* (pp. 541{550). New York, NY, USA: ACM. Available from http://doi.acm.org/10.1145/1526709.1526782

Krishnamurthy, B., & Wills, C. E. (2008). Characterizing privacy in online social networks. *In Proceedings of the first workshop on online social networks* (pp. 37{42). New York, NY, USA: ACM. Available from http://doi.acm.org/10.1145/1397735.1397744

Krishnamurthy, B., & Wills, C. E. (2010a, January). On the leakage of personally identifiable information via online social networks. *SIGCOMM Comput. Commun. Rev.*, 40, 112{117. Available from http://doi.acm.org/10.1145/1672308.1672328

Krishnamurthy, B., & Wills, C. E. (2010b). Privacy leakage in mobile online social networks. *In*

Proceedings of the 3rd conference on online social networks (pp. 4{4). Berkeley, CA, USA: USENIX Association. Available from http://portal.acm.org/citation.cfm?id=1863190.1863194

Kristol, D. M. (2001, November). HTTP cookies: Standards, privacy, and politics. *ACM Trans. Internet Technol.* , 1 , 151{198. Available from http://doi.acm.org/10.1145/502152.502153

Nash, A. (2009, December 28). *Linkedin for iphone 3.0: Let's get this party started*. LinkedIn Blog. Available from http://blog.linkedin.com/2009/12/28/linkedin-for-iphone-3-0-lets-get-this-party-started/

Palihapitiya, C. (2010, February 11). *Facebook mobile: 100 million and growing*. Facebook Blog. Available from http://www.facebook.com/blog.php?post=297879717130

Schneier, B. (2009, August). *Flash cookies*. Schneier on Security. Available from http://www.schneier.com/blog/archives/2009/08/flash\ cookies.html

Slee, M. (2007, January 10). *Facebook your phone*. Facebook Blog. Available from http://ja-jp.facebook.com/blog.php?post=2228532130

Tavani, H. T. (2007). *Ethics and technology: Ethical issues in an age of information and communication technology* (2nd ed.). United States of America: Bruce Spatz.

Tavani, H. T. (2011). *Ethics and technology: controversies, questions, and strategies for ethical computing* (3rd ed.). United States of America: Wiley.

Young, K. (2009). Online social networking: An Australian perspective. *International Journal of Emerging Technologies and Society,* 7 (1), 39-57.

Zuckerberg, M. (2010, July 22). *500 million stories*. Facebook Blog. Available from http://www.facebook.com/blog.php?post=409753352130

Virtual Reality Simulations: Who is responsible?

J Barlow

School of Arts and Sciences, Australian Catholic University, Sydney.
Email: John.Barlow@acu.edu.au

ABSTRACT: *There is no doubt that continued improvements to the output of simulation products using virtual reality techniques has significantly contributed to their entertainment, information representation, testing and training utility. However there is an increasing concern that many users of simulation products where virtual reality is a significant feature of the output often find it difficult to distinguish between the veracity of their decisions made in the context of the simulation output and the possible consequences of such decisions in the real world. This paper will initially examine the nature of virtual reality as a simulation output tool followed by an exploration of the limits of responsibility associated with the use and misuse of simulation products where virtual reality is a key feature of their performance and perceived utility as entertainment, information representation, testing and training tools.*

Teaching Ethics to ICT Practitioners

G R Seach[1], M Cattaneo[2], and O K Burmeister[3]

[1] *Pacific Database, Australia,*
E-mail: gseach@pacificdb.com.au;

[2] *ITMasters, Australia,*
E-mail: *marco.cattaneo@digano.com;*

[3] *School of Computing and Mathematics, Charles Sturt University, Australia,*
E-mail: oburmeister@csu.edu.au;

ABSTRACT: *Case-based ethics teaching is common in many disciplines, including in ICT. What is needed is a systematic approach that learners can employ to discover solutions to the ethical dilemmas raised in case studies. The Doing Ethics Technique has been used widely in tertiary teaching of ICT ethics in Australia. Its use in teaching masters students, all of whom were industry practitioners, is explored in this article, both from a teacher's and student's perspective. It was found to have limitations, including overlapping process questions and no independent assessment of the efficacy of ethical solutions that result from it. However, overall it was found to be effective in helping students to follow a systematic and relatively simple process to deriving good, though not necessarily the best, ethical solutions.*

Keywords: Case study, pedagogy, professionalism.

INTRODUCTION

In recent years there have been several disillusioning experiences in relation to information and communications technology (ICT) ethics education. A recent book Weckert and Lucas (2012) presents various findings from a national survey of the industry which found that ICT graduates were more likely to engage in unethical practices, than people working in ICT who had not graduated from a tertiary ICT course. This suggests that although all universities in Australia teach ICT ethics, there is a mismatch between what is taught and what is learnt. Similarly in research involving ICT graduates who had been working at least 18 months, it was discovered that although all of the participants had experienced ethical dilemmas in the workplace, little of what they had been taught at university had prepared them for what they confronted (Burmeister & Sharma, 2005). Thus it behoves educators to consider how ICT ethics are being taught and what more can be accomplished to improve the outcomes for graduates, that is, outcomes that help them to engage professionally in ethical situations that arise in the workplace.

This article considers how ICT ethics is taught to practitioners. In the early 1990s the Australian Computer Society introduced a requirement that ethics be taught in an ICT course, as one of the requirements for their accreditation of ICT courses. Since that time the majority of ICT courses at Australian universities have either incorporated ethical issues into existing subjects, or required students to take an ethics subject as part of their course. At Charles Sturt University (CSU), through a partnership with ITMasters, practitioners undertake advanced training in a combination of industry certifications and post-graduate tertiary subjects, to complete a Master's degree in a specialist ICT area. All the specialist areas share one subject in common, ITC506 Topics in IT Ethics. The discussion which follows first describes that subject, and demonstrates how one technique in particular reinforces and permeates the teaching. It is a simple technique that guides participants in ethical decision making. Experiences in teaching and learning that technique then are described.

ITC506 TOPICS IN IT ETHICS

ITC506 Topics in IT Ethics (ITC506) is taught in distance mode only; there are no on-campus ITC506 classes. At CSU ICT subjects beginning with 1, 2 or 3 (such as ITC331) are undergraduate subjects, a 4

indicates a postgraduate diploma and a 5, as in ITC506, indicates a masters level subject. The ITC506 student cohort consists of professionals, typically with 5 to 15 years experience in the ICT industry. Pedagogically ethics tends to be taught either following a 'golden thread' approach, in which ethical issues are incorporated into other subjects, or following a standalone subject approach. ITC506 is an example of the latter. The syllabus design for the subject is such that it begins with promoting the need for ethical competence. A variety of approaches have been employed, such as asking all students to view "I Robot", starring Will Smith, and to note all the ethical issues within that movie that are related to ICT. That tends to result in a lively discussion in the threaded email discussion list, in the course management software employed to teach this subject. It also serves to engage the students in ethical discussions from the very first week. The syllabus design next focuses on discussion of ethical concepts in a directed fashion, and on discussion of ethical theories, including consequentialism, deontology, utility and others. Case study analysis is a primary means of teaching the subject, utilising cases available on the website of the Australian Computer Society (ACS), that are all real situations, although some have had identifying details altered. The professional code, that is the ACS Code of Ethics, is also taught through case study analysis. The text employed in the subject is the only Australian ICT ethics text currently available (McDermid, 2008b). Following its use in that text, the main case study analysis tool taught to students is the Doing Ethics Technique (DET) (Simpson, Nevile, & Burmeister, 2003). The assessment supports the syllabus design, through case study analysis that requires not only the use of the DET, but evidence of appropriately discussing ethical theories and the ACS Code of Ethics, in the solution justifications. Structured comments on assessment items, and the timing of assignment feedback, assist students to learn from one assignment and improve performance in the next, and ultimately in the exam.

A TEACHER'S PERSPECTIVE[1]

A deep and lasting understanding of classical ethical theory can only be acquired through many years of focused academic study. A scaled appreciation of the general principles of ethics, on the other hand, can be achieved in a shorter timeframe. A practical understanding, for the purposes of ICT education, lies somewhere in the middle, but the most effective means of imparting that knowledge, and indeed what constitutes an acceptable level of understanding, is difficult to quantify.

   Teaching ethics to postgraduate ICT students is a challenge. Former teaching models involved a combination of classical ethical theory and structured argument, but the ability to apply a detailed knowledge of ethical theory in real-world contexts proved difficult to acquire within the time constraints of a single teaching session.

   The DET provides a procedural framework for teaching and learning about thinking ethically in real-world contexts, and in the process, acquiring an understanding of applied ethics. The term applied ethics is highly relevant here because the aim of ethics in postgraduate ICT education is to engender an understanding of how to determine the right thing to do in various scenarios – not to create professional ethicists. Co-incidentally, the approach offered by the DET aligns students' understanding of ethics with the principles proposed by industry codes of ethics.

   Because the DET is a framework, the practitioner can employ classical ethical theory, structured argument and industry codes of ethics in any combination to determine the best course of action in a given scenario. One of the benefits of the DET is its theory independence.

   Over the past three years of teaching ethics to postgraduate ICT students, a wide range of philosophical aptitude is noted at the beginning of the session, which is in-line with statistical norms. A marked degree of both cultural and socioeconomic relativism is noted, as is a clear difficulty differentiating strictly ethical issues from social, legal and other issues. Lastly, an unstructured and haphazard approach to scenario analysis is also evident. None of this is surprising as one would expect students to have little knowledge of the subject matter before undertaking ITC506, however, over the course of the teaching session, forum discussions and assessment item submissions indicate a deepening analytical ability and a growing capacity to think more broadly. For technologists who typically focus

---

[1] This section is predominantly a reflection from a sessional teacher of ITC506, who has been an ICT professional for over 25 years, and continues to work full time in the ICT industry. He has not taught ethics at any other university.

more on the technical aspects of their learning, rather than the so-called soft subjects, this conceptual growth is promising.

When compared to the observed progress achieved with the structured argument model taught in previous sessions, the DET approach appears more effective in teaching logical scenario analysis. Anecdotal evidence suggests a preference for the DET due to its simple logical structure and its lack of reliance on a deep understanding of theory. Students appear to have more difficulty understanding the logic of structured argument. In sessions where a hybrid DET/structured argument approach is taught, the quality of student analysis leans in favour of the DET.

Misunderstandings about ethical theories and the difference between ethical and non-ethical issues are naturally resolved by studying classical theories and industry codes of ethics, but even a superficial understanding of classical theories can be immediately applied to DET analysis.

The DET is defined by a series of steps, which when followed in sequence to analyse an ethical scenario, facilitates students' understanding. After the first semester of teaching the passive form of the DET, with a view to eliciting deeper analysis from the students, questions 1 and 5 were divided into two questions each, resulting in an overall eight questions. The procedural sequence remained the same. Although the eight-step format is optional, many students choose it, and experience shows that it does force them to think more deeply about the scenario under analysis. However, a statistically significant number of students fail to understand the difference between each of the exploded questions. For example, Question 1 (What's going on?) should elicit a generalised summary of the case, whereas Question 2, (What are the facts?) should be a factual description of the case. The same can be said of questions 5 and 6 (What can be done about it?, and What are the options?). These errors are not deemed important, however, because the overarching aim of the DET is to provide a framework for students to learn to analyse scenarios, isolate the inherent issues, to understand the implications they hold for all stakeholders, and to ultimately arrive at a preferred ethical outcome.

Similarly, the DET question, "What are the issues?" should elicit a wide range of issues, including factual, legal, social, professional and of course, ethical. Although students study classical and professional ethics in parallel with practice using the DET, some students still omit or confuse the purely ethical issues from this question. Again, this error is not important because Question 6 of the DET requires students to isolate and discuss purely ethical issues. Some students still manage to confuse issues in response to this question, however, the percentage of such errors is low. Experience shows that when students are able to converse with the teacher and each other, and practice the technique, they acquire a deeper understanding of the meaning and purpose of each question, and thus acquire more effective analytical skills. Participation in forum discussions has a similar impact.

In conclusion, using the DET as the model for ethical analysis, a marked improvement in the overall quality of analysis is noted in the majority of students which is qualitatively higher than that achieved by using a structured argument or a hybrid approach. It is expected that students will take this new expertise into professional practice. Certainly post-session feedback from students studying the DET model is more positive than that received from other students.

THE PASSIVE AND ACTIVE FORMS OF THE DET

The DET was first developed at Swinburne University of Technology (SUT), by Christopher Simpson in the 1980s. Simpson had been an ICT industry professional for all his adult life, and began teaching in his late 50s, taking over the ethics teaching as part of his portfolio. He found that few students understood how to systematically resolve an ethical dilemma and the earliest form of the DET resulted from his attempts to help his students. When Burmeister also began teaching ethics at SUT, the two academics progressively refined the DET, to the two forms it has presently, the passive and active forms.

The passive form of the DET, as seen in Figure 1 is what is taught in ITC506, as well as in undergraduate ethics teaching at CSU. The technique has also been widely taught in Australia (Burmeister, 2008; McDermid, 2008a; Simpson et al., 2003). It is passive, in that it is a systematic way for an individual to work through an ethical dilemma. The active form has also been effectively taught to ITC506 students, and others (Simpson et al., 2003). However, the active form requires the participation of multiple people, with individuals or groups taking the perspective of one stakeholder

group. The active form of the DET tends to result in a richer set of variables and better ethical solutions, because it takes into account the multiple and often competing viewpoints of different stakeholders. Furthermore, it can involve role-play and thus dramatic enactments, in which differing stakeholder groups can argue in favour of their position, or against the positions taken by other stakeholders. Consensus is not the aim, but rather, understanding and valuing each others' differences. Thus the active form of the DET is useful in workshops and face-to-face tutorials, and results in solutions that are qualified. That is, the solutions can articulate how certain options favour one or another stakeholder group, and thus unlike the passive form of the DET, a greater breadth and richness is reflected in the final solution. However, for distance students, engaging in the type of facilitated group work that the active form of the DET requires, can be difficult.

Within ITC506 the active form of the DET has been effective is in workshops. That is, CSU has organised workshops in a capital city and invited ITC506 students to attend. The feedback from students about the use of the active form of the DET in those workshops has been very positive. However, those workshops have been discontinued, because they raised equity issues. For example, it was not possible for all students to attend, and typically only about 20% of enrolled students took part in them.
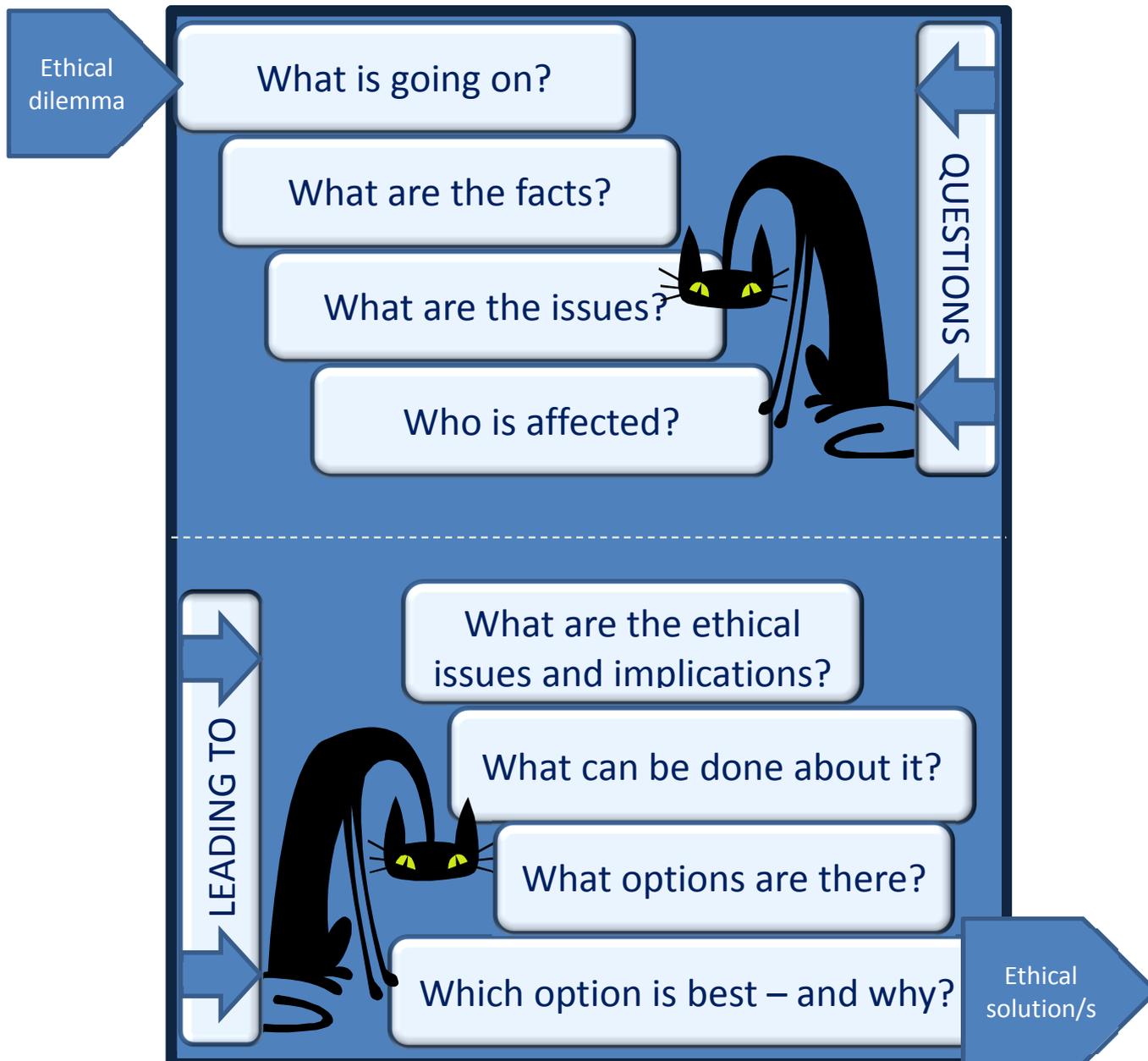

Figure 1: The passive form of the Doing Ethics Technique

Figure 1 represents Schrödinger's cat[2], as the outcome from an ethical dilemma only becomes clear once you look inside the box and start to examine the dilemma. The DET describes a logical process that avoids solving an ethical dilemma on the basis of emotions. Thus the box represents a system/process with standard inputs and outputs. The diagram also visually portrays a weakness of the DET, namely that there is no measure of its efficiency/effectiveness.

Q1. WHAT'S GOING ON?

This is a synopsis of what the case is all about. It can be taken from a variety of perspectives, for example, from the perspective of a person raising a complaint, in which case, it is a synopsis of the complaint. It can be taken from the perspective of an involved observer, in which case, it is an outline of what was observed, without going into too much detail. Where you see multiple perspectives, you should describe them here.

Q2. WHAT ARE THE FACTS?

This is a descriptive list of the facts of the case. This doesn't just describe the case; it lists the facts as they are known (from all sources and perspectives), and also what one might reasonably consider to be possibilities. For example, if a person was raising a complaint, Q1 would outline their complaint, and Q2 would provide the evidence to both support and refute that argument. All such facts must be demonstrable or supportable. It would be worthwhile to assign a credibility weighting to each fact, to help with later analysis.

Q3. WHAT ARE THE ISSUES?

This is a list of ALL the issues that are involved in the case, whether they be ethical, legal, or otherwise. In Q5 we can extract only the ethical issues for further analysis, but for now, simply extract and describe every relevant issue you can think of.

Q4. WHO IS AFFECTED?

This is a list of all the stakeholders involved in the case. This need not be restricted to the ones specifically mentioned in the case; you should consider who/what else might be affected by the issues listed at Q3, regardless of the degree to which they are affected. In this question, you should describe how each stakeholder is affected, both positively and negatively, and perhaps comment on the degree of effect.

The line separating the first four questions from those that follow, in Figure 1, indicates that the case analysis now changes from the general to specifically considering the ethics of the case.

Q5. WHAT ARE THE ETHICAL ISSUES AND IMPLICATIONS?

For this question, you need to extract only the ethical issues identified at Q3. List the ethical issues, discuss them in terms of classical ethical theory (as best you can), and discuss their implications – on the stakeholders, as well as on the ICT and wider community. Professional codes of conduct should also be considered in this evaluation of the issues and implications.

Q6. WHAT CAN BE DONE ABOUT IT?

This question elicits a general idea of what can be done to resolve the case, whether those ideas are practical, possible, or not. Generally what kind of resolutions might there be? You need not go into great detail to answer this question, as its purpose is to provide a basis for answering Q7, but you do need to think broadly and laterally to come up with several alternatives.

Q7. WHAT ARE THE OPTIONS?

This question requires that you list and describe (in detail) all the possible options that might be available to resolve the case. Be creative here; the most obvious options are not always the best. It's possible that not all options will result in a positive outcome for all stakeholders. List and describe at least three different options, and discuss the benefits and detriments of each.

Q8. WHICH OPTION IS BEST - AND WHY?

---

[2] Schrödinger's cat is a famous 1935 quantum mechanics thought experiment about possible outcomes involving a cat placed inside a box.

In answering this question, you need to assess which of the options described in Q7 is the best. You are recommending one of several options here, so you need to argue for your recommendation, providing a solid basis in fact and reasonable (and supportable) conjecture.

A STUDENT'S PERSPECTIVE[3]

As an ICT veteran, having grown up in a world of Commodore VIC-20s, IBM 390s, Prime computers and the first IBM Desktops being placed on office desks at a cost of $20,000 each, ICT ethics was something unheard of. We would be using Kermit to send over some files at 1,200 bps using an old analogue telephone line. Quickly copying something like Novell Netware 2.x would be virtually impossible, and WordPerfect licenses would arrive at pallets with one huge box of manuals and a stack of floppy diskettes for every single user.

Fast-forwarding into the 21st century things look rather different today. Daily news bulletins are showing us a world where big-shot executives are paying themselves multi-million dollar bonuses for losing billions or sending their own century-old company down the drains, young adults being jailed for trading on the share-markets with insider information, kids disclosing their complete lives on Facebook with potential groomers, and a business environment where so called "respectful" companies do literally anything as long as they can make some bucks and survive in this world, where all too often doing the wrong thing seems to be more lucrative, than doing the right thing. Unfortunately, as an IT professional I've seen too many organisations and so called friends ripping off intellectual property, for money. Democracy is a great thing, but too much freedom seems to have its disadvantages too, one of them being a system of values, morale and ethics highly vulnerable to outside forces, including ICT.

As a professional you start to put question-marks behind decisions. Is there such a thing as responsibly downloading a movie from the Internet? Is there such a thing as making the right or wrong decision? As a student in ITC506 I was pleasantly surprised that the answer to these questions is an absolute, carved in concrete, big-time, "yes". No one on this planet is perfect, and no-one has all the answers.

Ethical thinking and following a logical ethical decision-making process is something people need in this ever changing, sometimes chaotic world of global competition, virtuality and unlimited real-time information access. By following a process of information-gathering, asking the "right" questions, understanding the needs and concerns of all parties involved, and the various options and impact they may exert, it is possible to make the right decisions and select the best path forward given the information available at the time, and under the unique conditions and circumstances under which the decision is made. Realise that all decisions aren't made in a vacuum, but are made in a spectrum of possible decisions and outcomes.

We should all learn to apply systematic ethical guidelines and make these guidelines a part of who we are, ensuring all our decisions have the best possible outcome the moment they're taken. Cogito ergo sum: I think, therefore, I am - but also - I think, therefore I'm able to make the best possible ethically justifiable and defendable decision.

CONCLUSION

The DET is not being portrayed as the best approach, nor ITC506 as a model for teaching ICT ethics, but rather, this paper has shown that in the teaching of case-based ethics, a systematic process for dealing with a case is needed. At least in the teaching of ITC506, the DET has been effective, as a systematic means of applying ethical thinking in a situation. Telling students to 'think ethically' about a case study does not work. They do not know what to do. Having a systematic approach to follow, even if it does not result in the best outcome, will result in a much better outcome, than would otherwise be the case. That is, ITC506 demonstrates that good pedagogy is not about telling students what to believe, but about helping them to argue for their views, and about them developing well-reasoned positions. A future research strategy that is currently being investigated is a comparative analysis of the DET and other techniques for the systematic resolution of ethical dilemmas, with a view to either improving the DET by borrowing from other techniques, or replacing the DET with a better technique.

---

[3] This section is predominantly a reflection by a student, 12 months after completing ITC506.

REFERENCES

Burmeister, O. K. (2008). Introduction. In D. McDermid (Ed.), *Ethics in ICT An Australian Perspective* (pp. 1-26). Frenchs Forest, NSW: Pearson.

Burmeister, O. K., & Sharma, A. (2005). *Professionalism in ICT: meeting the challenge of ethical dilemmas in the workplace.* Paper presented at the Fourth Australian Institute of Computer Ethics Conference, Deakin University, Geelong.

McDermid, D. (2008a). Employment and work. In D. McDermid (Ed.), *Ethics in ICT An Australian Perspective* (pp. 231-248). Frenchs Forest, NSW: Pearson.

McDermid, D. (Ed.). (2008b). *Ethics in ICT An Australian Perspective*. Frenchs Forest, NSW: Pearson.

Simpson, C., Nevile, L., & Burmeister, O. K. (2003). Doing Ethics: A Universal Technique in an Accessibility Context. *Australasian Journal of Information Systems, 10*(2).

Weckert, J., & Lucas, R. (2012). *Ethics and the Governance of ICT*. Canberra, Australia: ANU E-Press.

Complexities in the Ethics of Informatics Research and Innovation

C McDonald

Faculty of Information Sciences and Engineering, University of Canberra, Australia
E-mail: craig.mcdonald@canberra.edu.au

.

ABSTRACT: *Ethics in ICT research and innovation is complex. This paper outlines complexities in the discipline itself, in the technology, in notions of ethics, in research and innovation and, finally, in the interaction of all these aspects. It argues that some of this complexity is exacerbated by conceptual difficulties and examines the* Framework for Responsible Research and Innovation in ICT *project as an approach to addressing complexity.*

Keywords: *Complexity, Ethics, Research and Innovation.*

INTRODUCTION

During the Second World War some human medical research and atomic technology innovation occurred which was later considered ethically questionable. Since that time there has been a growth in attempts to govern research and innovation from an ethical perspective. Research involving humans as participants is being addressed in institutions through governance and policy. For example Australia's National Statement on Ethical Conduct in Human Research says:

> ...the values of respect, research merit and integrity, justice, and beneficence have become prominent in the ethics of human research in the past six decades, and they provide a substantial and flexible framework for principles to guide the design, review and conduct of such research. This National Statement is organised around these values (NHMRC, 2009 p11).

However the ethics of research and innovation in technology is less settled. It is under continual debate, across the very wide range of technologies with journals (see for example biotechnology or nanotechnology (Weckert, 2007) and conferences, policies and regulation, courses and professional interest. ICT is no exception. This paper looks at some of the complexities associated with ethics in ICT research and innovation and an approach to making sense of them.

The term 'ICT' is slippery. Literally ICT would refer only to technologies that detect signals, transmit, store, process and present them, but, perhaps because it is so ubiquitous, it is often used much more broadly. This paper will use 'Informatics' to refer to the study of 'information' – its nature, the systems and technologies that create, store, process and present it, the human, organisational and social context within which it is set and the personal, relational, economic, political, aesthetic and environmental impacts it has. Where 'ICT' has been used by others, it is taken to mean informatics, while IT (information technology) will be used literally to refer to information processing hardware and software.

COMPLEXITIES IN THE INFORMATICS DISCIPLINES

There are two types of practical disciplines involved in informatics. Disciplines of the first type concern themselves with information as their ***subject***. This group includes technical infrastructure, data management, information management, knowledge management, information systems, web-based systems and content management, graphics design, multi-media, geographic information systems, librarianship, journalism, grid computing, agents, etc. The sorts of topics of interest here are how data, information and knowledge is created, stored, processed, communicated and presented; the technologies and techniques involved; the designing and building of systems; the issues it raises (reliability, validity, privacy, ownership, etc.); the environment of information use; and the repercussions of information control for the individual, the workplace and society.

The second type of practical informatics discipline examines the above topics in relation to a particular knowledge domain. These disciplines see information *instrumentally*. Health Informatics is the most advanced of the applied informatics disciplines. It examines topics from the GP looking after patient records, through to using knowledge-based systems for diagnosis, remote medicine, medical research and government health policy formulation. Other areas of applied informatics include business informatics, e-learning, e-government, e-law, e-research, etc. The sorts of topics of interest to these disciplines go to how practitioners can take more informed, effective, evidence-based actions, how knowledge in the domain can be better applied and how better systems can be created.

Additionally less practical disciplines address information in their own ways. The philosophy of information (Floridi, 2002) is at one extreme and popular literature (e.g. Gleick, 20110) at another. There is a ubiquity of interest in information across the whole range of human thinking. Many disciplines have perspectives on information and its role in their work. For some, genetics for example, information has become a defining conception, albeit a conception very different from that of ICT. So informatics thinking becomes riven by a plethora of conceptual frameworks and investigative approaches from genetics, science and technology studies, philosophy of information, engineering, humanities, neuroscience and psychologies, social sciences and so on. The many views of informatics leads to disciplinary complexity as the many approaches come with incommensurable vocabularies, conceptual structures and mores. Over time, disciplines form and sub-divide further complicating the issue. There is nothing inherently wrong with this pluralism, however in an increasingly interlinked world, one of keyword search across the human corpus, the disciplinary context of concepts can be lost and discussion fragments.

The informatics disciplines are complex.

COMPLEXITIES IN INFORMATICS PHENOMENA

Most academic disciplines study *apparent* phenomena - physical sciences study physical reality, social sciences study humans in their interactions with others, humanities… and all have a long history behind them. Information seems to be a *virtual* phenomenon that has remained largely in the philosophical domain until information technologies started having significant impacts on human activity. Much of the ethical force generated by informatics is in fact about the information being carried, a virtual entity, rather than the technology itself. This makes the information phenomena a difficult thing to define.

Further, to see informatics as a single category, as one phenomenon, is so broad as to be virtually useless. Computing is a very general, malleable technology. It plays very different roles in different applications. The issues raised in social media seem quite different from those of data warehousing, robotics or AI. The use of too abstract a conception is a major cause of discourse fracture.

Digital divides provide another problem for studying informatics. The divides based on infrastructure and technology availability, wealth, education, age, gender, culture, organisation and other factors mean that particular technologies play out very differently in different circumstances.

Rate of change is a further factor creating complexity in informatics. Technology change is fast and discontinuous while many of the human structures around it move to a different rhythm. The law, the economy, institutions, and research itself are naturally slow and based in stable views of their worlds.

A 'friend' in Facebook; a document in 'the cloud'; these are examples of concept re-use that is common in information technology. The issue here is that attributes of a pre-existing concept may, or may not be carried into its technology incarnation and other attributes may become associated with the concept making discourse disjoint. As this terminological adoption shifts over quite short time periods informatics is always a work-in-progress, continually changing. So a stable platform for discourse cannot be relied on and new research cannot necessarily build on what previous research no matter how rigorous and relevant it may have been at the time.

The nature of informatics then is complex.

COMPLEXITIES IN ETHICS

Ethical discourse has a long and complex history. The examination and creation of moral values their through ethical discourse is tough enough, but sorting them from

- the aesthetic (responding to the beautiful),
- political (responding to the powerful),
- economic (responding to market values),
- social (responding to engagement with others) and
- legal (responding to rules & enforcement)

Aspects of human activity is fraught. While ethics might be seen as another aspect of human activity like those listed (responding perhaps to the right and the good), it may also be seen as a more overarching idea embracing some of those other aspects, but giving an added moral force.

Ethical issues raised by informatics are discussed in many different places and in many different ways. One place that values coherent, objective discussion is a university course (Greening et. al., 2004). In ethics courses there seem to be four main kinds of discussion about ethics and systems development.

The first tackles particular ethical issues raised by the use of technology, like workplace surveillance, cybercrime, privacy or copying software. The legal system has a strong interest in this kind of discussion so it is critically important. The second kind of discussion looks at specific events, real or made-up. Particular situations throw up unusual ethical aspects and dilemmas that highlight the complexities of ethics. For example, the set of ethics cases studies provided by the Australian Computer Society (ACS, 2004) reveal the complexities and contradictions that seem inherent in ethical considerations of particular situations.

The third discussion revolves around prescribed ethics, including professional codes of ethics and conduct, specific codes and good practices (such as a university code of practice for research), UN Declaration of Human Rights and so on. The final kind of ethical discussion starts from first principles and sees issues and events as applications of ethical principle - the categorical imperative, the golden rule, harm minimization, etc. For example, if the utilitarian principle of 'the greatest good for the greatest number' were to be applied to a situation, how would we measure 'good', can we add it, how could we balance the good to one person against that to another, etc.

These four kinds of discussion go some way to framing complexity.

Professional Ethics also tries to frame complexity. It uses social instruments like codes of ethics and codes of professional practice and disciplinary committees to regulate professional activity (ACS, 2012). Research Ethics is akin to professional ethics in using similar techniques - national Statement on Human Research Ethics for example, institutional policies and procedures, Research Ethics Committees and ethical misconduct committees. Professional ethics seem to be fairly stable and increasingly widespread but not deep. ICT professional ethics seems to have little impact in the face of other innovation drivers (Lucas & Mason, 2008).

Ethics is complex.

COMPLEXITIES IN RESEARCH AND INNOVATION

Traditionally *research,* at least academic research, has been for creating coherent theory allowing the understanding of a phenomenon. Gregor (2008) highlights three main forms of understanding - gaining a clear description of the phenomenon, developing an account of its dynamics (a causal model), and developing predictive capabilities (which may be purely statistical and not relying on an account of its dynamics). In contrast, *innovation* has been for action - deliberative action supported in part by theoretical knowledge from research findings.

Information technology research and innovation doesn't often follow this pattern. Research and innovation in IT are not linear, and often hard to separate. 'Generate and test' (aka trial and error) is common IT development method for both research and innovation. This approach is aimed at finding

what works, not theory building about either the process or the product of the research. 'What works' seems not coherently constructed, contextualised or published as theory and theory change aims to be.

Much IT research and innovation is ungoverned. It happens:
- in industry, where innovation is secret and protected for commercial reasons,
- in defence, where innovation is secret and protected for reasons of national security and
- privately, which was not significant until the advent of open-source became a way for private innovation to be implemented in large scale, the internet that allowed private hacking and innovation around malware and which has accelerated in 'apps' development.

In contrast, regulated research environments such as universities are, largely, unable to act in the same way as industry, defence or private innovators. Ethics committees, for example, require research plans and reflections on plans that are not required elsewhere. As it turns out, however, Ethics committees see little of university-based IT research as they do not seem concerned with either secondary stakeholders (those not immediately participating in the research process but who are affected by it), or the consequences of the research and innovation. For example, it is not clear that a new algorithm to control a machine processing chemicals would go to an ethics committee, even if there was a possibility of enormous environmental damage were it to malfunction in practice.

IT is a technology accessible to anyone for unconstrained innovation - apps development, hacking, virus creation, cybercrime, etc. It does not require large investment or large numbers of people as research in many other fields do.

Research and innovation in IT is complex.

ADDRESSING EXPONENTIAL COMPLEXITY

Ethics in ICT research and innovation is a complex field because of the interactions of aspects which themselves are complex. We seem ill-equipped both in:
- our theories / frames of meaning around both ICT and ethics, and
- our capacity to govern / influence innovation.

The *Framework for Responsible Research and Innovation in ICT* (FRRIICT) is a project recently funded by the UK's Engineering Physical Sciences Research Council (EPSRC) in part to "develop an in-depth understanding of ICT researchers' ethical issues and dilemmas in conducting ICT [and] provide of a set of recommendations and good practice to be adopted by EPSRC and the community" (FRRIICT, 2012). The project comprises four major activities:
- Landscape of ICT Ethics: including a baseline study conducted using a bottom-up approach in order to understand current perceptions of ethics in ICT. We will identify challenges and changes suggested in practice or process as identified by those who most want and need them.
- ICT Community Ethics Network: develop a community to engage with the ethical challenges posed by ICT and some possible responses to them.
- ICT Ethics Case Studies: a number of cases will be taken from across the ICT spectrum to reflect a range of issues and contexts.
- Responsible Research & Innovation Observatory: the development of a Responsible Research and Innovation Observatory will be created to hold the information gathered within the project and to disseminate best practice, promote recommendations and engage external communities. Central in the resources held by the Observatory will be curriculum development materials, a New Research Support Pack together with tailorable resources for use in undertaking ethical assessments (FRRIICT, 2012).

These activities may well advance our capabilities for responsible research and innovation in ICT. The ongoing observatory will be an organising force showing how to operationalise normative ethical concepts through method & design technique so they can be used through ICT. The extension program will provide useful knowledge and tools to decision makers (in research ethics committees, professional bodies, funding bodies, policy formation) and to other actors (researchers, practitioners, teaching academics, students).

CONCLUSION

Yet underlying these FRRIICT activities is a formidable intellectual challenge. The challenge is to address the complexities touched on in this paper. A new kind of theoretical framework may be required. Two of its characteristics may be a:

- levelled structure with a long-term robust conceptual structure at its heart but that at more superficial levels can morph and reshape to address specific trends and re-conceptualizations,
- discourse component that shows how to move between levels and between the different discourses identified in this paper (for example McDonald et. al., 2010).

The first of two intellectual methods and tools that will be required is conceptual analysis or ontology. Part of the complexity noted in this paper results from incompatible and rapidly changing conceptual structures. New methods and technologies will be needed to address them. The second method is the systems approach to model situations coherently and points in systems where ethical issues might be best detected & addressed.

This paper has presented some of the complexities in the ethics of informatics research and innovation. It reviewed the FRRIICT as a current approach to the overall issues in the field and pointed to some of the intellectual issues that lie ahead.

REFERENCES

ACS (2004) ACS Ethics case Studies.
    http://www.acs.org.au/index.cfm?action=show&conID=200410061237076065
ACS (2012) Code of Ethics and Code of Conduct.
    http://www.acs.org.au/index.cfm?action=show&conID=coe
Floridi, Luciano (2002) What is the Philosophy of Information? Metaphilosophy, 33.1/2: 123-145
FRRIICT (2012) Framework for Responsible Research and Innovation in ICT
    http://www.oerc.ox.ac.uk/research/FRRIICT , http://responsible-innovation.org.uk/
Gleick, James (2011) The Information Forth Estate.
Greening, T., Kay, J. and Kummerfeld, B. (2004) Integrating ethical content into computing curricula.
    Sixth Australasian Computing Education Conference, Dunedin, NZ.
Gregor, S. (2002). A theory of theories in information systems In S. Gregor and D. Hart (Eds.)
    Information Systems Foundations: Building the Theoretical Base Australian National
    University, Canberra, 1-20.
Lucas, R. & N. Mason (2008) A Survey of Ethics and Regulation in the ICT Industry: Ethics
    Education, Journal of Information, Communication, & Ethics in Society, Volume 6 Number 4
    2008, 349-363.
McDonald, D., Bammer, G. & P Deane (2009) Research Integration Using Dialogic Methods ANU
    ePress.
NHMRC (2009) National Statement on Ethical Conduct in Human Research National Health and
    Medical Research Council
    http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/e72.pdf
Weckert, J (2007) NanoEthics Springer

Cyber-bulling and vigilantism: Should social media services be held to account?

S Leitch and M Warren

School of Information Systems, Deakin University, Australia
Email: shona@deakin.edu.au; mwarren@deakin.edu.au

ABSTRACT: *The Internet has developed into a global social network and reflects many of the world wide social problems that society in general faces. This paper examines a number of cases where physical social and ethical situations have transferred into the technology mediated communication domains. The paper will investigate the complexity around these issues. This paper will examines the new form of bullying that is being played out weekly in the media, that of cyber bulling, specifically on social networking sites. The traditional and direct forms of bullying are being replaced by consistent abuse via social networking due to the ease and accessibility of these new forms of communications.*

Keywords: social media, bullying and ethics.

INTRODUCTION

The initial focus of the Internet was the distribution of information in a static manner but over time the Internet developed into Web 2.0 (Leitch and Warren, 2011). The Web is no longer a collection of static pages of XHTML that describe something in the world. Now the web is the world where everything and everyone casts an "information shadow", an aura of data which, when captured and processed inelligently, offers extraordinary opportunities and mind-benign implications (O'Reilly and Battelle, 2009).

The initial concept of Web 2.0 has since evolved into "Social media". This paper uses definitions from Seendahera (2011) to define the different terms in relation to social media; "*Social Media are web based services that provide space for in-depth social interaction to share, discuss and collaborate, facilitated by one or more media rich functionalities, whereas Social Media Services (SMS) are individual websites that form the new social media landscape*".

The advent of social media has meant the issues with technology mediated communication have become more common, prolific and also impact sections of society that once were not affected. The largest group is now teenagers and school aged children. Whilst cyber bullying is not limited to this demographic it appears to have a more profound and severe measurable effect on this group. Due to this, a large amount of research has been conducted researching the reasons and solutions to the issue, however many of this research has theorised the reasons and not explored the specific demographics motivations behind this online bullying behaviour.

The paper will highlight a number of cases where new technologies in particular SMS are being used to undertake bullying activities.

CYBER BULLYING AND ANTI- SOCIAL BEHAVIOUR

In recent years there has been extensive research conducted in the sphere of bullying via electronic means, often termed cyber-bullying. Previously work undertaken in this arena was mainly in workplaces that used technology mediated communication means for group work, team and skill building. This paper will look at cyber-bullying in adolescent cases and online anti-social behaviour.

What constitutes bullying as opposed to everyday conflicts that often occur in children and teenagers, is that bullying is defined as "*repeatedly and over time*, to *negative actions* on the part of one or more other students *who are or perceived to be stronger*" (Olweus, 1993). It is also highlighted by the motivation that there is a genuine intent to cause harm and that the abuse is consistently repeated over a period of time, rather than an on-off conflict or argument (Whitney & Smith, 1993; Olweus, 1999).

The traditional view of bullying in the school yard such as name calling, other verbal abuse, physical assault or humiliation has now expanded into cyber bullying. Cyber bullying can take many forms and can refer to the use of emails, mobile communication messaging, website postings, blogging, and the misuse of pictures as a way to spread rumours, humiliate , isolate, embarrass of frighten those being victimised (Smith et al, 2006; Willard 2005).

Those engaging in bullying who are pre-pubescent tend to engage in direct bullying behaviours whilst those who are in their teenage years move more towards cyber bulling. Female bullies tend to use less direct strategies than their male counterparts (Wolke, 2010). Unlike traditional bullying, cyber-bullying

is not only perpetuated by individuals against another individual. It is become more prominent for groups to become the attacker, perhaps due to the anonymity of the Internet and the fact that this anonymity can lead to individuals forming a group with a pack mentality. A United Kingdom study in 2008 reported that up to 10% of students had been cyber-bullied (Smith et al, 2008) whilst a Canadian study undertaken in 2009 reported a rate of 35% (Cassidy et al, 2009). A predominant conclusion in much research (references) is that rather than the need for school policies to eradicate bullying, that the only way that bullying will be extinguished is to "teach" young people in the home as to the unacceptable nature of bullying type behaviour. This raises an even more important aspect in the issue of cyber bullying. Even in a more technologically savvy world many parents are unaware of their children's actions and behaviours online and many are not even aware of how the social media and other technologies work and therefore do not monitor closely what is occurring. It is easy for a parent to chastise bullying behaviour between siblings or friends when it occurs in the home but less easy to control and monitor such interactions and behaviours when they take place through technological means.

Another element of anti-social behaviour is that of vigilantism, whilst the perpetrators believe they are in the "right" and are defending others they are often engaging in the same behaviours as cyber bullies by defacing and attacking individual's social media pages and engaging in patterns of harassment (Wehmhoener, 2010).

The paper will explore a number of recent case studies and highlight the issues related to them.

CASE STUDY 1: THE JESSI SLAUGHTER INCIDENT

Based upon news reports (ABC 2010a, ABC 2010b, CBS, 2010 Farquhar, 2010). Jessi Slaughter was a pseudonym (real name Jessica Leonhardt) for an 11 year old girl (leaving in the USA) who rose to prominence in the media through dramatic events that unfolded through her use of social media services. The situation began with postings on a website called StickyDrama (which can be described as a blogging and rumour and gossip site contributed to by teenagers). The postings accused Jessi of being involved with a member of a band, which she denied. She reacted to this by posting videos and content of herself and attacking the people she thought had defamed her. The situation escalated when individuals gained personal information including home phone numbers and twitter account details about her and post this information on various other sites. She was a victim of prank calls at home and she received numerous hate emails, in spite of this, Jessi continued to taunt the trollers by blogging and commenting on the situation (Mathieu, 2011). In a final act, the young girl created a video which was subsequently posted on YouTube, in which she delivered a tearful and angry rant to those perpetuating the acts, at one point her father is present in the video and delivers his own angry message to the trollers (see figure 1). This video brought global attention to Jessi and the issue of cyber bullying and received over 785,000 views.

An important aspect of the case study was that information related to Jessi was posted on 4Chan. 4Chan is a simple image-based bulletin board where anyone can post comments and share images and is governed by a site set of rules than including "flaming" (4Chan, 2012). What happened was that Jessi story appeared on the message boards of 4chan, the *threats against Jessi started coming fast and furious* (ABC, 2010a), this enflamed the situation even further.
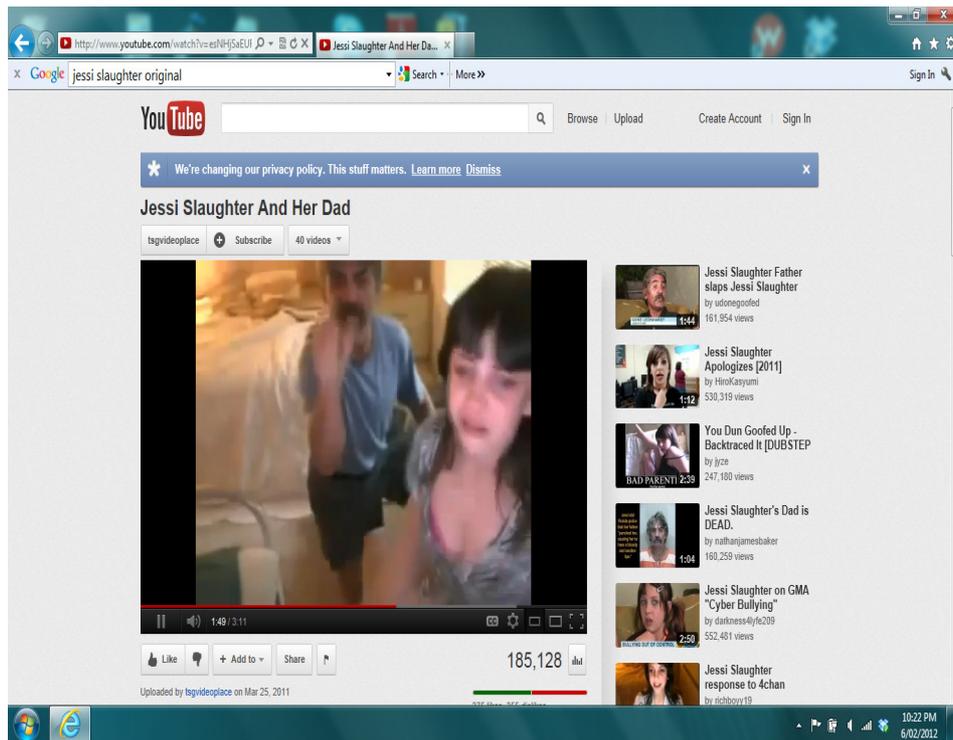
Figure1: *Jessi Slaughter and her Father on YouTube.*

A sad aftermath of the situation was that the people made fun of Jessi by making parody videos of her (including song remix's and comedy sketches) and posting them on YouTube, the most popular of these videos receiving over 900,000 views on YouTube.

ETHICAL CONSIDERATIONS

In light of this a number of ethical issues are clearly apparent. These are numerous and can be viewed from the perspective of either the parties involved in the above case. In regards to Jessi Slaughter, a major issue was the ability and desire of an 11 year old to post inappropriate material on social media sites. Another concern was the sub-optimal parental control and the lack of awareness as to her activities online.

In this case another factor was the action of the 4Chan site. Of issue, was the systematic attack on an 11 year old (legally a child) by anonymous posters. The use of social media services to escalate an issue rather than reporting the inappropriate material to legal authorities. The issue that posts on 4Chan breached their own behaviour rules, but they were unable to police themselves and remove or stop posts.

All of these ethical issues do not indicate the responsibility and control that social media services have over the content and behaviour of those using their services. In recent years social media services have taken active steps in order to control these issues but these have not decreased dramatically the number of cyber bullying cases or the severity of these cases. The governance of these services is clearly lacking.

CASE STUDY 2: THE IMPACT OF PUBLIC OPINION – AN AUSTRALIAN CASE

In Australia, the murder of Trinity Bates in Queensland in February 2010 saw a flurry of Internet and especially Facebook pages being set up. Some were tribute sites to mourn the loss of a child, others were hate sites set up by web vigilantes against the man accused of the murder. The Queensland Premier sent an open letter to Facebook's CEO asking "what it will do to block the 'sickening' hijacking of Internet memorials?" (Herald Sun, 2010). Whilst the Queensland Premier was concerned mainly about the users posting Internet pornography and other inappropriate material on the memorial sites, of as much concern is the ethical issue surrounding the use of Facebook to vilify and pre-judge the accused defendant. The man charged with the murder has been named in the mainstream press but

the vigilantes went further, posting much more personal information such as addresses and information about the defendant's family members. Facebook answered the letter by releasing a statement from its US based director of communications and public policy. Defending Facebook's monitoring systems, the response stated that users could draw attention to offensive content by clicking on a "report" button beneath any post on the SNS. This answer has done little to placate people who feel their grief has been compounded by the actions of a few, however they fail to understand or to realise the lack of control and limited monitoring that takes place on many SNSs (The Australian, 2010a).

The comments on the vigilante sites may have major consequences for legal trials and could lead to them being aborted. This could mean that jury selection could be put at risk because the process of innocence until proven guilty could be compromised. In terms of the Trinity Bates example, how could someone have a fair trial in Queensland, when public opinion has already found a person guilty?" (The Australian, 2010b). It appears that governments are struggling to deal with new media and are playing catch-up with methods of dealing with the issue. This incident has clearly highlighted, not simply the lack of security and monitoring on SNSs but the ethical issues surrounding the free speech on which such sites are based. The fact that such software could severely impact our judicial system, a fundamental core of society, means that this is an issue of great importance to all societies. Facebook currently has a low user to staff ratio with only 1000 staff across the world, therefore there are simply not enough resources to manage all the information that has been uploaded and posted in real time (The Australian, 2010b).

The solution to this situation is complicated. One option may be to employ more staff and put structures and boundaries in place to clearly define what is considered an acceptable Facebook group. In doing this, however, we are then fundamentally changing the core of Facebook and allowing a third party (government or public opinion) to decide what is or is not acceptable to society (Leitch and Warren, 2011). A more successful long term strategy would be to improve education and self-regulation of such sites but success is dependent upon the reliance of most people to act in a responsible manner and set their own rules and boundaries. As a result of the Trinity Bates case, the Australian Federal Government has announced that they will create an online ombudsman to deal with concerns regarding SNSs and inappropriate content (The Australian, 2010c).

ETHICAL CONSIDERATIONS

The sheer number of people using social-networking sites makes it difficult to monitor misuse, both for law-enforcement officials and site administrators. Tim Sparapani (Facebook's Director of Public Policy) estimates that Facebook users spend 18 billion minutes on the site each day. "We have 400 million active users and a tiny, tiny staff. We need to find novel ways to handle that kind of crushing amount of activity. It's the burden of being so immensely popular," (Time, 2010).

Some victims' advocates believe that as well as offenders losing civil liberties when they are found guilty of a crime they should also lose their "cyberliberties" (Time, 2010). Each social media service is dealing with these issues in different ways and governments are strategising to put into place policy and law to minimise the risks.

Facebook currently bans people who have been convicted of sexually based offences but has no specific policy for those convicted of other sorts of crimes; "policing" of this policy is not surprisingly difficult and therefore a number of countries and states have been required to bring about their own legislation. The US state of Illinois, has made it illegal for sex offenders to use social networks, and if found doing so can be charged with a felony offence. In the UK, however plans to do something similar have been thwarted as it was believed plans breach human rights law (Skinner, 2009). The issue arose when it was revealed that the police would be asked to share sex offenders' details and email addresses with social network administrators. These types of policies do not deal with the "average" cyber-bully who may not have a criminal record. In the same way identifying and prosecuting traditional bullying behaviour in schools and workplaces is challenging when we add in the electronic means of delivery, the 500 million users of social media services, along with the veil of anonymity and the "right to free speech, the expectation that cyber-bullying can be reduced in the near future is unlikely.

It is further demoralising that the US Federal Communications Decency Act clearly states that, "web sites aren't responsible for harassment by users" (Davis, 2009) and therefore cannot be held legally liable. This fact does little to calm the users who are becoming increasingly frustrated with the lack of concern regarding personal privacy, security from abuse and bullying.

CONCLUSION

The impact of social media and the Internet has brought great benefits to society. The problem is as well as the benefits it has brought issues as well, many of these issues mirror the physical world in particular the issue of cyber-bullying or the smearing of good causes. The paper has highlighted the weakness of social media providers to protect against these issues; this weakness could be due to limited governance models or the ability of SMS providers to react in real time to incidents.

REFERENCES

4Chan (2012). Rules, http://www.4chan.org/rules [Accessed 3/1/12]

ABC (American Broadcasting Company) (2010a). 'Jessi Slaughter' Says Death Threats Won't Stop Her From Posting Videos on the Internet, http://abcnews.go.com/GMA/Technology/jessi-slaughter-viral-tweens-violent-online-rant-spurs/story?id=11224731 [Accessed 1/12/11].

ABC (American Broadcasting Company) (2010b). Do Kids Need More Privacy Protection on Social Networks? http://abcnews.go.com/WN/social-networking-privacy-kids-protected-online-world-news/story?id=11831552 [Accessed 1/12/11].

Cassidy, W., Jackson, M., & Brown, K.N. (2009). Sticks and stones can break my bones but how can pixels hurt me? Students' experiences with cyberbullying. School Psychology International, 30, 383-404.

CBS (2010) 'Jessi Slaughter' YouTube Cyberbully Case: 11-Year-Old Tells GMA She Didn't Want it to Go This Far, http://www.cbsnews.com/8301-504083_162-20011349-504083.html [Accessed 1/12/11].

Davis, W. (2009). Facebook Harassment Suit Could Spur Cyberbullying Laws. The Daily Online Examiner. http://www.mediapost.com/publications/index.cfm?fa=Articles.showArticle&art_aid=114854 [Accessed 1/12/11].

Farquhar, P. (2010). Jessi Slaughter and the 4chan trolls - the case for censoring the internet. http://www.news.com.au/technology/jessi-slaughter-and-the-4chan-trolls-the-case-for-censoring-the-internet/story-e6frfro0-1225894369199#ixzz1lHbLxHqO. [Accessed 1/12/11].

Herald Sun. (2010). Governments powerless to stop Facebook vandalism, says IT expert. from http://www.heraldsun.com.au/.../governments-powerless-to-stop-facebook-vandalism-says-itexpert/story-e6frf7jx-1225834291255 [Accessed 1/12/11].

Leitch, S. and Warren, M. (2011) The ethics of security of personal information upon Facebook, in Quigley, Marian (eds), ICT ethics and security in the 21st century : new developments and applications, pp. 46-65, IGI Global, Information Science Reference, Hershey, Pa.

Mathieu, S. E. (2011). Misogyny on the web: Comparing negative reader comments made to men and women who publish political commentary online. Thesis: Master of Arts. University of Missouri-Columbia.

Mishna, F., Khoury-Kassabri, M., Gadalla, T. And Daciuk, J. (2011).Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims. Children and Youth Services Review. Volume 34, Issue 1, January 2012, Pages 63–70.

Olweus, D. (1999). Sweden. In P. K. Smith, Y. Morita, J. Junger-Tas, D. Olweus, R. Catalano & P. Slee (Eds.), The nature of school bullying: A cross-national perspective (pp. 7–27). London: Routledge.

Olweus, D. Bullying in schools: what we know and what we can do. Oxford: Blackwell Publishers, 1993

Seendahera, V. Warren, M. and Leitch, S. (2011). A Study into how Australian Banks use Social Media. PACIS '11, Brisbane, Australia.

Smith, P.K., Mahdavi, J., Carvalho, M., & Tippett, N. (2006). An investigation into cyberbullying and its forms, awareness and impact and the relationship between age and gender in cyberbullying. University of London. http://www.antibullyingalliance.org.uk/downloads/pdf/cyberbullyingreportfinal230106.pdf [Accessed 1/12/11].

Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, 49, 376-385.

The Australian. (2010a). Bligh hits out at sick net sites. http://www.theaustralian.com.au/politics/state-politics/bligh-hits-out-at-sick-net-sites/story-e6frgczx-1225834063831[Accessed 1/12/11].

The Australian. (2010b). Facebook vandal complaints futile. http://www.theaustralian.com.au/australian-it/facebook-vandal-complaints-futile/story-e6frgakx-1225834303404, [Accessed 1/12/11].

The Australian. (2010c). Online ombudsman for Facebook woes. http://www.theaustralian.com.au/australian-it/online-ombudsman-for-facebook-woes/story-e6frgakx-1225834756343, [Accessed 1/12/11].

Time Magazine, (2010), How Prisoners Harass Their Victims Using Facebook, http://www.time.com/time/business/article/0,8599,1964916,00.html#ixzz0gb2oD8Ge, [Accessed 1/12/11].

Wehmhoener, K. (2010). Social norm or social harm: An exploratory study of Internet vigilantism. Iowa state university.

Whitney, I. & Smith, P. K. (1993). A survey of the nature and extent of bullying in junior/middle and secondary schools. Educational Research, 35, 3–25.

Willard, N. (2005). Educators guide to cyber-bullying and cyber threats, Centre for Safe and Responsible Internet Use, http://www.csriuorg/cyberbully/docs/cbcteducator.pdf [Accessed 1/12/11].

Wilton, C. and Campbell, M. A. (2011). An exploration of the reasons why adolescents engage in traditional and cyber bullying. Journal of Educational Sciences & Psychology, 1(2), pp. 101-109.

Wolke, D. (2010). Bullying: Facts and Processes. Worcester Medicine, Vol.74 (No.4). pp. 13-15.

After Things Go Wrong

R Lucas[1]

[1] Discipline of Information Systems, University of Canberra, Australia,
E-mail: Richard.Lucas @canberra.edu.au

ABSTRACT: *This paper outlines the standard approaches to computer ethics, describes what I think is missing, and provides an analysis of restoration process. In brief I claim that a missing piece from the ethics puzzle is what to do after a moral wrong has been committed, after the ethical dimensions of a relationship have been torn asunder. I provide some examples from typical occupational categories to show how a reparation process might work.*

Keywords: Moral Repair, Ethics, trust, hope.

INTRODUCTION

Standard texts on computer ethics do a great service in bringing ethics to the masses. They do a great job in highlighting the importance of analysing the nature and social impact of computer technology (Moor, 1985). They "extend ordinary moral principles to situations created by computer technology" (Johnson, 1998).   They analyse the problems (usually social ones), bring standard ethical theories into play, and suggest what should have been done. Some provide guidance on how to avoid ethical problems. Some include codes of ethics from their local professional society (ACS for Australia, ACM for the US, BCS for the UK, IFIP internationally). Some worry about the future (i.e. Nanotechnology). However, for all the good work they do they do not address the issue of what the ICT professional might do in their professional work relationships after an ethical wrong has been committed. How do you go on working with someone you have harmed? How do you forgive someone who has not done their professional duty?

This does of course presume that there is something to be done, that ICT professionals want to have a healthy ethical working environment. In a recent study (Lucas & Weckert, 2008) John Weckert and I undertook we established that ICT professionals in Australia identified ethical wrongs in the workplace from the beginning of their entry into the workplace. It mattered not the length of time spent in ICT work, some had been in the workforce as little as six months, all respondents to our survey identified frequent acts that they considered to be unethical. Acts that they feel must be addressed, must be resolved. It is this felt need for resolution that occupies the remainder of this paper.

THE INITIAL REACTION

It is usually the case that after an ethical wrong has been committed the people involved, and their working relationships, go on. That is most of the time, except when one or more people have been removed from the workplace the ICT professional continues to work with the affected individuals. If I have harmed someone (or been harmed by someone), I, usually, will continue to see them, interact with them, and be responsible for, or to, them: Have some professional relationship with them. As everyone knows, this is a difficult and strained time.

A MISSING PIECE

What is an ICT professional to do?

I propose here that there are several things that need to be paid attention to in order to make the best of the situation and, perhaps, somewhat restore the moral environment in the workplace[4].

Walker (2006, p.28) gives six tasks that need to be addressed. However, Walker, in my estimation, overstates the capabilities of the ICT professional and I have added a precondition; recognition.

I take the structure of the tasks I describe here from Walker, 2006, Moral Repair and acknowledge a considerable debt to her subtle and nuanced treatment of this difficult topic 4

1. recognizing the problem;
2. placing responsibility;
3. addressing the wrong;
4. stating ethical notions and standards;
5. re-establishing trust;
6. nourishing hope;
7. creating a new moral relationship.

RECOGNIZING THE PROBLEM

When an ethical wrong has occurred it is critical that its occurrence be recognized. To those who are sensitive to ethical matters this might seem obvious, but if no one admits that an unethical act has occurred then there is no hope of a satisfactory resolution to a dislocating situation. If the harmed person does not recognize that they have been wronged then there seems to be little that can be done until they become aware.

Given the problematic nature of the unrecognised, by the wronged, harm I will now turn to the problem of the wrongdoer. Fundamental to the next task of moral reclamation is that the wrongdoer recognize their part in the ethical problem. Without recognition by a wrongdoer that a wrong has occurred the next task cannot be done. It is not my purpose here to examine the complexities of moral competence but rather to outline the steps that need to be followed.

Placing Responsibility

Once the wrong has been recognized by at least two people it must be correctly placed. Those who have caused the harm must be identified with the wrong. This may be a difficult process as those who have wronged may seek to evade being identified. Sometimes the wrong is a general harm with no easily identifiable culprit. Placing responsibility can be difficult in circumstances where the wrong is buried within a long and obscure procedure: sometimes it is just the system; nobody is to blame. This refrain is commonly heard coming from those who fear they (rightly or wrongly) will be blamed.

Addressing the Wrong

Addressing the wrong means that those who have caused harm must acknowledge that they have wronged. If they do not (they might genuinely believe that no harm has happened or they might simply be trying to evade responsibility. See the previous section.) then the work community that surrounds the wronged must step up; they must make it clear to the wronged that they acknowledge that the wrong has occurred and who is to blame.

STATING ETHICAL NOTIONS AND STANDARDS

The next task is for the community (or at least some significant others) to say why, exactly, the wrong is wrong. They must state the ethical norms and standards of the work community. Frequently they will be found lacking. In the survey I quoted above about 10% of the survey respondents were personally interviewed. In these it was common that the interviewee could not state the ethical norms of their workplace; it was common that the interviewee could not find the code of ethics for either the workplace or their professional body.

Where ethical standards exist, those in positions of authority in the workplace must make it clear that those standards still apply; still have force. If in the process of searching for the ethical ideals of the workplace none are found then they must be established. In saying this I do not trivialize the process of establishing and ethical environment, rather it is a significant and difficult undertaking that is beyond the scope of this paper. Equally it ought to be clear that simply having a Code of Ethics is insufficient (Bayerstein, 1993); simply pointing to the code and saying 'follow this' is not enough.

REESTABLISHING TRUST

One of the most significant consequences of a wrong is the loss of trust. It is well understood that trust is the oil that lubricates the wheels of any well-adjusted workplace. A wrong rocks the beliefs of the wronged, beliefs that this workmate can be relied upon. And not only with this workmate, trust is reduced in all relationships and in the workplace in general. Sometimes the loss of trust extends beyond merely the wronged and the wrongdoer. Frequently those with only a passing acquaintance with the wrongdoing also experience a loss of trust. A loss of trust in the wrongdoer and, sometimes, in the authority of those in charge. Finally, how can one wronged maintain a belief in the goodness of the workplace environment when, clearly, at least one workmate cannot be trusted?

One of the best ways of reestablishing trust is through the visible and active involvement by those in authority acknowledging that, yes, a violation has occurred, that it is not ok, and that something will be done to ensure that it will not happen again. Of course if it does happen again then trust is further eroded, sometimes irretrievably. The permanent loss of trust means that no moral environment is possible.

NOURISHING HOPE

While trust may be damaged by a wrong committed in the workplace it may be restored while there is hope. For the workplace to be effective and productive there must be a belief that the future will be better, ethically, than the past. Some of the features of there being no hope in a more ethical future are low productivity, increased absences, and high staff turn-over.

CREATING A NEW MORAL RELATIONSHIP

Finally to give hope and trust meaningful expression visible steps must be taken to create a new moral relationship. Between the wronged and the wrongdoer. If this is not possible then the least that must be done is to reinforce the moral relationship between the wronged and their immediate workmates, their working community. The second case while not the best solution will provide the wronged and their community with a basis for greater hope and greater trust. However, for this to take place two acts must be undertaken; forgiveness and making amends.

In the case of the wrongdoer and the wronged re-establishing a meaningful ethically based relationship the wronged needs to forgive the wrongdoer. This may not be desirable or possible though. Where the wronged cannot forgive there is little chance of any hope and even less likelihood of their being a trusting relationship.

SO WHAT?

So what has all this got to do with the ICT professional?

All of what I have said above is applicable to any workplace so what is so special in the workplace for the ICT professional? Nothing and everything. Nothing but recognition that ICT workers are in the same boat as all other workers. Nothing but the recognition that ICT professionals are no different, nothing special when it comes to workplace ethics.

Everything. Because ICT workers have special knowledge and special skills in the acquisition, analysis, and dissemination of information. This is important because information is the bedrock of hope, trust, and engaging in any sort of relationship, especially a moral relationship. People, mostly, need reasons for hope - reasons that are embedded in information. Trust absolutely depends upon quality of information; information about peoples acts and reasons for those acts.

SUMMARY

Up until now scant attention has been paid, in the (ICT ethics) literature, to the aftermath of moral transgressions. What little has been said is focussed on punishing the wrongdoer in an effort to show strength by the profession. When an ethical breach is reported to an ethics committee there is an ethics

committee meeting to determine the facts (after all that is what ICT professionals are good at). Usually these are held in secret, ostensibly to protect the privacy of the wrongdoer. If, and this is unusual, wrongdoing has been confirmed then some sort of sanction is placed on the ICT professional and that is the end of the story. Everyone is expected to just get on with it; business as usual. However it cannot be as usual. Even this, little as it is, is ineffective (Gotterbarn, 2009). So what is the ICT professional to make of all of this?

I have outlined some tasks from Walker (2006) that are necessary, for the ICT professional and their workplace, if the moral climate is to achieve some degree of goodness following an ethical wrongdoing. By examining what is currently done when things go wrong against these tasks it is relatively easy to see why little changes in the moral climate in ICT workplaces.

The first thing the ICT professional will notice is that of the seven tasks outline above only the first three, and the third only partially, are addressed. The steps that are active in doing something about the moral climate (tasks four through seven) in the workplace are simply missing.

It is clear that the policies and procedures that ICT professionals use in their everyday work need to include all the tasks in the process of engaging in moral repair. It is better to be prepared if something goes wrong ethically. Ethical fixing needs to be part of everyone's training.

REFERENCES

Beyerstein, D. (1993). Function and Limitations of Professional Codes of Ethics, in. Applied ethics: a reader, E. Winkler (ed.), pp. 417-425.
British Computer Society. (2006). Report on the Study of Established Professions to Validate the IT Professionalism Model.
Gotterbarn, D. (2009). ICT Governance and What to Do About the Toothless Tiger(s): Professional Organizations and Codes of Ethics, Australasian Journal of Information Systems, Vol. 16, Issue 1, pp.165-184.
Hamington, S. J. (1994). The impact of codes of ethics on information systems personnel. Proceedings of the 1994 computer personnel research conference on Reinventing IS: managing information technology in changing organizations: managing information technology in changing organizations, pp. 199-207, Retrieved from http://portal.acm.org/citation.cfm?id=186323.
Lucas, R. (2006). Ethics: Why do we differ? Information Age, August/September, pp.28-29.
Lucas, R. and Weckert, J. (2008). Ethics and Regulation in the ICT Industry, Technical Report, ARC Linkage Grant: LP0560659.
Reed, D. C. (2008). A model of moral stages, Journal of Moral Education, 37(3), 357-376. doi:10.1080/03057240802227759.
Walker, M. (2006). Moral Repair, Cambridge University Press, ISBN: 9780521810883.