Conference Proceedings of

A*i*CE 2013

Melbourne, 3rd December. 2013.

Seventh AUSTRALIAN INSTITUTE OF COMPUTER ETHICS CONFERENCE

Edited by:
Matthew Warren
ISBN 978-9872298-3-0.

Proceedings of

A*i*CE 2013

Edited by
Matthew Warren
ISBN 978-9872298-3-0.

Organised By
Information Governance and Security Research Group, School of Information and Business Analytics, Faculty of Business and Law, Deakin University.

Published by the School of Information and Business Analytics, Deakin University, Burwood, Victoria, 3125, Australia.

Welcome

The AiCE 2013 conference follows on from the highly successful initial AICE 99 conference and the AiCE 2000, AiCE 2002, AiCE 2005, AiCE 2008 and AiCE 2012 conferences. This conference looks at the continued development of Computer Ethics within Australia, taking into Ethics and Governance issues of new emerging technologies.

Papers were selected for their relevance in relation to the Computer Ethics and the conference theme. 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 2013 Organising Committee

Yeslam Al-Saggaf, Charles Sturt University.
Oliver Burmeister, Charles Sturt University.
Richard Lucas, University of Canberra.
Craig McDonald, University of Canberra.
Kirsten Wahlstrom, University of South Australia.
Matthew Warren, Deakin University. (Conference Chair).

Contents

Privacy and Brain-Computer Interfaces: clarifying the risks

Kirsten Wahlstrom[1,2], N Ben Fairweather[2,3], Howell Istance[3], Helen Ashman[1]

[1]School of Information Technology and Mathematical Sciences
University of South Australia
Adelaide, Australia
Email: kirsten.wahlstrom@unisa.edu.au

[2]Centre for Computing and Social Responsibility
DeMontfort University
Leicester, UK

[3]Faculty of Technology
DeMontfort University
Leicester, UK

Keywords

Privacy, Brain-Computer Interfaces

INTRODUCTION

This paper presents the core hypothesis of an ongoing doctoral research project aiming to identify privacy disruptions arising from Brain-Computer Interfaces (BCIS). The outcomes of this ongoing research project can be applied in several ways. For example, future BCIs may be designed or adapted in order to support privacy; policy direction may be informed; and so on.

The privacy disruptions identified in this paper will be explored, and possibly extended, in a forthcoming experiment with four phases. In the first phase, a questionnaire will screen participants into small groups so that, in each group, a range of privacy attitudes is present. In the second phase, each group will engage in a Habermasian communicative action (Habermas 1985 cited in Finlayson 2005; Horster 1992; Klein and Huynh 2004; Thomassen 2010) in order to overtly establish a privacy norm. In the third phase, individual participants will use a BCI and will participate in an interview aiming to expose and extend the potential privacy disruptions identified here. In the fourth phase, the small groups will re-convene and, in the light of their experience with the BCI, will re-examine and perhaps amend the previously established privacy norm.

In order to confirm or refute the project's core hypothesis, an analysis informed by Nissenbaum's contextual framework (Nissenbaum 2004; 2009) will be conducted over the data arising from the questionnaires, the small group discussions and the individual interviews.

BRAIN-COMPUTER INTERFACES

BCIs acquire, interpret and apply neural activity so that external devices can be controlled. Devices that interpret movement, such as the Wii, are not BCIs.

Vidal's early work (1973; 1977) stimulated interest in the field and focused on translating neural responses elicited with a stimulus. Vidal had a view to elevating "... the computer to a genuine prosthetic extension of the brain" (Vidal 1973, p 158). While this vision remains largely unfulfilled (Berger et al. 2007), there have been advances in the interim.

BCIs are rapidly approaching commercial viability (Brunner et al. 2011). Examples based on electroencephalographic (EEG) readings of human neural activity are on the market (Emotiv Systems ; IntendiX) and have been applied to the control of external technologies and devices (Hochberg et al. 2006), largely with a view to supporting the autonomy of people with disabilities (Berger et al. 2007) although online gaming has been emerging as an application area (Lotte 2011).

With a view to enabling identification of potential privacy disruptions, this paper presents a typology of BCI technologies that organises the field according to the way in which neural signals are acquired and interpreted.

TYPOLOGY

The typology organises BCIs into four main types.

- An *active BCI* acquires and interprets neural activity elicited when a user voluntarily and intentionally engages in a pre-defined task (Zander et al. 2010).

- *Reactive BCIs* elicit recognition responses from users (Zander et al. 2010). For example, in Gerson et al. (2006) users familiarized with a specific image observed many images in rapid succession on a computer screen. When the familiar image was recognized, their neural activity exhibited a reliably identifiable feature called an Event-Related Potential, in this case a visually-evoked potential.

- *Passive BCIs* acquire, interpret and apply neural signals from spontaneous, non-evoked neural activity generated as the user performs a complex real-world task. Furthermore, the interpretation of neural activity correlating to higher order cognitive and affective states (eg confusion and fatigue) has been identified as a research priority (Nijholt et al. 2008).

- *Hybrid BCIs* combine a BCI with some other technology (perhaps another BCI) to improve system performance via a richer set of data (Pfurtscheller et al. 2010).

POTENTIAL PRIVACY DISRUPTIONS

Westin's (1970) early theory of privacy as control over information is contrasted by Gavison's (1980) theory of restricted access to information. In addition, economic models of personal information as private property emerged (Schwartz 2004), along with the contextual framework for information privacy analysis (Nissenbaum 2009) and the ontological theory of information privacy (Floridi 2005).

In order to identify potential privacy disruptions, each privacy theory frames a discussion of BCIs.

Control theory

The control theory defines privacy as the ability for an individual to control when, how and to what extent their personal information is communicated with others.

Active Where users are obliged to use BCI technology (for example, people with disabilities) circumstances may necessitate control of privacy. Otherwise, users are knowingly and deliberatively engaged in specific tasks designed for controlling the BCI and thus active BCIs do not appear to disrupt privacy.

Reactive While users are not engaged in deliberative tasks, they are knowingly engaged in using a reactive BCI. Also, the design focus on ERP signals means that other neural activity is filtered out.[1] Therefore, there is no potential for privacy disruption.

Passive Users do not control the BCI and may become unaware of it. Therefore, genuine informed consent is required if privacy is not to be disrupted.

Hybrid Where users do not directly control a hybrid BCI, they may become unaware of it and if so, genuine informed consent is required if privacy is not to be disrupted.

Restricted access theory

The restricted access theory suggests that technologies make direct control over personal information increasingly difficult to achieve. Therefore, a requirement for regulatory frameworks can be identified.

If the data acquired by BCIs is protected under regulatory frameworks, privacy will not be disrupted. This applies to all four types of BCI.

Also, as the restricted access theory does not exclude the possibility of a user exerting control should the opportunity be present; where this occurs, the potential privacy disruptions identified for the control theory will be relevant.

Data privacy as a commodity

Theories of privacy as a commodity seek to establish markets in which personal data can be traded. Under commodification theories, if data is excluded from such markets, privacy is disrupted.

[1] An exception exists for users coerced into using a reactive BCI (for example, when under interrogation). In such a context, the user may be at risk of generating a P300 ERP in response to a stimulus they would prefer to not have recognized.

With respect to BCIs, the ownership of the data acquired and interpreted by a BCI is a relevant and open question. Should a third party retain a copy of BCI data without having purchased it, privacy will be disrupted. This potential privacy disruption applies to all four types of BCI, including any non-BCI component of a hybrid BCI.

The contextual framework

The contextual framework supports the assessment of new technologies with respect to privacy: if an information flow disrupts the normatively established integrity of a context, privacy is likely to be disrupted.

Active As above, where users are obliged to use an active BCI, circumstances may necessitate control of privacy. Otherwise, users are knowingly and deliberatively engaged in specific tasks designed for controlling the BCI. As users are knowingly engaged, they are empowered to stop at any time. As this is consistent with the opt-out privacy norm, active BCIs do not appear to disrupt privacy.

Reactive Users are knowingly, but not deliberatively, engaged in controlling a BCI. As for active BCIs, users are knowingly engaged and empowered to opt-out. Therefore, reactive BCIs do not appear to have potential for disrupting privacy.

Passive Users are engaged in complex tasks that are not related to controlling a BCI; instead they are knowingly and deliberatively engaged in task completion. If the privacy norms relevant to task contexts do not persist, privacy will have been disrupted.

Hybrid Users may be engaged in tasks from either active, reactive or passive BCIs. Any privacy disruptions arising from either active or reactive BCIs can be mitigated by genuine fully-informed prior consent. Also, if a hybrid BCI has a passive BCI component, there is potential for the privacy disruptions noted immediately above. Furthermore, in hybrid BCIs, data from a second system component is acquired in order to robustly support interpretation. Therefore, the extent to which the second component disrupts privacy is relevant.

The ontological theory

Under the ontological theory, data is constitutive and technologies are inherently neutral, but can either increase or decrease the traction of the infosphere, which increases or decreases privacy accordingly.

As BCIs upload a new form of data to the infosphere, they decrease the traction of the infosphere and therefore they decrease privacy. Furthermore, under passive or hybrid BCIs, it may be that neural data is more highly constitutive than descriptive data, in which case disruptions to privacy will be of greater significance.

REFERENCES

Berger, T., Chapin, J., Gerhardt, G., McFarland, D., Principe, J., Soussou, W., Taylor, D., and Tresco, P. 2007. "International Assessment of Research and Development in Brain-Computer Interfaces."

Brunner, P., Bianchi, L., Guger, C., Cincotti, F., and Schalk, G. 2011. "Current Trends in Hardware and Software for Brain-Computer Interfaces (BCIs)," *Journal of Neural Engineering* (8:2).

Emotiv Systems. "Emotiv: You Think, Therefore, You Can." Online, http://emotiv.com/ visited September 17 2012.

Finlayson, J. 2005. *Habermas: A Very Short Introduction*. Oxford University Press.

Floridi, L. 2005. "The Ontological Interpretation of Informational Privacy," *Ethics and Information Technology* (7:4), pp 185-200.

Gavison, R. 1980. "Privacy and the Limits of Law," *The Yale Law Journal* (89:3), pp 421-471.

Gerson, A.D., Parra, L.C., and Sajda, P. 2006. "Cortically Coupled Computer Vision for Rapid Image Search," *Neural Systems and Rehabilitation Engineering, IEEE Transactions on [see also IEEE Trans. on Rehabilitation Engineering]* (14:2), pp 174-179.

Habermas, J. 1985. *The Theory of Communicative Action, Volume 2: Lifeworld and System: A Critique of Functionalist Reason*. Beacon Press.

Hochberg, L., Serruya, M., Friehs, G., Mukand, J., Saleh, M., Caplan, A., Branner, A., Chen, D., Penn, R., and Donoghue, J. 2006. "Neuronal Ensemble Control of Prosthetic Devices by a Human with Tetraplegia," *Nature* (442:7099), pp 164-171.

Horster, D. 1992. *Habermas: An Introduction*. Pennbridge.

IntendiX. "Personal EEG-Based Spelling System." Online, http://www.intendix.com/ visited October 8 2012.

Klein, H.K., and Huynh, M.Q. 2004. "The Critical Social Theory of Jürgen Habermas and Its Implications for Is Research," in: *Social Theory and Philosophy for Information Systems*, J. Mingers and L. Willcocks (eds.). Chichester: Wiley.

Lotte, F. 2011. "Brain-Computer Interfaces for 3d Games: Hype or Hope?," *Foundations of Digital Games (FDG'2011)*.

Nijholt, A., Tan, D., Pfurtscheller, G., Brunner, C., del R. Millán, J., Allison, B., Graimann, B., Popescu, F., Blankertz, B., and Müller, K.-R. 2008. "Brain-Computer Interfacing for Intelligent Systems," *Intelligent Systems, IEEE* (23:3), //, pp 72-79.

Nissenbaum, H. 2004. "Privacy as Contextual Integrity," *Washington Law Review* (79:1), pp 119-157.

Nissenbaum, H. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books.

Pfurtscheller, G., Allison, B.Z., Brunner, C., Bauernfeind, G., Solis-Escalante, T., Scherer, R., Zander, T.O., Mueller-Putz, G., Neuper, C., and Birbaumer, N. 2010. "The Hybrid BCI," *Frontiers in neuroscience* (4).

Schwartz, P. 2004. "Property, Privacy, and Personal Data," *Harvard Law Review* (117:7), pp 2056-2128.

Thomassen, L. 2010. *Habermas: A Guide for the Perplexed*. London ;New York: Continuum.

Vidal, J.J. 1973. "Toward Direct Brain-Computer Communication," *Annual Review of Biophysics and Bioengineering* (2:1), pp 157-180.

Vidal, J.J. 1977. "Real-Time Detection of Brain Events in EEG," *Proceedings of the IEEE* (65:5), pp 633-641.

Westin, A. 1970. *Privacy and Freedom*. Bodley Head.

Zander, T., Kothe, C., Jatzev, S., and Gaertner, M. 2010. "Enhancing Human-Computer Interaction with Input from Active and Passive Brain-Computer Interfaces," in: *Brain-Computer Interfaces*, D. Tan and A. Nijholt (eds.). Springer London, pp. 181-199.

COPYRIGHT

Social media and the abstract self

Dr Penelope Rush,

The University of Tasmania

Penelope.Rush@utas.edu.au

The focus of this paper will be on the idea that what we believe or implicitly assume about the nature of abstract reality, information, and interaction is an important determining factor in the construction of an ethics of online social networking and online encounter generally. But an important factor in understanding and determining those beliefs is the set of beliefs we have about the nature of *ordinary* physical reality. Examining the relationship between these sets of beliefs and the effect of both on an ethics of social networking will help us to fully understand the impact that fundamental conceptions of reality may have on our actions and responsibilities online.

When we're immersed in social interactions online, we commonly understand what we are engaged in simply as an extension of our ordinary, everyday concept of reality. But the role of such implicit beliefs about reality at play in our common experience of online social interaction presents an important and largely unexplored challenge to our conception of ordinary reality itself. In turn, that conception plays a crucial role in determining our online behaviour and consequently in informing an ethics of social networking.

We construct and conceptualise a digitised self in myriad ways, but in a sense, all of these can be understood as reinforcing the notion that streams of data fill out their own robust reality, and thus that physical and digital reality share important similarities. Self-expression and interaction with others on social media are often conceptualised in literal terms: for example, we commonly assume that our 'Facebook self' is simply an aspect or an alternative mode of expression of our real self. This conceptualisation already blurs our online and offline identities in a way that calls for a re-examination of our underlying assumptions about what constitutes our real self.

It could also be argued that such blurring is exacerbated and extended by a phenomenon well characterised by the Twitter slogan: "Follow your interests, Discover your world" (Twitter slogan 2013), in which online interaction is conceptually set apart from other forms of mediated interaction such as letters and phone calls. This phenomenon is the construction of an online identity with its own 'shape' and its own digitised world, which either essentially participates in, or (if conceptualised as separate in some way) may be conceived as equally real to our offline identity. This sort of perception, along with similar reported perception accompanying World of Warcraft- and Second Life-type immersive experiences, suggests there is evidence to be gathered of a pervasive, subtle shift in our common conceptualisation of reality in general, including our conceptualization of both our on- and off-line selves.

An important aspect of this discussion is the phenomena of data mining and its implications. The mining of digital data for individual preferences, opinions and personal characteristics opens the possibility of a future internet akin to an individual virtual reality – one designed for a largely online persona (Stray 2012, Google Project Glass 2013).

In short, in order to understand the impact of social media on society, we need to ask whether and to what extent a pervasive reconceptualisation of reality is defendable: to what extent can and should the online self be correctly understood as part of our real self, or as a real self at all? I will examine the question whether the blurring of the two realities can be explained or defended on the basis of existing philosophical work on the nature of abstract and ordinary reality.

Possible causes and motivations behind the shift also need considering here: particularly the role of interested groups (primarily software companies): e.g. we need to investigate whether there are good philosophical and ethical reasons to believe that there are important differences between the digital self and physically embodied self that may be deliberately obscured in the push to exploit interactive and immersive technology as it unfolds.

The online self and the digital world it increasingly inhabits have so far been studied primarily from technological or sociological perspectives (e.g. van Doorn, N, Wyatt, S & van Zoonen, 2008, Boyd 2007, Floridi 2010). Perceptions of presence, degrees of interaction, etc. have been researched, but it is only very recently that philosophers have begun to look at the problem of online and digital *reality* at all. When they have, they've typically approached the problem from having noted *similarities* between online and physical reality (Floridi 2011, Hongladarom, 2011). The resultant theories (in particular Floridi's theory of the informational nature of reality (2008)) echo the apparent trend in our communal implicit beliefs: i.e. they often appear to entail that physical reality and digital reality are only as real as each other.

The careful examination the impact of these theories (again, both implicit and explicit) on the ethics of social networking services, as well as a comparison of this impact with the potential impact of other possible theories of on- and off-line reality, is a vitally important task, not just in the field of computer and information ethics, but in distinguishing genuine from fabricated encounter and so developing respect, trust and confidence in any interaction with another whatsoever.

Boundaries blurred, reality reconceptualised

Given that to varying degrees, the boundary between on- and off-line reality is blurred: in our common experience; in our common implicit beliefs and preconceptions; by companies with vested interest; and in current philosophical theorising; the remainder of this paper will sketch some ways in which we might begin to measure the impact of this blurring on our ethical conduct and values.

On one hand, we might argue such blurring has a positive impact on the grounds that it extends our perception of others as embodied genuine agents into the online realm, and so encourages the carry-over of established offline (ordinary, real world) moral norms and behaviour in our online interactions (see, for example, Stokes 2013). But this seems right just to the extent that this sort of 'carry-over' or extension of 'real' morality to online encounter is predicated on there being a difference between the two sorts of encounter in the first place. That is: if we need, in the online sphere, to remind ourselves that a genuine independent other is behind the lines of digital text, Instagram images, even Facetime conversations – we need also to remind ourselves that this may be because an online encounter is different in kind to an offline encounter. If so, an essential part of the successful extension of offline to online morality will involve understanding that difference better.

On the other hand, we might argue such blurring has a negative impact. What grounds are there to suppose this might be the case? We can begin to outline one central reason supporting the claim that the impact is negative, by appeal to the core elements of attention epistemology and the values it supports. Attention epistemology "assumes the *intrinsic* value of anything, everything, that is not the self" (McFague 1993, 50, italics in original text). I suggest that rather than emphasise 'intrinsic' here, we look carefully at the term 'not'. A key element in valuing the other for its own sake ("in and of itself (and not "for me")", (McFague 1993, 50) is in acknowledging the other as *not* us – as essentially different, with its own point of view from which it exists, as opposed to from our point of view by which we know and understand it.

There are quite a number of complexities within the idea of *not* in this context, which, when we can begin to tease them out, suggest that this particular *not* may in many ways constitute, or at least effectively indicate, a real encounter of a real other. There are a number of ways in which we are not what (or who) we encounter, when we allow that (or when indeed it is the case that) the other has a reality independent of our own. One of these might best be captured by the notion of *incomplete circumscription:* the encounter between us and a wholly other cannot be circumscribed by us – any complete circumscription of such an encounter must involve both individual perspectives from their own points of view and with (all) of their own reality (again, 'as it is in itself'); so, *not* here can encompass the notion: 'not circumscribable'.

This means that any such circumscription: by our knowledge, our intellect, our comprehension in general, must always be essentially incomplete. A helpful comparison might be drawn with knowledge of mathematics: as Hartry Field puts it, mathematical objects are, in an important sense, just whatever satisfies mathematical theory. He points out that even if there is a single mind-independent mathematical universe[2], "the mathematical sentences we accept so directly determine their content that they are bound to come out true so long as they are consistent" (Field 2008, 326). So, while mathematical reality is, in this sense, completely circumscribable, the reality of an independent other is not.

But there's also an aspect of this *not* at play even within the knowledge we *can* acquire of such independent others. In an encounter with an independent reality, the positive knowledge *we* gain of it is always only our own. It is knowledge from our point of view. This by itself does not necessarily undermine the status of such knowledge as itself knowledge, but it does introduce an essential *'also not'* into every positive piece of knowledge, understanding, or circumscription of the other: a sort of shadow stands behind each, reminding us that even our clear claims to knowledge are limited simply because they are ours.

Iris Murdoch said: "Art and morals are ... one. Their essence is the same. The essence of both of them is love. Love is the perception of individuals ... the extremely difficult realization that something other than [i.e. not] oneself is real. Love, and so art and morals, is the discovery of reality" (quoted in McFague 1993, 50). Taking our lead from Murdoch, morality and ethical behaviour originates in the recognition of the other as other. I suggest that this recognition is only available as an import in online encounters (i.e. it can only be imported from our experiences of real encounter and projected onto online encounter, not found within online encounters themselves). That is, online interaction is (arguably) missing the *not.* This is where it may be essentially different from offline interaction: what we access online is fully circumscribable, much like mathematics is. What we read and view online is fully encoded and

[2] I happen to think there is, even though mathematical reality is in this sense, completely circumscribable. But that's an argument for another day.

so fully de-codable (in principle) information. It is not only accessed, but inherently *accessible.* By itself, it has no *also* and no *not.*

This framework gives us a way in to understanding the affects of the blurring of our conceptions of on and off-line realities, and the beginning of a means by which we can weigh the risks and advantages of theories that propound it (especially, for instance, Floridi's informational ethics (outlined in his 2006), which treats everything there is as "informational objects" constituted by "clusters of data" (Bynum 2011). It might also serve to illuminate other philosopher's analysis of online social networks, such as Borgmann's differentiation between 'indifferent' and 'commanding' self-presence (corresponding to its on- and off-line expression); and his contention that it is only in offline (real-world) experience that we "[see] people in the round" (quoted in Vallor 2012).

Degrees, manifestations and types of blurring.

On a more practical note, we need also to examine the ways in which the blurring of the two realities is present in different degrees[3] (to different people, in different media, across different soft and hardware); it's various possible manifestations (e.g. our experience of immersion in *Second Life* compared to emailing or text messaging) and types (e.g. mobile devices, roomed-sized holographic projections, photos, text). Mobile technology, for instance, arguably engenders a more embodied blurring, due to the way in which we treat tools as an extension (rather than primarily a means of expression or communication) of the self: akin to the way we famously treat our car, for example.

This is an area needing more research, but it seems likely that different mediums (programs, applications, services) engender or encourage correspondingly varying degrees of self-presentation and awareness of the self and the other *as* presented. Likewise, different users (depending on factors such as age groups, backgrounds, frequency of use) will likely experience themselves and others online in quite different ways.

References

Bynum, T. 2011: "Computer and Information Ethics", *The Stanford Encyclopedia of Philosophy* (Spring 2011 Edition), Edward N. Zalta (ed.), URL = <http://plato.stanford.edu/archives/spr2011/entries/ethics-computer/>Feild H. 2008: *Saving Truth From Paradox,* Oxford University Press, New York.

Floridi, L. 2006, "Information Ethics: Its Nature and Scope," *Computers and Society*, 36(3): 21-36.

Floridi, L. 2011: 'The Informational nature of Personal Identity'*, Mind and Machines*, 21: 549-566.

Floridi, L. 2010: *The Cambridge Handbook of Information and Computer Ethics*, (ed), Cambridge University Press, UK.

Google Project Glass 2013: https://plus.google.com/+projectglass. Accessed February 28, 2013

Hongladarom, S. 2011: 'Personal Identity and the Self in the Online and Offline World', *Minds & Machines* 21:533–548

McFague, S. 1993: *The Body of God: An Ecological Theology,* Augsburg Fortress, Minneapolis.

Stray, J. 2012; neiman lab: http://www.niemanlab.org/2012/07/are-we-stuck-in-filter-bubbles-here-are-five-potential-paths-out/ Accessed February 28, 2013.

Stokes, P. 2013: *Do You Really Exist Online?,* in New Philosopher Magazine, Bull Publishing, NSW.

Twitter 2013: http://discover.twitter.com/. Accessed February 25, 2013

[3] Thanks to an anonymous referee for suggesting this

Vallor, S. 2012: "Social Networking and Ethics", *The Stanford Encyclopedia of Philosophy* (Winter 2012 Edition), Edward N. Zalta (ed.), URL = <http://plato.stanford.edu/archives/win2012/entries/ethics-social-networking/>.
van Doorn , N, Wyatt, S & van Zoonen , L. 2008: 'A Body of Text', *Feminist Media Studies*, 8:4, 357-374

ICT Research Ethics Regulation and Governance: Issues with the Human Research Ethics Committee

Craig McDonald

University of Canberra, ACT, Australia.

The Human Research Ethics Committee (HREC) is the primary regulator of ethics in research involving humans, at least where that research is conducted in public institutions in Australia. The HREC takes its mandate and ethical parameters from the *National Statement on Ethical Conduct in Human Research.* To respond to the National statement organisations such as universities, hospitals and so on set up and operate internal procedures that require research projects involving human participants to be evaluated by an HREC.

A range of general issues and frustrations have been articulated by researchers complying with the system, including discomfort with bureaucratic nature of the HREC, irritations with compliance and its conflict with autonomy, etc. A different range of issues is experienced by those concerned with the overseeing the ethics of research. Like the researcher, the regulator has issues with the bureaucratic nature of the HREC in particular with researcher resistance, workloads and cost.

However the bigger picture is much more problematic, particularly when it comes to the ethics of ICT research, as shown by the following extract from *Complexities in the Ethics of ICT Informatics Research and Innovation*, a paper from the 2012 AiCE conference (See following supporting document).

While the big picture is problematic, it is always the individual taking an action that is the locus and focus of actual ethical evaluation. It is the actual circumstances of the individual, how she sees her situation and what she knows and values, that determines her action and so the ethical aspects of that action and its aftermath. It is this situation that the ethics regulator should be addressing if it wants more ethical research. The HREC is part of the integrity system of a research organisation - is that system explicit, operational and effective? Is the HREC role effective? Arguable the answer to these questions is 'no'.

The purpose of the discussion at AiCE is to canvass the practicalities of the research ethics integrity system and the role of the HREC in it, then to make proposal for improvement. Sample proposals might be:

Proposal 1: Broaden the focus of the HREC from considering harm to immediate research participant to also considering *consequential ethic*s - harm to others down the track. Presently few ICT research projects go to the HREC as they don't have human participants, but they have, potentially, enormous human consequences.

Proposal 2: Integrate research ethics with the research organisation's professional ethics and quality systems. The HREC scope is at once too narrow (much research-like activity is conducted in coursework so does not come to the HREC) and at too low a level.

Proposal 4: Scrap the HREC Application. Ethics applicants should have their research proposal itself reviewed from an ethics perspective and where it is found wanting, the proposal should be changed to better embed ethics into its design.

SUPPORTING DOCUMENT TO DISCUSSION PAPER

Complexities in the Ethics of Informatics Research and Innovation

Craig McDonald

University of Canberra, ACT, Australia.

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 (eg 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 is 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.

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) T*he 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, G Bammer & 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

Managing information and communication technology in schools.

Steven Vella, DER-NSW Technology Support Officer, Junee High School;

Charles Sturt University, NSW.

Managers of information and communication technology (ICT) work in a rapidly changing global industry and face many challenges, including ethical ones. Whether or not they are sufficiently equipped to recognise when an ethical challenge confronts them and what to do about it when they do recognise it, is debatable. After briefly putting these challenges in the global context, this discussion paper focuses on my experiences in the education sector during a period where the national Digital Education Revolution injected over 967,000 mobile devices through the National Secondary School Computer Fund (NSSCF) to Year 9 to 12 students across Australia (Australian Government, 2013a).

When considering the ethical implications of a situation a number of techniques could be used. Challenges are increased by the cultural differences in interpreting ethics in ICT (Jagger & Strain, 2007; Burmeister, 2013). However, the application of these techniques in the ICT sector may not be in common use by ICT professionals (Weckert & Lucas, 2012; Al-Saggaf & Burmeister, 2012).

On the one hand, skills and techniques useful to managers of ICT start with classical utilitarian (Driver, 2009) and contemporary deontological (Alexander & Moore, 2012) ethic theories and extend to such tools as reasoning software such as Rationale 2, the Australian Computing Society (ACS) code of ethics and professional practice (McDermid, 2008), the ethical decision making process (McDermid, 2008), professional ethics theory (Nello, 2010) and the doing ethics technique (Simpson, Nevile & Burmeister, 2003).

On the other hand, even if these techniques were taught, would there be a way to evaluate their ability to apply them because of the many factors that could influence their answers, including those mentioned by Jagger and Strain (2007) such as culture, financial pressures and comprehension of questions.

It is then interesting to investigate these issues in a specific context, namely that of managing ICT in Australian schools.

- The breakdown of NSSF by the Australian Government (2013b) between each State and Territory and the government, independent and Catholic schooling sectors show wide variations, for example in the government sector where 0.8% and 38% of government sector funding went to the NT and NSW respectively. The funding based on the school's location, its sector as well as student numbers and the socio-economic status of their community impacts decisions for managing ICT at many levels, for example, whether the school's ICT support services should install a high definition imaging printer for photography, purchased and approved by the school because of a perceived need and effective product marketing even though it is outside the support services scope of work.
- Laaly, Sharples, Tracy, Bertram and Masters (20120) discuss changes to facilitate ethics approval for researching students learning with mobile and ubiquitous technologies. A similar discussion may be needed for the provision of technology in primary and secondary schools dealing with students who are primarily children. Changes could consider ways to define participation, teacher roles, informed consent, attachment, suitability of material and privacy as boundaries are greyed, authenticity is more difficult to ascertain and outcomes are less predictable. For example, where some schools will transition to a bring your own device (BYOD) strategy and single-

vendor cloud-based applications even though the Australian protocol for storing data offshore has not been defined (Australian Computer Society, 2013) and an in-house or alternate vendor solutions could provide a similar or better result.

- Any reliance on school management, from observation traditionally recruited from teachers, to address local issues not defined in ICT-project policies and procedures questions whether teacher education (Phelan, 2011) provides an adequate grounding in ethics to deal with such issues. For example, where a school principal is asked to decide how to action broken devices requiring students from both wealthy and low socio-economic circumstances to pay for repairs under a high (in relative terms) fixed single price model for repairs, whether it is for a keyboard or a new screen;

References

Al-Saggaf, Y., & Burmeister, O. K. (2012). Improving skill development: an exploratory study comparing a philosophical and an applied ethical analysis technique. *Computer Science Education, 22*(3), 237-255. doi: 10.1080/08993408.2012.721073

Alexander, L., & Moore, M. (2012). Deontological Ethics. In Zalta, E. N. (Ed.), *The Stanford Encyclopedia of Philosophy*. Retrieved 15/11/2013, from http://plato.stanford.edu/archives/win2012/entries/ethics-deontological/

Australian Computer Society. (2013). Cloud Computing Consumer Protocol - Discussion Paper. Retrieved 14/11/2013, from http://www.acs.org.au/information-resources/public-policy/2013-australian-cloud-protocol

Australian Government. (2013a). *Education*. Retrieved 14/11/2013, from http://www.budget.gov.au/2013-14/content/bp3/html/bp3_03_part_2c.htm

Australian Government. (2013b). *National secondary school computer fund funding allocations for all rounds and all sectors*. Department of Education, Employment and Workplace Relations Retrieved from http://docs.education.gov.au/system/files/doc/other/d13_410508_national_secondary_schools_computer_fund_all_rounds_funding_allocation_by_sector_0.pdf.

Burmeister, O.K. (2013) Achieving the goal of a global computing code of ethics through an international-localisation hybrid, *Ethical Space: The International Journal of Communication Ethics*, 10(4), 25-32.

Driver, J. (2009). The history of utitarianism. In Zalta, E. N. (Ed.), *The Stanford Encyclopedia of Philosophy*. Retrieved 15/11/2013, from http://plato.stanford.edu/entries/utilitarianism-history/

Jagger, S., & Strain, J. (2007). Assessing students' ethical development in computing with the defining issues test: Challenges to be addressed. *Journal of Information, Communication and Ethics in Society, 5*(1), 33 - 42. doi: 10.1108/14779960710822674

Lally, V., Sharples, M., Tracy, F., Bertram, N., & Masters, S. (2012). Researching the ethical dimensions of mobile, ubiquitous and immersive technology enhanced learning (MUITEL): a thematic review and dialogue. *Interactive Learning Environments, 20*(3), 217-238. doi: 10.1080/10494820.2011.607829

McDermid, D. (Ed.). (2008). *Ethics in ICT: an Australian perspective.* Malaysia: Pearson Education Australia.

Nello, A. (2010). The circumscribed quadrature of professional ethics. *Ramon Llull Journal of Applied Ethics, 1*(1), 143 - 164.

Phelan, A. M. (2011). Towards a complicated conversation: teacher education and the curriculum turn. *Pedagogy, Culture & Society, 19*(2), 207-220. doi: 10.1080/14681366.2011.582257

Simpson, C. R., Nevile, L., & Burmeister, O. K. (2003). Doing ethics: A universal technique in an accessibility context. *Australasian Journal of Information Systems, 10*(2), 127 - 133.

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

Ethics and Governance of ICT-based social engagement in institutional aged care

Ken Eustace* and Oliver Burmeister*

* School of Computing and Mathematics, Charles Sturt University, NSW, Australia.

Abstract

A pilot project in 2010-2011 aimed to determine whether the introduction of technology at an aged care facility in North-East Victoria had increased social engagement for residents. The study aimed to determine the extent to which ICT and Internet access had increased the social engagement of residents, within and outside the aged care facility. This study uniquely included the views of staff and management and provides a focus for discussion about the ethics and governance of ICT-based social engagement in institutional aged care.

Introduction

Governance is an important area of ethical consideration, including in the business of institutional aged care. More widely, governance as an area of ethical discussion, has been addressed both nationally and internationally (Weckert & Lucas, 2012; Burmeister, 2013), and some recent work has also examined governance in technology use by seniors (Burmeister, Foskey, Hazzlewood & Lewis, 2012), and in institutional aged care (Bernoth, Dietsch, Burmeister & Schwartz, 2013). Use of ICT and Internet in aged care by residents was relatively new in 2010 even as many retirement villages were introducing technology for use by residents. The key question for this study was:

> ***Has the ICT introduced at the aged care facility, increased the social engagement of its residents?***

The data collected using ethnographic interviewing techniques and the criterion based purposive sampling of information rich-cases would also contribute to the in-depth analysis of ethics and governance issues.

3. Snapshots of some Rich Data Observations

T1 is retired teacher and began using computers in 1983 in primary schools. T1 is a **volunteer trainer** and "pet therapist" whose mother was living at the aged care facility, and is continuing her contact with the home as a volunteer each Thursday afternoon.

The training goes for an hour as the seniors may get tired. T1 is experienced in working with training seniors having done work with the University of the Third Age. Her approach is friendly, conversational and uses self-paced student-centred approach small groups, with 2 learners as the best training format. In her opinion, training in small groups works better for older people.

Many with eyesight and motor skill problems find it hard but one male R3 is looking at ways to participate in training. Up to five residents have started the computer training but have dropped out for several reasons including frustration and lack of confidence.

R1 and R2 are friends. Knowing that R2 is deaf in her right ear and that R1 can't move her neck to the left so all is well as long as R1 always sits at the left side of R2. R2 is a keen computer user due to life experience and told that her family members do make big use of computers around their home.

Now R1 and R2 are together in ICT training focused on use of the Internet. Both women are bright, alert and an open mind towards use of computers and certainly not afraid but rather excited about using the technology to “break out” or escape from the walls of the home, even though they enjoy being there. Regular family contact is a big motivator.

In their working lives, R1 as personnel officer in Human Resources while R2 had worked for the PMG in telecommunications and worked on teleprinters and for OTC. Both had supervised other staff as team leaders.

R1 interview results

R1 uses a track ball as the mouse was too hard with arthritis and the cursor with trail made it easier to see. R1 was in her late 90s and had trouble with her neck movements to the left. R1 uses hotmail account that her daughter set up but T1 prefers Gmail as the interface pops up ready to use and the good spam filtering, giving the uncluttered feel. R1 has relatives in Norway and Nova Scotia and hopes to make contact with great grandchildren.

Facebook is scary to R1 while all agreed that it has privacy issues and is blocked on the local network. R1 says it may be in the future to they get to use Facebook, after further developing their self-efficacy with email and Skype as the first step.

R2 interview results

R2 was using her Gmail account to write an email message and she uses the room quite often and was the “power user” of some influence. She is quite confident in some ways although feels she still has so much to learn. R2 has Skype contacts with 3 family members. R2 was fascinated with the key size of the iPad and with how small and light it was to carry around. During an iView benchmark R2 was introduced to the service as service oriented motivation, she was able to watch the last 6 minutes of the New Inventers grand finale that she missed the previous evening.

4. Summary and discussion of findings

The user experience by the residents in this study was influenced by several interplaying factors. These included some factors to enhance the experience while others were limiting factors:

1. Motivation to use ICT to stay in touch with the family;
2. Prior experiences with ICT, including privacy issues with social networks;
3. The individual’s own self efficacy, confidence and pride in using ICT;
4. Access to and availability of the ICT services in the aged care facility;
5. Support and encouragement from family, peers and staff;
6. Reluctance to go beyond using e-mail, Internet and Skype on a computer to using social media, mobile device and applications;
7. Device interaction and usability (computers and tablets preferred over smart phones)
8. Physical disabilities with sight, hearing and motor skills (hand movements).

For the staff at the aged care facility, the ethics and governance is providing ICT as an Enterprise System requires changes that will increase running costs (e.g. wireless networks and keeping up to date with new ICTs) as well as a need to make changes to governance processes, people and existing systems such as a re-design of ICT infrastructure and processes, possible job re-training for staff and Integration with other core services at the aged care facility.

In the two years since the study, there have been some huge changes in both the technologies available, like tablet devices and the changes on the horizon with the National Broadband Network or NBN, and the style of ICT-based social engagement by seniors, but further research is needed to investigate the

scope of it all again in 2014 for both the residents in institutional aged care and the wider ethical implications, role and governance of management in an aged care facility.

Research conducted in the USA by Zickuhr & Madden (2012) revealed findings of significance and pointers for future research in Australia on the patterns of behaviour with seniors and ICT use as shown in the short list of their findings below:

- Over 53% of seniors over 65 use the Internet, with 70% of that group going online daily;
- Once online, Internet use becomes a regular part of seniors lives with 39% having broadband at home;

However after age 75, the Internet and Broadband use drops away significantly and this category has strong representation in our aged care facilities:

- 68% of those aged 75+ did not feel confident and needed someone to help them get online;
- Only 20% of users in this cohort use social networking sites and just 8% on a daily basis;
- Relevancy of the Internet and lack of interest in using e-mail became an issue for 38% over those aged 75+

Conclusion

Technology use by seniors is not new. Many studies have shown that seniors of all ages enjoy learning to use technology (Arjan, Pfeil & Zaphiris, 2008 ; Burmeister, 2012; Burmeister, Weckert & Williamson, 2011; Sayago & Blat, 2010; Xie, 2008) and that there are many benefits to gain apart from social engagement for those with reading and physical issues, in using iPad and other Tablet applications (Silveira, Daniel, Casati & de Bruin, 2013).

This study was an Australian first in that it looked both at resident and staff use of technology for social engagement, in institutional aged care. The future plan of this research is for regular and more detailed examination on the ethics and governance of ICT-based social engagement to include staff and residents as a community with equity and access to technology, particularly before the “baby boomers” populate the aged care communities in the 75+ age category from 2020.

References

Arjan, R., Pfeil, U., & Zaphiris, P. (2008). *Age differences in online social networking.* Paper presented at the Computer-Human Interaction '08, Florence, Italy.

Bernoth, M., Dietsch, E., Burmeister, O. K., & Schwartz, M. (2013). Information Management in Aged Care: Cases of Confidentiality and Elder Abuse. *Journal of Business Ethics*. doi: 10.1007/s10551-013-1770-7.

Burmeister, O.K. (2013). Achieving the goal of a global computing code of ethics through an international-localisation hybrid, *Ethical Space: The International Journal of Communication Ethics*, 10(4), 25-32.

Burmeister, O. K., Foskey, R., Hazzlewood, J., & Lewis, R. (2012). Sustaining online communities involving seniors. *Journal of Community Informatics, 8*(1).

Burmeister, O. K. (2012). What seniors value about online community. *Journal of Community Informatics, 8*(1).

Burmeister, O. K., Weckert, J., & Williamson, K. (2011). Seniors extend understanding of what constitutes universal values. *Journal of Information, Communication & Ethics in Society, 9*(4), 238-252.

Sayago, S., & Blat, J. (2010). Telling the story of older people e-mailing: An ethnographical study *International Journal of Human-Computer Studies, 68*(1-2), 105-120.

Silveira, P., Daniel, F., Casati, F., & de Bruin, E. (2013). Motivating and assisting physical exercise in independently living older adults: A pilot study ***I****nternational Journal of Medical Informatics*, 82(5), 325-334.

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

Xie, B. (2008). The mutual shaping of online and offline social relationships. *Information Research, 13*(3).

Zickuhr, K. & Madden, M. (2012): Older adults and internet use. *Pew Research Center's Internet & American Life Project*, http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_Older_adults_and_inter.net_use.pdf, (accessed June 02, 2013)

Are We Failing a Generation?

Gillian Harvie

Judicial Support Specialist, Information Technology Services

Courts Administration Authority; and

Doctor of Philosophy student, Charles Sturt University, NSW.

INTRODUCTION

The digital divide literature addresses many areas, including gender, ethnicity, literacy and more, and yet the oldest-old people in society are rarely mentioned. Although the literature shows that younger seniors are actively using many forms of computer technology (Czaja & Lee, 2007; Burmeister, Weckert Williamson, 2011; Hanson, 2011; Burmeister, 2012), it seems that with regard to access of information, resources and services, we are failing a generation namely the oldest-old (Hanson, 2011).

DISCUSSION

Increasingly, commerce is being conducted electronically. Bricks and mortar stores are unable to compete and are closing at an alarming rate. Where will our ageing population purchase their goods? Will there be a select and niche market aimed solely to the elderly and charging accordingly? Magazines now have apps embedded in their pages for smart phone users to download information. Television programmes are appealing to the technologically savvy to download and view programmes and movies. Bookings for buses, cinemas, and health appointments can all be done online now, leaving the elderly disadvantaged. With the advent

of digital viewing, is it possible that there will emerge a generation of viewers who view solely on their hand-held devices, negating the need for televisions at all? What will this mean to the elderly? How will they stay in touch with the expanding technology?

Some advances in technology may appear to be gimmicks or fads. People are starting to take note of Google glass, for instance as a way of accessing data from anywhere with a computer built in to spectacle frames. This should not be unwieldy for our elderly users as theoretically they should just attach, reasonably unobtrusively, to their own spectacles. There are a number of legal and ethical issues that would need to be overcome for wide-spread use of this technology but it seems fair to say that even if it proves to be a short-lived gimmick, there will be something else to take its place. Whether this would affect the oldest technology users in any substantial way is worth considering.

It is likely that laptops and computers will become relics of the past. Already some businesses are providing wireless tablets such as iPads to their employees, making the desktop computer obsolete for their work activities. As the demand for handheld devices becomes more prevalent so the supply of older technology may become more difficult to obtain. It may be that app-based technologies may make it easier for the elderly to access information. This may be an area for further investigation as to whether this will be cognitively easier for them to understand and whether failing eyesight and physical dexterity will enable them to access it. Is it possible that the inability to keep up may lead to depression, loneliness and isolation?

It is important to carefully define what is meant by old or older. This is not as easy as it sounds. Varying factors such as social demographics, educational background, financial status, health

etc will affect abilities and perceptions of all people. For any group of people of the same age there will be varying levels of ability. An active 90 year old could be more capable than another person 20 or 30 years younger with different life experiences. However, for the purposes of this research, old is defined as aged 80 and over. A preliminary search of the literature has resulted in the following discussion.

There are three main areas of discussion that this paper is addressing. Firstly, there are methodological considerations in research that addresses the digital divide for seniors. According to Czaja & Lee (2007) "…although the use of technology such as computers and the Internet among older adults is increasing, there is still an age-based digital divide" (Czaja & Lee, 2007, p. 341). These authors discuss services available via the Internet, which put the elderly at a disadvantage. They acknowledge that computers by themselves don't impact the well-being of the elderly. "Many of the studies that have examined this issue have been plagued by methodological shortcomings. As such, there is a need for more rigorous research in this area". (Czaja & Lee, 2007, p. 342) Is this still true? What would add rigor?

Secondly, there is the divide of finance. It appears that older adults are not averse to using computers and technology. In fact they can see the benefits, but problems such as training and assistance, cost factors and available applications are hindrances (Czaja & Lee, 2007, p. 343). It could be argued that geographical isolation also provides a barrier. Governments are providing NBN technology around coastal areas of Australia but these are not available to remote, country and inland communities. However, consideration would need to be given to whether this is an age-related problem, or one experienced by all members of such

communities. Are the elderly any more disadvantaged in these areas than their younger generations?

Thirdly, there is the cognitive divide. Older people may have age-related deterioration in their ability to process information as well as multi-tasking and many other activities inherent in computer use. Things that would be intuitive to a younger user are not so for the elderly. "Age-related changes in cognition have important implications for the design of technical systems" (Czaja & Lee, 2007, p. 344). Elsewhere related observations have been made about increased learning difficulties that come with older age, especially for the oldest-old (Burmeister, 2010). Burmeister (2010) highlights failing memory as a hindrance to the elderly, with particular regard to remembering login credentials. Increasingly websites require user names and passwords to facilitate access. Without these, there are significant security concerns. Renaud and Ramsay, 2007 recognise the difficulties experienced by those with failing memories to recall these authentication details and discuss the possibility of using biometrics such as the user's handwriting or doodles. While these would not be suitable for highly secure websites, they could be applicable for low-risk sites (Renaud & Ramsay, 2007, p. 313).

Dwivdei, Weerakkody & Janssen (2011) discuss the implementation by governments and acceptance by society of e-government programmes to provide government services and information electronically. It is acknowledged that among the numerous challenges to e-government projects is the exclusion of the elderly and disabled, the less educated and poorer members of society. This scenario is currently playing out in the US with the health care reforms.

Hanson (2011) suggests that the current younger generations, who have grown up with technology and are proficient in its use, appear to hold the view that problems experienced by the older generations will be self-limiting and will cease to be an issue with the extinction of that generation. Many believe that (1) as they grow older they will not experience any of the age-related disabilities with the use of technology and (2) their current proficiency and understanding of technology will enable them to "keep up" with future technology. Hanson (2011) explores whether these beliefs are valid by working with older adults to determine what are their strengths and difficulties in the use of technology?

I use the term "extinction" of a generation advisedly. The term seems harsh. Why would you give up on an entire generation and just wait for them to disappear? These beliefs of the younger generation in their inherent ability to "keep up" with technological advances, as stated above, would seem to be naïve. The problem will not go away with the disappearance of our current old-old. As our younger generation ages they will inevitably be faced with the same age-related disabilities of cognition failure, deterioration of physical health and memory loss. If we give up on the elderly now, we are failing them as a generation and the problem will still be there for future generations to address.

REFERENCES

Burmeister, O. K. (2012). What seniors value about online community. *Journal of Community Informatics,* 8(1).

Burmeister, O. K., Weckert, J., & Williamson, K. (2011). Seniors extend understanding of what constitutes universal values. *Journal of Information, Communication & Ethics in Society*, 9(4), 238-252.

Burmeister, O. K. (2010). Websites for seniors: Cognitive accessibility. *International Journal of Emerging Technologies and Society*, 8(2), 99-113.

Czaja, SJ, & Lee, CC, 2007, 'The impact of aging on access to technology', *Univ Access Inf Soc*, Vol 5, pp. 341-349.

Dwivedi, YK, Weerakkody V, & Janssen, M, 2011, 'Moving Towards Maturity: Challenges to Successful E-government Implementation and Diffusion', *The DATA BASE for Advances in Information Systems*, Vol 42, No. 4, pp. 11-22.

Hanson, VL, 2011, 'Technology skill and age: what will be the same 20 years from now?', *Univ Access Inf Soc,* 10, pp. 443-452. Online 20 April 2011.

Renaud, K, & Ramsay, J, 2007, 'Now what was that password again? A more flexible way of identifying and authenticating our seniors', *Behaviour & Information Technology*, Vol 26, No. 4, pp. 309-322.

Operational Possibility for Information Systems

Dr Ian Storey

RMIT, Business Information Systems and Logistics

ian.storey@rmit.edu.au

The matter of who or what is responsible if a computer performs a harmful action is a complex one, but there is some meaning in saying that computers consider options and that a computer, even when operating on deterministic algorithms, is capable of making a choice. With today's technology it is unreasonable to talk of the moral responsibility of the computer, but the responsibility of the computer's designers depends on their intent and what they perceived as the possibilities of the technology they produce. The technology is currently at the point where the complexity of the "independent" actions of information systems is such that unintended consequences complicate the issue.

The issue requires a distinction in the modality of possibility at a fundamental level. A logical model is proposed here which carries with it a simple distinction in terms. The term "operational possibility" is intended to delineate a number of issues to do with systems which collect information and make models of the world. Crucially, these systems have *incomplete* "knowledge" of the world.

A simple subset relation between different many-world frames suffices for the model. This results naturally in an order relation (a transitive, anti-symmetric relation based on the subset relation). This model has a practical impact in the communication between agents and information systems, which in turn has a fundamental impact on ethical issues.

The central element of this model is that there are distinct agents, who *have different knowledge of the world*. One agent may know that a statement is false, and another may think that the statement is *possible*. Similarly, one agent may know that a statement is true, and another agent, because of their imperfect knowledge, thinks that the statement is *possible*.

Temporal possibility is widely applied: it may rain tomorrow but it did not rain yesterday, a coin toss may land a head, but afterwards it is impossible that it landed a head. However there is a similar change that occurs when an agent/information system makes observations, or when they communicate. Even day-to-day uses of the modality of possibility show this: a coin toss landing in front of our eyes takes some time to be registered in the brain of the viewer, but also, someone who is informed about the coin toss later clearly changes their notions of possibility in response to *information*.

In another context, because of operational possibility, it is meaningful to talk of, say, the search for life outside the solar system, even though this is either a certainty or an impossibility.

This discussion is deliberately non-technical, partly to demonstrate that there is value in the analysis beyond a purely technical exercise.

With these caveats and qualifications, the distinction between an operational, "subjective" form of possibility and objective possibility is as valuable as the distinction between the subjective perception of the sound of a tree landing in a forest and the vibrations in the air that are caused by the tree's fall.

Appendix – Full Paper

Operational Possibility for Information Systems

Introduction

The matter of who or what is responsible if a computer performs a harmful action is a complex one, but it there is some sense in saying that computers consider options and that a computer, even when operating on deterministic algorithms, is capable of making a choice.

With today's technology it is unreasonable to talk of the moral responsibility of the computer, but the responsibility of the computer's designers depends on their intent and what they perceived as the possibilities of the technology they produce. To say the least, the technology is currently at the point where the complexity of the "independent" actions of information systems is such that unintended consequences complicate the issue. The issue requires a distinction in the modality of possibility at a fundamental level.

This is perhaps the most difficult question being addressed in this paper but the intent is to examine in a more general way the issue of the modality of possibility when different agents/information systems interact. By use of examples it will be shown that the distinction applies in more prosaic environments and the extension to information systems generally is quite natural.

A simple logical model is proposed here, and along with it a simple distinction in terms. The term "operational possibility" in contrast to "objective possibility" is intended to delineate a number of issues to do with systems which collect information and make models of the world. Crucially, these systems have *incomplete* "knowledge" of the world.

Finally this essay looks briefly at the various senses in which an information processing system can be said to "make choices", even one running a deterministic algorithm. So for example, in what sense can a chess program be said to make a choice between moves?

These matters hinge on the distinction between different *forms* of possibility, and this is used to delineate ways in which agents describe the extent of their knowledge. This has practical impact in the communication between agents and information systems, and this in turn has a fundamental impact on ethical issues.

The distinction proposed here is fundamentally an epistemological tool rather than a linguistic one. The logical machinery required is extremely simple. Examples taken from a variety of contexts demonstrate the theory.

This essay is not intended to advocate an objectivist or relativist approach. It is "agnostic" also about determinism and indeterminism. The aim is to investigate the inter-relation between ways in which agents use the modality of possibility to refer to real-world possibilities within the limits of their knowledge.

"Operational Possibility"

The term "operational possibility" has been adopted here. It is closest in meaning to epistemic possibility. Epistemic possibility has an important role in the study of grammar and the use of language, but the term is also open to a number of interpretations. It can be refer to a priori possibilities, known before empirical knowledge. Or it can simply express an agent's lack of knowledge, "It is possible that it is raining in Toronto, for all I know". This later meaning is closest to what is being referred to here. But more particularly, the kind of possibility that is referred to here as "operational possibility" is intended as an epistemic tool, and it applies specifically to an information processing system operating in an environment of which it has imperfect knowledge.

The term "subjective possibility" rather than "operational possibility" might have been convenient, because it contrast nicely with "objective possibility". But it can be confused with a term in statistics which refers specifically to an agent's subjective judgment of probability.

The term "relative possibility" also suggests itself, because the relative states of the knowledge of different agents is compared. But this text is agnostic over a relativist approach. Indeed, in its most general form it includes a reference to a shared "objective" world (which might be empty), but which is imperfectly known by agents. Possibilities which exists in the real, objective world are contrasted with operational possibilities and are here termed "objective possibilities". Objective possibilities, as meant here are more than simply physical or metaphysical possibilities (Berger, 2011; Wikipedia, 2013).

The term “operational possibility” then is used to refer strictly to the agent’s limited knowledge of the world. It is a form of epistemic possibility which contrasts with actual, real-world possibilities, called “objective possibilities”.

Temporal modality (Øhrstrøm and Hasle, 1995; Cresswell and Hughes, 1996; Wikipedia, 2013) has been used for technical purposes in computer science, such as proving correctness. Time features as an important element of this essay. However, temporal effects here are studied for a wider purpose, and a different model is used.

It should be said that this essay is not advocating operational possibility as the only way of interpreting modalities of possibilities. It is a tool for casting light on various epistemic questions which have to do with the states of knowledge of agents.

For the author, the notions of operational possibility arose from the consideration of ethical questions, and from this, problems of decision making. However, in hindsight, statistics also may have been a source of inspiration.

Inferential statistics is based around the notion of hypothesis testing. By using the hypothetical “if”, the statistician seems to be considering “possibilities”. This logic of hypothesis testing is used to advantage on a daily basis by statisticians.

Method and Theory

A simple basic theory is proposed and a simple model is described. A series of examples will show how a distinction between operational and objective possibility illuminates a number of issues which can otherwise be quite baffling.

There is more than a passing analogy with the celebrated tree falling in a forest, often obliquely related to a musing from Berkeley (1710). Once the distinction is made between the “subjective” perception of sound (in the brain presumably) and the “objective” event of sound (sound waves in air), the problem evaporates. The philosophical problems associated with the use of the modality of possibility are illuminated by distinguishing objective possibilities from “subjective” operational possibilities, which result from the agent’s limited knowledge.

For the purposes of this essay, an *agent* is *an information processing entity who can make assertions about the world*. The set of assertions that they “believe” are called their *knowledge*.

Now there is an objective world, one can assume, and in this world statements about probability may be true or false. For example the following statement could be objectively true, “the chance that the coin may come up a head is 0.5”.

The most crucial element of this model however is that there are different agents, who make different assertions about the world and who *have different knowledge of the world*. What is known to be true by one agent may only be possible to others.

It will be assumed here that an agent’s set of possible worlds include the real objective world. A consequence of this is that it *cannot* be the case that one agent knows that a statement is true and another knows that it is false. In this case the agent’s beliefs will be said to be *incompatible*. We will use the convenient terminological shorthand of saying that, “True is *incompatible* with false”. Incompatibility is not the same as inconsistency as will be shown below.

If an agent thinks that something is impossible, they know that it is not true. In this scheme, “impossible” means exactly the same as “false”. Thus problems can be simplified somewhat by equating “impossible” with “false”, and also with zero probability. Similarly “certainty” is interchangeable with “truth”, and with a 100% probability.

The most crucial element here is that one agent may know that a statement is false, and another agent, because of their limited knowledge of the world, thinks that the statement is *possible*. Similarly, one agent may know that a statement is true, and another agent, because of their imperfect knowledge, thinks that the statement is *possibly false*. In convenient shorthand form, both true and false are compatible with possible, although they are incompatible with each other.

Incompatibility can arise between the beliefs of different agents. It occurs only in the case that there is a statement that one agent believes is true and another believes is false. This is the only rule of compatibility. A consequence of this rule is that the possible worlds of different agents must overlap, and they will presumably contain objective possibilities in their shared beliefs.

Inconsistencies between agent’s belief sets are allowed. It is *inconsistent* for a single agent to think that a statement is possible (has a non-zero probability) and to think at the same time that the statement is also false. But what is consistent for one individual agent to think is not the same as what is compatible for different agents to believe. It is compatible for one agent to know that a statement is false (and hence the statement really is false) and for

another agent, with imperfect knowledge, to think that it is possibly true. *Consistency*, as used here, is not the same as *compatibility*. It may be that two statements which are inconsistent if asserted by one agent are nonetheless compatible if asserted by different agents.

This is essentially all there is to the theory, but a corresponding set theoretical model is presented below. The theory has been kept as simple as possible but the reader will certainly need to see it fleshed out in examples.

Before passing on to examples, it should be pointed out that one of the most potentially confounding aspects of the modality of possibility is the matter of time. Different agents at different times will have different beliefs. For logical purposes, a single agent at different times has different beliefs. These could formally be treated as separate agent belief sets. This would be a convenient place to leave the matter except that it is very useful to consider how an agent's knowledge progresses over time, as the agent learns more about the world. How do statements about possibility change, as an agent's knowledge becomes "more certain"?

Examples

A few examples should help to explain the intention behind the theory.

Rain

Suppose you live in Melbourne and today has been a very sunny day in the middle of a heat wave. The weather report has said that it will not rain tomorrow. Is it possible that it will rain tomorrow? What is the probability that it will rain?

This example seems very simple. We don't know for certain that it will rain tomorrow, and so it seems possible that it will rain tomorrow, albeit with a low probability. It is possible that it will rain tomorrow, and after tomorrow, after we have observed the weather, we will know that it will have either rained or not.

There are a few cracks in the story however. Firstly, suppose that tomorrow it does not rain. In the system proposed here, it becomes an objective impossibility that it rained. On the day *after* tomorrow, it will also be known by the agent that it did not rain, so for that agent it becomes operationally impossible that it rained. What was a possibility previously now becomes an impossibility.

After tomorrow we might ask the question "Was it possible that it *could have* rained?" This can be a subtle question of the use of language. The focus of this essay however is the best knowledge of the agent. Previously, the agent did not know if it would rain or not, and either outcome seems *possible*. Afterwards the agent knows that it does not rain and so rain is *impossible*. The agent's knowledge changes.

The question of whether or not, *objectively*, rain is possible, opens up many technical, scientific issues to do with quantum mechanics, chaos and modelling complexity. Is the weather truly indeterministic or is it deterministic? It is well known that weather is chaotic (in the technical sense of non-linear dynamics). In fact it was in modelling weather that chaos was first discovered. But chaos is merely unknowable in practice. Even a deterministic system can be chaotic. On the other hand, perhaps purely random quantum events affect the weather. The familiar saying that a butterfly moving its wings can affect a hurricane perhaps also applies to events at the very small scale of quantum effects. The precursors to probabilities in quantum mechanics are complex numbers. How do these correspond with "possibility" and "impossibility"? Could the many-worlds interpretation of quantum mechanics be adapted to the background of true objective possibilities? Added to all this there is the sheer complexity of modelling all the minute details of a weather system.

All these issues are important but they are not the focus of this essay, which remains "agnostic" on the issue of determinism and indeterminism. To cater for both possibilities *many* truly objective possible worlds will be allowed. If the world is deterministic then the number simply reduces to one (determined by previous states). So, on the one hand the weather might be truly deterministic and the inability to predict it results from chaos or just sheer information complexity. On the other hand the weather could be truly indeterministic, perhaps as a consequence of quantum mechanical effects, and perhaps it is *objectively* possible that it will rain tomorrow.

To accommodate indeterminism it must be allowed that objective knowledge can change over time, otherwise we have the following two inconsistent statements,

> It is possible it will rain tomorrow.
>
> It is not possible that it will rain tomorrow.

Suppose it is *objectively* possible that it will rain tomorrow, maybe because of quantum mechanical effects. Now *after* tomorrow, it has been observed that it did not rain, and the second statement is true. So it is impossible that

it rained yesterday. If indeterminism is allowed then statements of possibility must be couched in terms of time (even in the many-worlds interpretation of quantum mechanics this will occur as we "enter" different possible worlds). Therefore, the option is left open for indeterminism by allowing objective possibility to be time dependent,

> Before: The day before yesterday it was objectively possible that it rained.
>
> After: It did not rain yesterday and it is now impossible that it rained yesterday.

These sentences are not inconsistent because they are referenced at different times. In temporal modality statements are issued in different worlds which exist at different times. In this way, the time at which the statement is made is part of the modal statement.

It might seem then that the entire matter is settled. It is *time* which affects possibility. After all, if indeterminism is allowed, then operational possibility would seem to be essentially the same as objective possibility. There is no need to worry about operational possibility? But what about the case of a deterministic universe?

Yesterday's rain

Consider again yesterday's rain but this time with two agents. Suppose Meredith lives in another part of the world, say Canada, while Ludwig lives in a suburb of Melbourne, Australia. Suppose it did not rain yesterday in that part of Melbourne where Ludwig lives, and Ludwig knows this fact through direct observation. Meredith however has not had reason to look up the weather in Melbourne and is completely unaware of whether it rained or not.

The first thing to note is that objectively it did not rain yesterday. Secondly, Ludwig believes that it did not rain, and finally Meredith believes that it is possible that it did rain. For Meredith it is operationally possible that it did rain, even though it is objectively false (refer to Meredith t_2 in Figure 1). While they do not communicate, the beliefs of the two agents are compatible. Furthermore, Meredith's operational possibility does not lead to an inconsistency with objective reality because she also believes that it is possible that it did *not* rain in Melbourne (there is for her a possible world in which it did not rain).

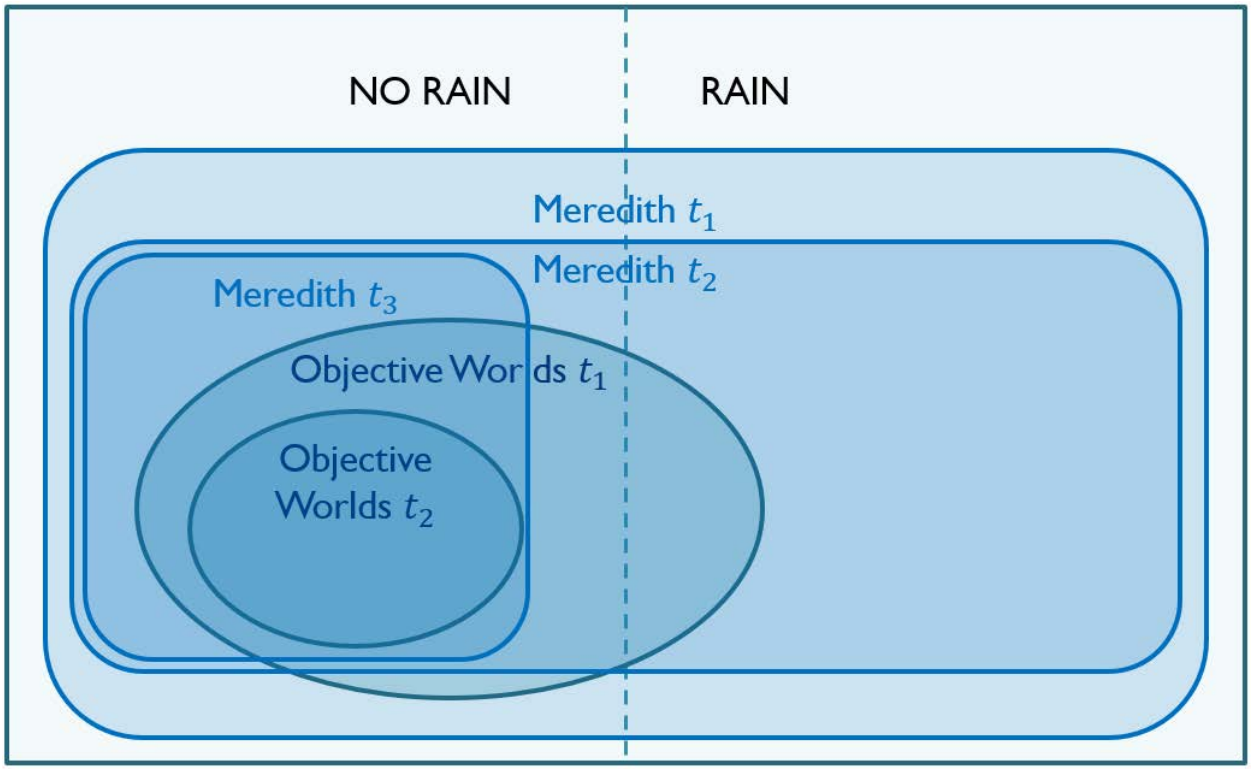

Figure 1

Suppose Meredith communicates with Ludwig and learns that it did not rain in Melbourne. Her belief set changes with more knowledge (Meredith t_3 in Figure 1). Importantly, it is *not* time which changes operational possibility, it is *knowledge*. Time may change objective possibility, but knowledge changes operational possibility.

Inferential statistics uses much the same logic. The population value does not change when the statistician rejects or accepts (technically, fails to reject) the null hypothesis. The statistician does make the null hypothesis true or false by their analysis. It is knowledge gained through sampling which affects the statistician's understanding of the world.

Now we could ask at what time the universe changed and rain in Melbourne went from being a true objective possibility to an objective impossibility. Ludwig may have had more certain knowledge than Meredith but perhaps his knowledge also lagged behind the objective impossibility. Perhaps it became *objectively* impossible for it to rain in Melbourne at 10 PM. Before 10 PM the weather conditions were such that there could still have been a shower between 10 PM and midnight, but after 10 PM not even the best possible conditions would produce rain (no matter how many butterflies flapped their wings in just the right way). However, Ludwig, not having this detailed information, himself might only became certain at 5 minutes to midnight, or perhaps even after he wakes up the next morning? Surely the information gained by real-world agents lags behind empirical events, even if only for a fraction of a second. This kind of thing would seem to apply to *any* given empirical event, even in the most indeterministic of all possible worlds.

Logicians and mathematicians often use hypotheticals in proof by contradiction. Is it possible that Colonel Mustard committed the murder in the library? No, because he was in the conservatory with Miss Scarlet at the time. The contradiction, assuming that one person cannot in two places at once, leads to the conclusion of a falsehood. As it is meant here, operational possibility is akin to this kind of hypothetical. It is possible that Colonel Mustard committed the murder, if we don't know that he has a water-tight alibi. If we are on the other side of the world then rain in Melbourne is a hypothetical possibility, until we have better information.

Different agent's belief sets can contain inconsistent beliefs about possibility, as long as they haven't communicated with each other, but it would seem that a single agent's beliefs should not be inconsistent. So for example, when Ludwig wakes up the next morning and observes that it did not rain, the possibility of rain is removed from his belief set. Later, when Meredith talks to Ludwig and learns that it did not rain, the possibility is removed from her belief set.

Football recording

Suppose Nick's favorite football team, the Saints, are playing Collingwood on the weekend. Collingwood are in good form and the Saints have, unfortunately, been playing badly. What is the objective possibility that they will win the game? What is the likelihood?

Suppose it is the day *after* the game and Nick has successfully avoided any "spoilers" and is unaware of the game's outcome. However, he has recorded the game and is about to sit down to watch it. What is the possibility that the Saints won the game? What is the likelihood? As he watches the recording Nick discovers that the Saints lost. Now what is the possibility that they win the game?

Having looked at the previous case, this example should be able to proceed more quickly. Let us first consider the objective world. There are deterministic and indeterministic possibilities; either the Saints were always going to lose or there was a time, presumably some time before the end of the actual game, when their loss went from being an objective possibility to a certainty.

Either way, in Nick's thinking as he watches the replay, it was operationally possible that they won. The agent, Nick, does not currently have the information needed to know either way. The information he needs is in the recording of the game. As he watches the recording he discovers, much to his chagrin, that they did not win and the operational possibility becomes a falsehood.

Again, it may be time that changes objective possibility, but it is clearly knowledge which changes operational possibility.

The coin toss

Now consider a slightly more complex example involving probabilities.

Frank is tossing a coin and is offering bets to Dean. Suppose for the sake of argument the coin toss is fair and the objective probability that the coin lands a head is 50%. Let us also suppose that the objective change from a 50%

probability to a certainty occurs over a small period of time and it occurs only at most a small period of time before the coin lands (so we will ignore issues of when the outcome is say 80% certain).

Now consider three separate cases.

> Coin toss 1: Before the coin toss, Frank offers odds of three to one on the coin landing a head. Dean considers this a good bet, using the odds of 50% in his calculations. In this case, the coin lands in plain view of both Frank and Dean, and the coin lands a tail. It would seem that before the toss, a head was possible with a chance of 50%, while after the toss it is impossible (false) with a chance of zero. It could seem that time has changed the knowledge of the agents.
>
> Coin toss 2: Now Frank tosses the coin but then covers it over with his hand so that neither he nor Dean can see it (assume that Frank has not cheated). Now Frank offers a second bet with the same odds as before, three-to-one, and again Dean considers this a good bet. Is it possible that the coin landed a head? They both eventually discover that the coin landed a tail.
>
> Coin toss 3: Next Frank tosses a coin and takes a look at the coin without showing Dean, although he makes it clear that he is looking at the coin. He covers over the coin and again offers a bet of three to one odds. Is it possible that the coin landed a head? Does Frank think it is possible? Does Dean think it is possible? What is the probability that Frank should assign to the chance that it is a head? Finally, Frank reveals the coin to Dean and it has landed a tail. How does this change the knowledge of the agents?

There are three coin tosses and three bets. The first coin toss is uncontroversial. It can be analyzed without referring to operational possibility because changes in operational and objective possibility are virtually simultaneous. We can argue however that Frank and Dean took some time to register the event (sight takes about a third of a second) but this seems perhaps a trivial point in this case.

The second example, however, must be analyzed using operational possibility. The coin has landed a tail, but because neither agent can see the coin, it is operationally possible for both agents that the coin came up a head, even though this is objectively impossible. Indeed, because of their lack of knowledge, Dean can still use the 50% probability in his calculation of the value of the bet, even though the event has already occurred. He would almost certainly make money over time accepting such bets. Operational possibility and operational probability can be useful in making decisions, hence the term "operational".

In the third coin toss the two agents have *different* views of the event. Frank knows that the coin landed a tail but still offers a bet of three-to-one. Dean thinks that it is possible that it landed a head although he is suspicious, because Frank has already looked at the result. Given competing interests of the players, Dean would be ill-advised to accept such a bet. It is unwise to use the 50% probability model for the bet, even though this might seem to be the most "objective" model possible.

As science advances various scientists, acting as agents, alter the combined pool of scientific knowledge. However, the veracity of any one scientist is not assumed. The statements of various scientists are examined and hoaxes such as Piltdown man are exposed and are excised, hopefully, from the body of shared knowledge. There is room for considering the relative knowledge of agents even in the most rigorous objective background, perhaps especially.

In a many worlds model, frames (sets of possible worlds) (Cresswell and Hughes, 1996; Carnielli et al., 2008) would become more restrictive, either over time or as more information is gathered. That is to say "later" frames would contain subset restrictions of former worlds. So if G_1 is a set of possible worlds at a given time, and G_2 is a set of possible worlds for the same agent at a later time then we would expect that $G_2 \subseteq G_1$ and further that the accessibility relation would be given by the restriction of the former accessibility relation. That is,

$$wR_2v \Leftrightarrow wR_1v$$

where w and v are worlds in G_2 and R_1 is the accessibility relation for the first frame and R_2 is the accessibility relation for the second. Since this is a subset relation, it is an ordering relation. Thus we could write $F_1 \succcurlyeq F_2$ where $F_1 = (G_1, R_1)$ and $F_2 = (G_2, R_2)$ are the respective frames and the ordering relation outlined above holds.

Suppose the objective possibilities at a certain time, if they exist, are given as O_t. We would expect that the frame of objective possibilities is more restrictive than any agent's frame, $F_t \succcurlyeq O_t$ where F_t is the agent's frame at the same time. Furthermore, any two agents should have overlapping frames, $F_{1,t} \succcurlyeq O_t$ and $F_{2,t} \succcurlyeq O_t$, where $F_{1,t}$ and $F_{2,t}$ are the frames of the two agents at the same time. Finally we would expect that the objective frame also becomes more restrictive over time, $O_{t_1} \succcurlyeq O_{t_2}$ where t_2 is later than t_1. This rule might need to change slightly for quantum mechanics, but the accommodation could no doubt be made. These then are the many-world rules that apply for *compatibility*.

A coin toss prepared earlier

Here is an operational possibility "that I prepared earlier". At 10:30 AM on Wednesday March 30th, 2005, I tossed a coin. Is it possible that it came up a head? What is the chance that it came up a head? I should add that in fact I tossed the coin just *after* framing the question and I did not "skew" the result.

At this point, without reading further down, it seems reasonable to say that there is a 50% operational possibility that the coin landed a head, at least for the reader. Once the reader has read to the bottom of the article their knowledge will change.

Drake equation

The Drake equation estimates the chance of life outside the solar system. It is a relatively simple equation which breaks down into a number of components to give at least a first-order estimation of the probability of life in outer space (excluding life on Earth). The Drake equation (Friedman, 2010) was popularized by Carl Sagan. Now, either there is life on other planets or there isn't. Should we be searching for life on other planets?

Whether or not there is life outside the solar system is pure conjecture. The Drake equation seems to indicate that there are many prospects for life but, as yet, there has been no evidence of life. In terms of objective possibility, either there is life in outer space or there is not. In terms of operational possibility, there may be life in outer space.

Even if there is a relatively low chance of discovering life outside the solar system, the modest expenditure required for a search by scanning the stars with radio telescopes is strategically defensible. Insofar as it assists in the decision to search for life outside the solar system the Drake equation is an estimation of the operational likelihood that there is life to find.

What perhaps makes this example slightly different to the previous ones is that the shared discovery of life outside the solar system would become a scientific fact, known at least by all serious scholars. We are assuming of course that such information would not be with-held by the "government" and studied in a secret facility, say, Area 51.

The results of Frank's coin toss are not universally known facts. They are facts that have relevance only for some agents in some circumstances. Other agents will quite happily be ignorant of such facts. The discovery of life outside the solar system on the other hand would quickly become universally shared scientific knowledge, at least on planet Earth.

Cold fusion

Joan is a researcher who has found a series of chemical reactions that appear to propel atoms together in close proximity, opening up the possibility of cold fusion. Is cold fusion objectively possible? Suppose she then produces some very sophisticated computer models which show the possibility of a nuclear fusion reaction in a simple chemical solution. How likely is cold fusion?

This is similar to the previous example. Unless it can be proven scientifically that it is impossible for a chemical reaction to produce fusion it must remain an open question whether some sort of "catalyst" might produce such a reaction. Again, it is either objectively possible or impossible. Barring proof otherwise, it is operationally possible.

Again, it might be not be a completely pointless exercise to attempt to produce cold fusion. On the other hand, at this point in time when weighing up the likely costs and benefits of the exercise, it is probably wise that huge resources are *not* spent on research into this question. The operational likelihood of cold fusion seems low. But again, the decision whether to engage in such research is dependent on estimations of operational likelihood.

The billionth digit of π

Suppose Carl is a mathematician who has written a computer program to calculate the digits of π. Suppose Henri is a colleague who is offering a bet that the billionth decimal digit of π is 6. What is the "probability" that the billionth digit is 6? If Henri offers odds of 12 to 1, is this a good bet?

Here we turn from empirical facts to logical facts. Now an agent's knowledge is inconsistent if it contains even just one logical contradiction. Logicians routinely use proof by contradiction to show that certain hypotheses should not be true: Colonel Mustard cannot be in the library and the conservatory at the same time. Inconsistency is a kind of logical filter. It might seem then that it is operationally useful to exclude logical inconsistency from

the belief set of an individual agent, just as it is operationally useful for a detective to exclude logical contradictions from their thinking once the facts are discovered. Indeed, this filter is assumed as part of the application of sound logical principles.

However, does it not seem that Carl could reasonably use the "randomness" of the digits of π to place a bet on the outcome of the computer's program? But the digits of π are not empirically determined; they are determined by mathematics. Mathematics is based in logic, and π has a logical definition. A mathematical fact is a logical fact. If the billionth digit of π is say 7 and *not* 6, then it is *logically inconsistent* to say that it is *possibly* 6.

If we look at this in terms of the agent's computational capacity then the billionth digit of π, as far as the agent is concerned, is possibly 6. The sheer complexity of the problem prevents Carl from discovering the billionth digit of π, at least not before his computer program has found the result. It is not the objective facts here which limit the agent's knowledge, it is the agent's ability to draw the logical conclusion from the facts.

Let us allow then that sets of beliefs can contain such contradictions. They can contain worlds with logical contradictions, as long as those contradictions are not yet discovered by the agent. Worlds would be excised once the agent discovers contradictions in them, as the agent's knowledge becomes "more certain" because of logical deduction. Such belief sets can still be usefully defined as compatible, and they can still be compatible with objective possibilities as the "most certain" of all possible worlds.

Perhaps there should be different terms for operational possibility that is internally logically consistent, and operational possibility that is "operationally consistent" but which allows internal inconsistency. Of course, the least restrictive case is the second, and this definition of operational compatibility is workable.

Some degree of depth to the consistency of the beliefs of a morally responsible agent might be expected. Sets of beliefs should not contain obvious and simple inconsistencies, but logical inconsistencies requiring enormous information processing power beyond the capacities of the agent seem reasonable. At the very least, the process of using logical deduction is seen as an "operational" one.

Finally, suppose the billionth digit of π becomes an important bet for a group of Carl's acquaintances. Carl sets up a special display to announce the billionth digit of π to the world. This display will no doubt be capable of displaying any of the digits 0 to 9, even though only one of these digits is truly logically possible as the answer. This display would then be evidence that these agents think that any of these digits is operationally possible.

The chess computer

Suppose Helen is playing chess against a computer. Suppose the game is at a stage where the subsequent moves in the computer do not depend on a "randomizer". Such randomizers are generally only pseudo-random in any case, but it simplifies the example if we assume that the moves are deterministic. Suppose it is the chess program's turn to move and it is deliberating on its move. For the sake of discussion let us say the chess computer is currently considering the consequences of "moving the pawn", but the move it eventually makes is "the knight move". Is the pawn move possible? Is the computer program making a choice?

Helen knows, we assume, that the computer's moves are deterministic. Thus she knows that both moves cannot be objectively possible, although she doesn't know which move the computer will make.

At first sight, it might seem that because the chess program's moves are deterministic and so the pawn move is "impossible". However, Helen needs to know all the details of the computer program if she is to predict the chess computer's move. And even if she has this information, it is doubtful that a human alone has the processing capacity to accurately perform in real time the calculations needed to predict the computer's move. The only practical way for her to make the prediction would be to run the exact same program on another computer (or even on the same computer at another time). It is feasible to do this but is this a "prediction"? Without such a "prediction" it would seem that, for Helen, both the pawn move and the knight move are *operationally* possible.

The possibility from the standpoint of the computer is undoubtedly problematical since the computer, we can suppose, does not make statements about the world. Nonetheless it uses logical states which eventually will result in chess moves. It considers for instance the "pawn move" and its possible outcomes. We could say that the pawn move is "considered" possible in the *algorithm* of the chess-playing program. There is a sense at least in which the pawn move is an operational possibility (note that optimization algorithms in general make selections from possible outcomes). Again, the pawn move is not an objective possibility, since the program is deterministic, but it is an option considered by the program.

Although the chess program's moves are deterministic there is no question of the computer itself "predicting" its own move when deciding which move to make. It is feasible to do this, perhaps, by running the program twice, once as a prediction and the second time as a choice, but this seems a hollow answer. Furthermore, operationally, the chess computer would be better off using any extra computational resource to provide a better chess analysis (assuming the method of looking ahead to a limited depth) and once this has been done the move has been potentially changed anyway! The sheer complexity of the move itself requires an information processing resource which makes "prediction" useless and operationally unsound.

If we take this line of reasoning and apply it to humans it becomes even more absurd. Computers are designed to follow logical rules deterministically, so we can predict what the physical computer does by following the computer's program. Now it is true that human brains process logic but they certainly do not do so deterministically. A human playing chess may be influenced by how their last meal affects their mood. The chemical makeup of their meal may produce slightly different chemical concentrations in the blood which then have a subtle effect on the agents thinking about chess. A glint of light out of the corner of your eye may affect one's concentration when considering a complex move. Brain processing is dependent on the details of the complex shape of tree-like growths of dendrites. Presumably estimates of the probabilities of human actions are affected by an immense number of small, complex, physiologically messy brain processes.

There are enormous difference between a human making a choice and a modern computer considering a chess move. How much more complex would the chess program example become if a prediction required a detailed physical model of all the electronic states in the computer? Computer circuits use electronic feedback so that the components can function reliably and predictably under a wide range of conditions (different temperatures, but also differences in the manufacture of components). We can imagine that there might be similar processes in brain events, but they are almost certainly not predictable, even in small details. Furthermore, there are many brain events running in parallel over wide areas in the brain while a computer just a few threads in parallel. Brain activity is much more complex and less "predictable" than a computer program.

At any one point in a game chess has only a small number of moves. Nonetheless processing the full minimax algorithm for chess (at the first move) lies well beyond the processing capacity of modern computers. The number of possible abstract chess games is enormous, roughly estimated to be in the vicinity of 10^{120} games. Computers must use heuristics to handle this complexity. And yet the brain is many times more complex, and is physically "messy". The complexity of just a moment's processing in the human brain, even if it were deterministic, is many, many orders of magnitude more complex. Human choices, even if they were deterministic are unpredictable in practice, and would seem so for the foreseeable future.

A coin toss made by the author

The coin came up a head.

Conclusion

The modality of operational possibility requires a minimum of theory based only upon a model of separate agents with limited knowledge. Technically the model presented here requires different sets of many-world frames which change both over time and with extra information. A simple subset relation between frames establishes a simple theory which distinguishes *compatibility* between frames from consistency within a frame.

This theory is the very minimum that takes account of the knowledge limitations of agents and is consistent with standard formal logic, but which is also general enough to cover determinism and indeterminism, relativism and realism, and yet still provide a coherent explanation of use of the modality of possibility in epistemological questions.

Everyday use of the term "possible" clearly employs operational impossibilities: for someone in Canada it is possible that it is raining in Melbourne, watching a replay of a football game an agent can entertain the possibility of either winning or losing. As argued above, the difference between the objective possibilities may involve the factor of time but it is clear that the change in the agent's knowledge is brought about by information. Even a coin toss landing in front of our eyes takes some time to be registered in the brain of the viewer. But, less controversially, someone in another place who is informed later about the coin toss clearly their views at a much later time.

This analysis is not an attempt at explaining all aspects of the modality of possibility directly as it relates to complex phenomena such as grammar, language or ethics. Ethical responsibility in particular depends on complex social factors. However, the distinction between operational possibility and objective possibility, and the theory about the relative knowledge of different agents, provides an epistemological element needed in these discussions.

The fact that temporal and operational changes to frames are modelled the same way suggests that there may be an equivalence with temporal logic. This could mean a more general form of the current model could be developed. On the other hand the subset model proposed here is extremely simple and would seem to be quite intuitive. It is also interesting to speculate how the model proposed here might accommodate a quantum-mechanical many-worlds interpretation. These are matters for further research.

This discussion has remained as non-technical as possible, and examples have been used to draw out the impact of the theory in various contexts, demonstrating that this form of possibility has value beyond a purely technical exercise.

With these caveats and qualifications, the distinction between an operational, "subjective" form of possibility and objective possibility is as valuable as the distinction between the "subjective" perception of the sound of a tree landing in a forest and the vibrations in the air that are caused by the tree's fall.

References

Berger, A. (2011) *Saul Kripke,* Cambridge University Press.

Berkeley, G. (1710) *A Treatise Concerning the Principles of Human Knowledge,* Jacob Tonson, London.

Carnielli, W., Pizzi, C. and Bueno-Soler, J. (2008) *Modalities and Multimodalities,* Springer.

Cresswell, M. J. and Hughes, G. E. (1996) *A New Introduction to Modal Logic,* Routledge, 11 New Fetter Lane, London EC4P 4EE.

Friedman, S. T. (2010) *Flying Saucers and Science: A Scientist Investigates the Mysteries of UFOs: Interstellar Travel, Crashes, and Government Cover-Ups,* The Career Press, Inc., 3 Tice Road, PO Box 687, Franklin Lakes, NJ 07417.

Øhrstrøm, P. and Hasle, F. V. (1995) *Temporal Logic: From Ancient Ideas to Artificial Intelligence,* Springer, P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

Wikipedia (2013) *Modal Logic,* http://en.wikipedia.org/wiki/Modal_logic, 20-Nov-2013, 2013.

Online tracking by social network sites: is there any hope after all?

Rath Kanha Sar

rsar@csu.edu.au

Charles Sturt University

Users' online movements can be tracked and recorded by numerous third party sites including advertisers, data aggregators as well as major social network sites (SNSs) such as Facebook, Twitter and Google (Sar & Al-Saggaf, 2013c). The tracking by SNSs appears to be worrisome because SNSs are able to acquire information about their users' online activities in addition to personal information voluntarily provided by them. Cambodian participants, interviewed by the researcher, were not happy with the tracking and expressed concerns over privacy loss. From the perspective of Contextual Integrity (Sar & Al-Saggaf, 2013a) and its decision heuristic (Sar & Al-Saggaf, 2013b), the tracking by SNSs violates users' right to privacy because this is happening without users' awareness and informed consent. Based on these findings, this paper discusses some existing and future measures that can be used to bring the change to the current issues of online tracking by SNSs.

The first aspect to be discussed is protection at the browser level such as regularly cleaning cookies and browsing histories, and using browser extensions in order to reduce the chance of tracking. Existing extensions such as AdBlock (Palant, 2013) and Ghostery (Ghostery, 2013) can be used to remove or block extraneous contents such as advertisements on the first party site pages, whereas Priv3 extension can protect users from the tracking by social network sites if users do not interact with those sites (Priv3, 2012). Unfortunately, these tools did not prove to be an effective solution to the problem because, for one reason, they did not completely eliminate the tracking (particularly by SNSs) and second, not many users are aware of online tracking, let alone of these tools (Krishnamurthy & Wills, 2006).

The second aspect to be considered is users' awareness and informed consent. As discussed in (Sar & Al-Saggaf, 2013b), the tracking violates users' right to privacy because SNSs failed to get their informed consent. In order to make an informed choice, users must know all the details involved in the information collection such as who have access to what information about them and how their information is processed or used once collected (Barocas & Nissenbaum, 2009; Krishnamurthy, 2013). However, online users are from different countries, background and cultures, and speak different languages other than English. Therefore, getting informed consent from online users worldwide and raising awareness about online tracking and precaution could be a hard work. Let us assume that users are aware of all of online tracking, and some users are enjoying targeted advertisements on their SNS profiles while some do not wish to be tracked (McDonald & Cranor, 2010a). Will SNS users be able to opt out of tracking by SNSs while still enjoying their online browsing?

A further aspect to be discussed is the involvement from related sites such as Facebook, Twitter and Google. It appears that they hold the power to make changes because they have control on the systems, and they understand the economic values of online tracking (Krishnamurthy, 2010; Gill et al., 2013). One possible option is those organisations can start to think ethnically by applying ethical guidelines or frameworks before making any decision to avoid negative impacts on the others involved in the business - e.g., online users and their privacy. However, eliminating online tracking can result up to 75% drop of advertising revenue for major players

like Google and Facebook (Gill et al., 2013), and this obviously affects advertising ecosystem as well as business trends. Are they willing to do this?

Another aspect to be discussed is the contribution from researchers across different fields under the interest of ICTs (e.g., technical, social, and philosophical) and the role of the media. Technical accounts of privacy report on the technical flaws that may impinge users' right (e.g., Krishnamurthy and Wills (2010); Humphreys, Gill, and Krishnamurthy (2010); Mayer (2011)) but do not explain why privacy matters whereas philosophical accounts of privacy (e.g., Moor (1997); Floridi (2005); Nissenbaum (2010); Tavani and Moor (2001)) are not empirically based. Meanwhile, the findings from social aspect of research that involved users' perspectives are also crucial to report on users' awareness and perception on how they manage their privacy online (Pempek, Yermolayeva, & Calvert, 2009; McDonald & Cranor, 2010b; Al-Saggaf, 2011). However, findings from different disciplines usually contain area-specific jargons that may be hard to understand among general audience or audience whose native language is not English. An option taken into consideration could be the simplification of language in reports and findings. In addition, a collaboration among researchers from these areas would be efficient in pointing out the technical flaws while also explaining how they may impinge on users' privacy, and while also reporting on users' awareness and concern over those flaws.

However, despite the facts that many researchers have contributed large amount of works into the area of online tracking, the findings are usually ignored by the publicity; hence the tracking is still happening and keep growing Krishnamurthy (2010). However, a Wall Street Journal article (Steel & Vascellaro, 2010) caused public breakouts and eventually triggered the response from Facebook founder about various privacy issues. Hence, both the researchers in ICTs and the media are seen to be effective in bringing the publicity's attention to the any issues brought by the technology and cause the change or response from the involved organisation like Facebook.

Last but not least, another aspect to be considered is the involvement from governments in designing and imposing policies and laws regarding the collection and secondary use of users' information. Privacy commissioner in Canada as well as the European Union, for example, have been concerned about privacy online and there is also a new proposed law that require first party sites to receive consent before placing a cookie on a user's computer in the European Union (Krishnamurthy, 2010). Again, this could be challenging because different cultures may hold different views regarding importance and value of privacy. Although Cambodian participants expressed concern over privacy loss from online tracking, comprehensive data protection or privacy law does not exist in Cambodia (Anonymous, 2012); hence, there is no restriction on data collected online.

Based on the rationales above, neither a single measure proves to work. For the changes to occur, it requires an on-going and long-lasting collaboration and involvements among different community of interests such as the first and third party sites, online users, ICT researchers across different fields (e.g., technical, social and philosophical) who may discover the issues overlooked by the responsible organisations, the media that helps to spread the words, and the government who holds the power to impose the laws and rules.

References:

Al-Saggaf, Y. (2011). Saudi females on Facebook: An ethnographic study. International Journal of Emerging Technologies and Society, 9 (1), 1 - 19. Retrieved from http://www.swinburne.edu.au/hosting/ijets/journal/V9N1/ vol9num1article1.html

Anonymous. (2012). Privacy law in cambodia. Cambodian Law Blog. Retrieved from http://cambodianlaw.wordpress.com/2012/04/04/privacy-law-in-cambodia/

Barocas, S., & Nissenbaum, H. (2009). On notice: The trouble with notice and consent. In Proceedings of the engaging data forum: The first international forum on the appli- cation and management of personal electronic information. Retrieved from http:// www.nyu.edu/projects/nissenbaum/papers/ED\ SII\ On\ Notice.pdf

Floridi, L. (2005). The ontological interpretation of informational privacy. Ethics and Information Technology, 7, 185 - 200.

Ghostery. (2013). Knowledge + control = privacy. Author. Retrieved from http:// www.ghostery.com/

Gill, P., Erramilli, V., Chaintreau, A., Krishnamurthy, B., Papagiannaki, D., & Ro- driguez, P. (2013). Follow the money: understanding economics of online aggregation and advertising. In Proceedings of imc 2013. Barcelona, Spain. Retrieved from http://www.research.att.com/~bala/papers/imc13.pdf

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

Krishnamurthy, B. (2010). I know what you will do next summer. SIGCOMM. Rev., 40, 65–70. Retrieved from http://doi.acm.org/10.1145/ 1880153.1880164 doi: http://doi.acm.org/10.1145/1880153.1880164

Krishnamurthy, B. (2013, June). Privacy and online social networks: can colourless green ideas sleep furiously? Security & Privacy IEEE, 11(3), 14 - 20.

Krishnamurthy, B., & Wills, C. E. (2006). Cat and mouse: content delivery tradeoffs in web access. New York, USA: ACM.

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

Mayer, J. (2011, August). Tracking the trackers: where everybody knows your username. Standford Law School: The centre for Internet and society. Retrieved from http:// cyberlaw.stanford.edu/node/6740

McDonald, A. M., & Cranor, L. F. (2010a). Americans' attitudes about internet behavioural advertising practices. New York: ACM.

McDonald, A. M., & Cranor, L. F. (2010b). Beliefs and behaviours: Internet users' understanding of behavioural advertising. Telecommunications Policy Research Conference.

Moor, J. H. (1997, September). Towards a theory of privacy in the information age. Computers and Society, 27(3), 27 - 32. Retrieved from http://www.site.uottawa.ca/~stan/csi2911/moor2.pdf

Nissenbaum, H. (2010). Privacy in context: technology, policy, and the integrity of social life. Stanford, California: Stanford University Press.

Palant, W. (2013). Adblock plus. Mozilla Firefox. Retrieved from https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/

Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students? social networking experiences on facebook. Journal of Applied Developmental Psychology, 30 (3), 227–238. Retrieved from http://linkinghub.elsevier.com/retrieve/ pii/S0193397308001408

Priv3. (2012). Add-ons: Priv3. Mozilla Firefox. Retrieved from https://addons.mozilla.org/en-US/firefox/addon/priv3/

Sar, R. K., & Al-Saggaf, Y. (2013a). Applying contextual integrity to the context of social networking sites tracking. In T. W. Bynum, W. Fleishman, A. Gerdes, G. M. Nielsen, & S. Rogerson (Eds.), Proceedings of the ethicomp 2013: The possibilities of ethical ICT (p. 413 - 418). Print and Sign University of Southern Denmark.

Sar, R. K., & Al-Saggaf, Y. (2013b). Contextual integrity's decision heuristic and social network sites tracking. Ethics and Information Technology, 1-12.

Sar, R. K., & Al-Saggaf, Y. (2013c, June). Propagation of unintentionally shared information and online tracking. First Monday, 18 (6). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4349/3681

Steel, E., & Vascellaro, J. E. (2010, May). Facebook, Myspace confront privacy loophole. The Wall Street Journal. Retrieved from http://online.wsj.com/article/ SB10001424052748704513104575256701215465596.html

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. Computers and society, 31(1), 6 - 11.

A survey of Australian ICT professionals' perceptions regarding the most common ethical problems they face in the workplace

Yeslam Al-Saggaf

School of computing and mathematics, Charles Sturt University, Australia yalsaggaf@csu.edu.au

Oliver Burmeister

School of computing and mathematics, Charles Sturt University, Australia

oburmeister@csu.edu.au

Introduction

Professionals in information and communications technology (ICT) face ethical situations in the workplace and need to deal with them effectively. Various attempts have been made to assist them. On the one hand, there have been attempts to educate professionals on how to conduct ethical reasoning (Simpson, Nevile & Burmeister, 2003; Al-Saggaf and Burmeister, 2012). On the other hand, there have been attempts to help professionals better utilise the codes of conduct of their professional society (Burmeister & Weckert, 2003; Bowern, Burmeister, Gotterbarn & Weckert, 2006; Burmeister, 2013). The present study, supported by the Australian Computer Society and the Australian Research Council, surveys ICT professionals in Australia about their perceptions regarding the most common ethical problems they face in the workplace.

Previous work

There are widespread unethical practices in the ICT industry (Aziz, Lokman & Yusof, 2012; Khanifar, Langaghi & Bordbar, 2012; Ethics Resource Center, 2012). In Europe, these include violation of intellectual property rights, breaches of data security and data protection, software bugs and moral damage, systematic discrimination, software flaws, inferior software quality and economic damage, engaging in conflict of interest, and unauthorised access (Van den Bergh & Deschoolmeester, 2010, p. 6). In Malaysia and Taiwan, the main ethical problems are negligence, broken promises, abuse of power, failing to follow guidelines, unfairness, absence of truthfulness, personal responsibility, and violating the 'Golden Rule', among other things (Sherratt, et al., 2005). In Australia, the main issues concerning unethical behavior in the ICT industry are compromising quality, engaging in conflict of interest, unprofessional behaviour, invasion of privacy, making false promises, copyright violations, spreading malware and virii, and compromising functionality (Lucas & Weckert, 2008, p. x). Lucas and Bowern (2007, p. 28), for example, found that 'compromising quality to meet deadlines' was the most important ICT issue then, constituting almost 55% of all cases, with 'compromising user requirements to meet deadlines' and 'compromising functionality to meet deadlines' neck-and-neck at almost 30%.

Method

Survey procedure

To answer the research questions, the study employed a quantitative survey that was implemented on the web. The survey questionnaire was administered using SurveyMonkey.com to allow the participants to fill the questionnaire and return it over the internet. The survey questionnaire was also administered online because of issues such as convenience, cost, time and accessibility. The survey questionnaire was informed by the results of a previous survey conducted by Lucas and Mason (2008) and also by the instrument they used.

All active Australian Computer Society (ACS) members (approximately 18,600) were invited to participate in the web-based survey by direct email sent to them by the ACS once on 12 September 2013. The survey was closed on 6 November after the response rate reached 12.4%. The online questionnaire was prefaced by the ethics consent sheet (including assurances of anonymity) and a description of the study. The questions comprised both closed ended and open ended questions. This paper focuses only on the component of the study relating to the most common ethical problems experienced by Australian ICT professionals.

Sample

A total of 2,315 participants completed the questionnaire. Out of the 2,315 respondents who participated in the study 84.5% (N=1940) were males, and 15.5% (N=356) were females. By age, 30% (N= 692) of the respondents indicated that they were under 35 years; 22.3% (N=516) indicated that their age fell between 36 and 45 years; 25% (N=576) said their age fell between 46 and 55 years; and 22.7% (N= 524) indicated that they were 56 years and above. According to the survey results, 33.8% (N=698) of the participants in the study described their occupational category as manager, 14.8% (N=307) said they were developers; 24.3% (N=502) indicated they were consultants and 13.3% (N=277) said they worked in technical support.

Analysis

The main question this analysis tried to answer is: which ethical problems were selected as the most frequently faced by ICT professionals? Since the question about the most common ethical problems allowed respondents to select more than once answer, a Multiple Response Frequency (MRF) analysis was judged to be the most appropriate analysis technique. In addition, cross tabulations were also performed to see if there are differences in responses based on geographical location and self described occupational category. The findings from the MRF analysis and the cross tabulations are summarised below.

Findings

With regards to the question: how often does unethical behaviour occur in the ICT workplace, the results of this survey revealed that 13.1% of the respondents indicated that unethical behaviour occur frequently in the ICT workplace; while 47.1% noted that it occurs occasionally with only 32.4% saying it occurs rarely. This suggests that 60% noted that unethical behaviour occur at least occasionally. This is different from the 85% result that Lucas and Weckert's (2008) study has found.

Of the 57 ethical problems listed for respondents to select, the MRF analysis revealed that 'Compromising quality to meet deadlines' (5.4%) was highest on the list of the most common

ethical problems experienced by ICT professionals, followed by 'Blaming others for own mistakes' (4.7%) and 'Compromising functionality to meet deadlines' (4.2%). Table 1[4] below provides more details. With the exception of 'Blaming others for own mistakes' ethical problem, this result is consistent with the Lucas and Bowern's (2007) finding suggesting the 2007 ethical problems are also major problems for ICT professionals in 2013.

	Responses		Percent of Cases
	N	Percent	
Unprofessional Behaviour	633	3.1%	30.3%
Conflict of interest	682	3.3%	32.6%
Compromising quality to meet deadlines	1,104	5.4%	52.8%
Compromising functionality to meet deadlines	846	4.2%	40.5%
Compromising user requirements to meet deadlines	632	3.1%	30.2%
Compromising security to meet deadlines or make things work	611	3.0%	29.2%
Blaming others for own mistakes	957	4.7%	45.8%
Bullying	630	3.1%	30.1%
Incompetence	750	3.7%	35.9%
Overworking staff	762	3.7%	36.5%
Total	20,368	100.0%	974.5%

Table 1: Ethical problems frequencies

An inspection of the results of the cross tabulations based on geographical location (see Table 2 below for more details) revealed that, with the exception of respondents in the Northern Territory and those Overseas, respondents in all other Australian states ranked 'Compromising quality to meet deadlines' as the highest on the list of the most common ethical problems in the IT workplace. For respondents in the Northern Territory and those Overseas 'Blaming others for own mistakes' was the highest on the list with 'Compromising quality to meet deadlines' as the second. In addition, with the exception of respondents in Tasmania and those overseas, respondents in all other Australian states selected 'Compromising functionality to meet deadlines' as the third most common problem after 'Blaming others for own mistakes'. For respondents in Tasmania 'Blaming others for own mistakes' was considered the third most common problem after 'Compromising functionality to meet deadlines'. Interestingly, for respondents outside Australia, the third most common problem was 'Conflict of interest'.

[4] Items with less than 3% were dropped from this table. Thus the percentages of items shown below do not add up to 100%.

State	Unprofessional Behaviour	Conflict of interest	Compromising quality to meet deadlines	Compromising functionality to meet deadlines	Compromising user requirements to meet deadlines	Compromising security to meet deadlines or make	Blaming others for own mistakes	Bullying	Incompetence	Overworking staff
ACT	78	78	118	100	86	72	107	80	89	86
NSW	189	202	329	249	183	170	307	199	219	228
NT	7	4	8	6	3	6	9	8	7	7
Qld	67	88	141	118	80	71	118	81	111	99
SA	34	34	75	45	39	39	55	28	40	39
Tas	13	11	19	18	8	16	14	10	15	13
Vic	167	162	275	208	152	161	231	149	176	201
WA	57	77	109	78	63	60	82	57	72	67
Overseas	18	23	26	21	16	13	31	14	18	20
Total	630	679	1100	843	630	608	954	626	747	760

Table 2: Ethical problems frequencies based on geographical location

The results of the cross tabulations based on self described occupational category (see Table 3 below for more details) revealed that, with the exception of respondents who described their occupation as 'Administrator' and 'Technical support', all other respondents ranked 'Compromising quality to meet deadlines' as the highest on the list of the most common ethical problems in the IT workplace. For respondents who described their occupation as 'Administrator' and 'Technical support', 'Blaming others for own mistakes' was the highest on the list with 'Compromising quality to meet deadlines' as the second. Moreover, 'Blaming others for own mistakes' was ranked second by Mangers and Consultants while to Developers 'Compromising functionality to meet deadlines' was the second most common problem. Respondents selected different problems as their third most common problem. While Developers and Educators[5] considered 'Blaming others for own mistakes' as the third most common problem, the administrator and technical support respondents ranked 'Overworking staff' as the third most common problem. Mangers and Consultants, on the other hand, selected 'Compromising functionality to meet deadlines' as the third most common problem.

[5] Those in education ranked also 'Conflict of interest' as their third most common.

Self described occupational category	Unprofessional Behaviour	Conflict of interest	Compromising quality to meet deadlines	Compromising functionality to meet deadlines	Compromising user requirements to meet deadlines	Compromising security to meet deadlines or make	Blaming others for own mistakes	Bullying	Incompetence	Overworking staff
Manager	223	228	372	267	209	182	303	196	240	246
Developer	73	66	146	118	76	83	109	77	97	90
Consultant	151	188	279	230	190	153	247	146	201	180
Administrator	34	38	54	37	28	49	60	36	42	53
Technical support	62	58	100	78	51	64	111	76	75	90
Education	44	50	51	38	22	27	50	43	35	44
Total	587	628	1002	768	576	558	880	574	690	703

Table 3: Ethical problems frequencies based on self described occupational category

Conclusion

The preliminary results confirm and extend earlier findings about the common problems faced in the ICT workplace in Australia. Unlike that previous work where the response rate was approximately 2%, this survey had a response rate of over 12%, giving further credence to the results obtained. The present study is ongoing, with further followup interviews and focus groups planned across Australia, to tease out the implications of the survey and to describe in detail how professionals interpret each of these major ethical problems. Furthermore, the study seeks to discover effective strategies that are currently being employed to address these problems. The study recommends surveying the Australian ICT professionals about their perceptions regarding the most common ethical problems they face in their workplace annually so as to plan effective strategies for solving them accordingly.

References

Al-Saggaf, Y., & Burmeister, O. K. (2012). Improving skill development: an exploratory study comparing a philosophical and an applied ethical analysis technique. Computer Science Education, 22(3), 1-19.

Aziz, A., Lokman, A., & Yusof, Z. (2012). Information Technology Ethics: The Conceptual Model of Constructs, Actions and Control Measure. International Journal On Computer Science & Engineering, 3(6), 2580-2258

Bowern, M., Burmeister, O. K., Gotterbarn, D., & Weckert, J. (2006). ICT Integrity: Bringing the ACS Code of Ethics up to date. Australasian Journal of Information Systems, 13(2), 168-181.

Burmeister, O. K., & Weckert, J. (2003). Applying the new software engineering code of ethics to usability engineering: A study of 4 cases. Journal of Information, Communication & Ethics in Society, 3(3), 119-132.

Burmeister, O. K. (2013). Achieving the goal of a global computing code of ethics through an international-localisation hybrid. Ethical Space: The International Journal of Communication Ethics, 10(4), 25-32.

Ethics Resource Center. (2012). 2011 National Business Ethics Survey

Khanifar, H., Jandaghi, G., & Bordbar, H. (2012). The professional and applied ethics constituents of IT specialist and users. European Journal of Social Science, 27(2-4), 546-552

Lucas, R., & Bowern, M. (2007). Ethics Survey: Haste sours quality in ICT. Information Age, June/July 2007, 28-30.

Lucas, R., & Mason, N. (2008). A survey of ethics and regulation within the ICT industry in Australia: ethics education. Journal of Information, Communication and Ethics in Society, 6(4), 349-363.

Lucas, R., & Weckert, J. (2008). Ethics and Regulation in the ICT Industry. Canberra: Centre for Applied Philosophy and Public Ethics.

Sherratt, D., Rogerson, S., & Fairweather, B. (2005). The Challenge of Raising Ethical Awareness: A Case-Based Aiding System for Use by Computing and ICT Students. Science & Engineering Ethics, 11(2), 299-315

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

Van den Bergh, J., & Deschoolmeester, D. (2010). Ethical Decision Making in ICT: Discussing the Impact of an Ethical Code of Conduct. Communications Of The IBIMA, 1-10. doi:10.5171/2010.127497

Fit for purpose?

Project Governance Models and Emergent Approaches to Software Development

Kelsey van Haaster,

Charles Sturt University

Kvanhaaster@csu.edu.au

Abstract

The rapidly increasing rate of adoption of value based, Agile approaches, amongst organisations involved in the commercial development of software has resulted in the emergence of new models of software development governance. But the rate of awareness and adoption of APM (Agile program management) by organisations has lagged behind the adoption of the methodology. Whilst organisations have embraced the concepts of lower project failure rates and reduced times to market, they have struggled to integrate the changes to organisational cultures and governance models that Agile demands. Whilst some organisations have adopted Agile methodologies at an organisational level, most have not, leading to significant challenges for those tasked with delivering Agile projects. This paper identifies some of reasons why this is so difficult and proposes one possible approach to gaining a better understanding of the problem.

Introduction

Good governance is important in many areas of business and that includes new and emerging areas of business information systems. Governance, as an area of ethical discussion, has been addressed in various settings at both national and international levels [1, 2] and has recently become a key topic for discussion as a result of the emergence of Agile approaches to software development. Since the publication of the Agile Manifesto [3] the adoption of Agile software development methodologies has had a significant impact on the way software is developed; particularly within the commercial software development sector, which has been moving away from the use of plan driven methodologies at an increasingly rapid pace [4]. As the rate of adoption of Agile approaches and techniques by software teams within commercial organisations accelerates, questions have arisen about whether the well understood project governance models are still fit for purpose and meet organisational needs [5].

Project Governance Models

Regardless of its domain and the project governance model being applied, the discipline of project management defines success in three dimensions; a product delivered on time, within a fixed budget and which includes functionality defined by the business. This definition assumes that the business is able, (in advance) to accurately define the right functionality, such that the detailed requirements and the time and resources required to develop the product can be specified. Further, it is assumed that it is possible to accurately record this information in a plan and, once the project is underway, track progress against that plan [6]. This leads to the underlying premise of project management, that the effort required to deliver a project is reliably estimable regardless of the product or service to be delivered.

Project Governance Models and Software Development

The result of these assumptions is that the software development project manager has an unenviable task, regardless of the software development methodology being used to facilitate delivery of their project. The essay, The Tower of Babel Did Not Fail [7] discusses the challenges associated with attempting to succeed at something, which (historical evidence suggests [8]) has around a 70% chance of failure. This essay argues that software development projects are distinctly different to civil engineering projects in several fundamental ways. Some of the key differences are that there are few known or fixed variables, such as the strength of materials, or the impact of gravity and that much of what is developed is completely novel to those developing it. In particular, software

products are expected to be modifiable, scalable and reliable, over an unspecified period of time and regardless of the domain and environment in which they are asked to operate.

Agile Approaches as a Response

In response to the challenges described above, the development of iterative and incremental approaches to software development [8] and the development of formal *software development governance* (SDG) models [9] have been credited with some modest improvements to the dismal success rates of software development projects. More recently however, in his discussion of the 2012 Standish, CHAOS report [10] Mike Cohn, claims that use of Agile methodologies (rather than those classed as iterative and incremental) offer even greater advantages, with reported success rates for Agile software development projects of up to 42% [11]. This has led to an increasing number of organisations; (up to 83% of those surveyed in the VersionOne 7th Annual State of Agile Survey) experimenting with or formally adopting Agile approaches to the implementation of software development projects. This represents a significant increase since the 2011 survey which reported that 59% of organisations were considering Agile approaches [12].

Agile is first and foremost a value based approach to software development [3]; as a result, projects are change driven; meaning that the right functionality delivers the highest business value to project stakeholders within a fixed time period. Agile projects do not attempt to predict the time and cost of developing a particular feature until enough is known about the feature to do so. The only fixed variable in an Agile project is time; the scope of the project being defined by the functionality which can be delivered within the time. This is not to suggest that Agile projects do not include detailed planning, they do, it is just done very differently [13]. There are examples of organisations which have adopted Agile values and approaches at all organisational levels, such as Cisco Systems [14], and where the structures and reporting requirements of the organisational governance models are aligned to consume the metrics produced by Agile projects, however these are a minority. 52% of the Version One State of Agile Development Survey respondents cited that the biggest challenge to adopting Agile was an inability to change organisational culture [15].

For project managers reporting on Agile software development projects within the context of traditional (*tayloristic*) governance and reporting structures, a significant challenge remains specifically around the questions:

1. To what extent do the measures and metrics produced by Agile software development projects meet the needs of project managers using them for reporting purposes?
2. Should, as a result of any perceived shortcomings in 1, modifications be made to the metrics produced by the Agile software development project?

A proposed approach

Direct comparisons between the performance metrics afforded by Agile and traditional software projects are difficult due to their dissimilarity. However, the lens of symbolic interactionism [16] may provide an approach through which to view the set of project artefacts that form the inputs to formal project governance models and form a comparison. Such artefacts include; planning tools, progress and status reporting tools, as well as any tools or techniques used to record, calculate and communicate project metrics. They exist in both Agile and in traditional software development projects, but take different forms.

Artefacts in Traditional Projects

The artefacts found in traditional projects, usually take the form of documents. Each document is a symbolic representation of the body of work done by the project team. Specifically, project governance artefacts such as, the project charter and the project plan, define the phases of the project. Others, such as Gantt charts, status reports and change requests, serve to both measure progress and maintain a shared history of decisions made and the reasons behind them. Taken together, these artefacts represent the shared vision of a project and tell the story of discovery that leads to the vision [17].

Artefacts in Agile Projects

Methodologically strict Agile projects eschew the production of lengthy formal documents [3]; preferring instead artefacts which are just sufficient to record conversations between the developer of a product and the client. Project progress is measured by the delivery of working software, deemed to be of high business value to project stakeholders; changes, which arise from early feedback, are sought after and welcomed.

A major premise of symbolic interactionism is that symbols are interpreted based on their context [18] taking this perspective allows us to ask; can Agile software development project artefacts be reinterpreted in order to provide

an answer to the question; is this project performing in a way consistent with that expected by the business running it?

Conclusion

The issues raised in this paper, touch on just a few of many unanswered questions about how the use of Agile methodologies to deliver software development projects can best coexist within organisations which employ formal approaches to project governance [19]. If Agile, as an approach to software development continues to deliver improvements to the success rate of commercial software projects, perhaps the most important question to ask is: Should we be re-examining our existing models of software development project governance in response to this emergent approach?

Ethical Aspects of Controlling Information Disclosure on Social Networking Sites

D Pallegedara, M Warren and D Mather

School of Information and Business Analytics, Deakin University, Australia

Email: dpallege@deakin.edu.au; matthew.warren@deakin.edu.au; dineli.mather@deakin.edu.au

ABSTRACT : *Inadvertent disclosure of information is a key concern for organisations, especially in an era of social media. 'Inadvertent' is accidental disclosure, rather than deliberate disclosure of information. Social media is considered to be a challenging channel for the information disclosure to be happened due to the ubiquitous usage of mobile devices to access social networks. Acceptable social media policies in organisations may assist the employees to improve their decision making behaviours as well as a controlling mechanism to mitigate the issue of disclosure. This paper discusses the ethical aspects of controlling information disclosure on Social Networking Sites.*

Keywords: information disclosure, inadvertent, social networking sites, ethics

INTRODUCTION

People tend to talk about their personal and work life within a community of their friends in social networking sites (SNS) such as Facebook, Twitter, and LinkedIn etc. Nevertheless, the conversation that was once intimate is available for public domain, indexed by Google and archived for some time or permanently accessible in a virtual space via a search engine (Schneier, 2009). A status update may contain a company secret or information about an upcoming launch and these mistakes by employees could cause havoc to the entire organisation. Careless or accident use of social media may often cause a wide range of negative impacts to an organisation in terms of financial loss, productivity loss, reputational harm, erosion of competitive advantage, potential lawsuits, legal penalties and malware risks (Gudaitis, 2010; Colwill, 2009; Young, 2010).

Many media reports reveal that organisations face incidents where employees inadvertently disclose confidential information and corporate secrets on social networking sites. The chief technologist and interim vice president of engineering for HP's new cloud services business, accidently posted the plans for HP's upcoming cloud computing, networking and storage services, shared management services on his LinkedIn page in advance of the company's official news release in 2011 causing damage to the company's reputation and giving advantages to their competitors (Braga, 2011). In 2012, Reuters reported that a well-known retail company called Francesca's Holdings Corp -fired their Chief Information Officer for improperly leaking company information via social media (Reuters, 2012). Multinational companies such as Google and AOL have incurred reputational damages due to inadvertent postings of sensitive information on websites and some companies have found their internal information and intellectual property details were posted on blogs, YouTube, MySpace, etc without gaining permission (Claburn, 2007; Olson, 2006). Incidents of disclosure are often reported in media and the above mentioned examples are just to name a few.

Disclosure occurs not only in social media but also through the use of information and communication technologies and traditional forms of communication such as face-to-face conversations, documents, file, servers, printing facilities, and portable data services (Ahmad

et al., 2005; Molok et al., 2011; CISCO, 2008). However, social media is the most powerful channel of disclosure when considered with other forms of communication channels (Gudaitis, 2010). Ubiquitous nature of social media makes it difficult for the users to draw a true boundary between work and personal life and that leads them to share personal and business information with a trusting attitude (Colwill, 2009). As a result, organisations are concerned about disclosure of information through social media (Gaudin, 2009; Wilson, 2009) .

Information disclosure is now becoming a social media crisis in the modern world (Desouza, 2006). Disclosure occurs when information such as client confidential details, competitively sensitive knowledge, corporate strategies, internal policies, production processes, profitability, etc disclosed to unauthorised parties (Anand and Rosen, 2008). Disclosure can occur deliberately by a disgruntled employee or inadvertently due to human error but the latter is potentially regarded as difficult to control (Hoecht and Trott, 2006). 'Inadvertent' is the accidental and unintended disclosure rather than deliberate disclosure of information. However, the real concern is when employees start sharing information about the meetings they are having and what customers they are dealing with regardless of the respective audience listening to the conversation shared on social media (Braga, 2011). If this particular information is seen by an ordinary person who has no interest in this regard, there is no harm but when it comes to a potential competitor of the company, then there is a potential issue to consider.

The focus of this discussion paper is to discuss the ethical aspects of controlling information disclosure on social networking sites. The authors discuss social media policy development as a controlling mechanism and the ethical considerations in implementing these guidelines in organisations.

SOCIAL MEDIA POLICY DEVELOPMENT AS A CONTROLLING MECHANISM

Organisations both large and small, government or private agencies have established mechanisms to control this problem while relying on technical controls, information security policies, security education, training and awareness (Molok et al., 2010). The majority of the research conducted in this specific area has typically focused on technology enabled information security measures such as computer and network security, privacy controls, encryption, firewalls and intrusion detection systems to control the disclosure of information. The security based mechanisms work well in some channels where disclosure occurs but these approaches do not work in the same success level for inadvertent disclosure through SNS. Some literature sources allude to the fact that a security-oriented process is not sufficient and the protection mechanism should be implemented in order to manage employee behaviour, conduct and incentives (Gold et al., 2001). Information systems literature emphasises the advantage of information security policy and practices, awareness training and strategies as a possible solution to mitigate disclosure and academic researchers recommend that the awareness of information leakage and its routes could mitigate this issue (Straub et al., 2004; Workman and Gathegi, 2007). Some researchers suggest that introducing information security policies and practices to an organisation, in effect, is influenced by organisational, environmental and behavioural factors.

Practically, it would be difficult to censor or limit what people write on social media and companies find it challenging (Broughton et al., 2011). As stated by Molok et al., mitigating information disclosure on SNS is about influencing the decision-making behaviour of employees and academic literature suggest that organisations can mitigate this problem by tackling the root causes of the problem and by changing employees' attitude towards SNS use (2011). Hence, information systems security management literature proposes policy development as an effective controlling mechanism compared to technical and legal controls

(Bulgurcu et al., 2010; Theoharidou et al., 2005; Workman and Gathegi, 2007). Hence, the authors believe that implementing acceptable social media use policies is the foundation for controlling inadvertent disclosure through social media in a corporate environment. Having said that, a company can have a social media policy framework to draw a boundary where company secrets are protected within the boundary.

ETHICAL ASPECTS OF SOCIA MEDIA POLICY GUIDELINES

The disclosure of information has been in focus for several years but emerging social media tools plus mobile devices make matters worse due to the boundless sharing of personal and business information on social networking sites (Colwill, 2009). Human behaviour is difficult to manage in terms of social media usage by employees because of the easy access to personal devices during office hours (D'Arcy and Hovav, 2009). In fact, many organisations point out the need for a more inclusive in defending their critical information assets as well as solutions for information governance by developing proper social media policies.

Emerging social media applications used at work and home with the increased improvements in the mobile technology create difficulties for the employees to have a true boundary between work and home life (Colwill, 2009, Molok et al., 2011). Mobile technologies and their compatibility in accessing social media make it more challenging for organisations to monitor employees' social media misuse due to the popularity of using mobile devices (Everett, 2010, Molok et al., 2010, Young, 2010). For example, even if an organisation restricts the use of social media during work hours using security mechanisms, the users would still be able to login to social networks through other devices such as mobile devices (Molok et al., 2010). The issue is even though the systems forbid the usage of social media; employees would still find other ways to access their personal devices. These characteristics of social media may pose ethical challenges for both employees and the organisation in terms of professional and personal use.

After conducting a preliminary content analysis of publicly available social media policy documents of 20 organisations in Australia, the authors identified several gaps in the current social media policies in organisations. The sample was chosen from four different industries: Australian Federal Government, Australian State Governments, Australian Universities and a sample from the Australian Stock Exchange 100. According to the pilot content analysis, many organisations allow reasonable personal use of social media during work hours. In particular, few organisations have differentiated the boundaries between personal, professional and official use of social media. In most cases, the policy applies only if a person mentions the organisation's name or makes references to related issues of the organisation in his/her personal use of social media. Some organisations have restricted the use of social networking during work hours whereas others monitor the access to social networking sites for reasonable personal use. Simultaneously, most policies do not address the personal use of computers, tablets, mobile and any handheld devices. Nonetheless, it is mentioned that personal use of social media should not interfere with employees' work performance nor hinder productivity. Also, employees' act of disclosing company information is considered to be an ethical issue in the first place.

Some scholars argue that information disclosure can be addressed by professional ethics, social control and legal instruments whereby addressing professional ethics in social media policies. However, the question is to what extent a social media policy can control employees' behaviour in relation to their personal use. Social media surveys indicate that employees' most preferable device to access SNS is the smartphone. The Yellow Pages social media report (2013) discovered that 22% of Australians use social media during breaks and 12% during work hours and smartphones are the most popular device to access social media. Hence, the following

questions arise when considering the ethical aspects of controlling employees' behaviour in the workplace.

1. Is it ethical to use your own personal device during office hours?
2. Is it ethical to control employees' usage of personal devices to access social networks during office hours?
3. Is it ethical to control employees' social networking activities after office hours?

As a result, organisations develop social media policies to provide acceptable use policies to clarify corporate ethics. However, social media-based employee behaviour control may raise several ethical issues. One ethical issue involves accessing social networking sites using personal devices during office hours. Another related ethical issue involves accessing social networking sites after working hours. The concern is whether it is possible to control people's behaviour outside work hours. The fact is that companies cannot restrict employees' personal usage of social media although they could disclose confidential company information using their personal accounts. Social media policy may provide guidelines on acceptable use of SNSs using personal devices during work hours but the ethical concern is whether the policy could impact the employees' personal usage after working hours.

Furthermore, employees' irresponsible use of social media, either professional or personal use may expose privacy and integrity risks in an ethical perspective. The challenge in developing a social media policy is to clarify acceptable use of employees' personal and professional use of social media without limiting their freedom of speech. Hence, an organisation needs to provide guidance to address these ethical aspects when implementing a social media policy in regards to employees' personal use and professional use while complying with other organisational policies and ethical standards. It is also important to understand the ethical role of social network providers (e.g. Facebook) to play in controlling information disclosure because in most situations the users do not have a control over SNS but the users have a control over their own behaviours.

CONCLUSION

Proliferation of social media brings new challenges to organisations and its employees. Out of many challenges associated with social media, information disclosure is becoming a potential risk for many organisations. While some organisations develop controlling mechanisms, many organisations do not have formal policies on social media use. Although there is a social media policy is put in place, the ethical dilemma of having some controls on employees is not properly discussed in the current research space. Therefore, future research will continue to examine the ethical issues of controlling employee behaviour in a social media context.

REFERENCES

Ahmad, A, Ruighaver, AB & Teo, WT 2005, 'An Information-Centric Approach to Data Security in Organizations', in *TENCON 2005 2005 IEEE Region 10*, pp. 1-5.

Anand, V & Rosen, C 2008, 'The ethics of organizational secrets', *Journal of Management Inquiry*, vol. 17, no. 2, pp. 97-101.

Braga, M 2011, *Can't stop the tweet: the peril—and promise—of social networking for IT*, arstechnica retrieved 15.03.2013 2013, <http://arstechnica.com/business/2011/10/cant-stop-the-tweet-the-periland-promiseof-social-networking-for-it/>

Broughton, A, Higgins, T, Hicks, B & Cox, A 2011, *Workplaces and Social Networking: The Implications for Employment Relations*, The Institute for Employment Studies, Brighton, UK.

Bulgurcu, B 2010, 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness', *Women*, vol. 221, no. 243, p. 243.

CISCO 2008, *Data Leakage Worldwide: Common Risks and Mistakes Employees Make*, Cisco Systems Inc, San Jose, CA.

Claburn, T 2007, *Minor Google Security Lapse Obscures Ongoing Online Data Risk*, Information Week: The Business Value of Technology, retrieved 19.09.13 2013, <http://www.informationweek.com/minor-google-security-lapse-obscures-ong/196902585>.

Colwill, C 2009, 'Human factors in information security: The insider threat – Who can you trust these days?', *Information Security Technical Report*, vol. 14, no. 4, pp. 186-96.

D'Arcy, J & Hovav, A 2009, 'Does one size fit all? Examining the differential effects of IS security countermeasures', *Journal of business ethics*, vol. 89, pp. 59-71.

Desouza, K 2006, 'Knowledge Security: An Interesting Research Space', *Journal of Information Science & Technology*, vol. 3, no. 1, p. 7.

Everett, C 2010, 'Social media: opportunity or risk?', *Computer Fraud & Security*, vol. 2010, no. 6, pp. 8-10.

Gaudin, S 2009, *Study: 54 percent of companies ban Facebook, Twitter at work.*, September 12, 2012, Computerworld, <http://www.wired.com/business/2009/10/study-54-of-companies-ban-facebook-twitter-at-work/>.

Gold, AH, Malhotra, A & Segars, AH 2001, 'Knowledge Management: An Organizational Capabilities Perspective', *Journal of Management Information Systems*, vol. 18, no. 1, pp. 185-214.

Gudaitis, T 2010, 'The Impact of Social Media on Corporate Security: What Every Company Needs to Know', <http://www.cyveillance.com/>.

Hoecht, A & Trott, P 2006, 'Outsourcing, information leakage and the risk of losing technology-based competencies', *European business review*, vol. 18, no. 5, pp. 395-412.

Molok, NN, S, C & A, A 2010, 'Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats', paper presented to 8th Australian Information Security Management, Edith Cowan University, Perth Western Australia, <http://ro.ecu.edu.au/ism/93/>.

Molok, NN, Ahmad, A & Chang, S 2011, 'Exploring The Use of Online Social Neworking By Employees: Looking At The Potential For Information Leakage', paper presented to 15th Pacific Asia Conference on Information Systems, <http://aisel.aisnet.org/pacis2011/138>.

Olson, P 2006, *AOL Shoots Itself In The Foot*, Forbes, retrieved 19.09.13 2013, <http://www.forbes.com/2006/08/08/aol-internet-update-cx_po_0808privacy.html>.

Reuters 2012, *Francesca's fires CFO for leaking info on social media*, retrieved 18.03.2013, <http://www.reuters.com/article/2012/05/14/us-francescas-idUSBRE84D0T820120514>.

Schneier, B 2009, *Special Report: Industry experts debate social networking risks* Security Asia retrieved 08.04.2013, <http://security.networksasia.net/content/special-report-industry-experts-debate-social-networking-risks>.

Straub, D, Rai, A & Klein, R 2004, 'Measuring firm performance at the network level: A nomology of the business impact of digital supply networks', *Journal of Management Information Systems*, vol. 21, no. 1, pp. 83-114.

Theoharidou, M, Kokolakis, S, Karyda, M & Kiountouzis, E 2005, 'The insider threat to information systems and the effectiveness of ISO17799', *Computers & Security*, vol. 24, no. 6, pp. 472-84.

Wilson, J 2009, 'Social networking: the business case - [IT internet]', *Engineering & Technology*, vol. 4, no. 10, pp. 54-6.

Workman, M & Gathegi, J 2007, 'Punishment and ethics deterrents: A study of insider security contravention', *Journal of the American Society for Information Science and Technology*, vol. 58, no. 2, pp. 212-22.

Yellow Social Media Report, 2013, Yellow Pages.

Young, K 2010, 'Policies and procedures to manage employee Internet abuse', *Computers in Human Behavior*, vol. 26, no. 6, pp. 1467-71.

Who is looking at myCloud - Angels or Demons?

Abayomi Baiyere

Turku Center for Computer Science, University of Turku, Finland.

Information Technology Trends

There are observable trends recently in the domain of information technology, which are triggering different issues worthy of ethical consideration. Some notable current trends are highlighted below and subsequently discussed in this paper.

- The pervasiveness of SoCloMo[6]
- The Big Data and Data Analytics race
- Ownership dilemma of Ecommerce transactional data
- Data Security and Trust – the Snowden saga

The pervasiveness and increasing popularity of *social media, cloud computing and mobile devices* have brought along with them the issue of data privacy among other ethical concerns. This trend now sees more people generating data on-the-go via mobile, sharing data freely to potentially thousands/millions of people via social media and storing vital data in the cloud without having any clue where on the planet the server is located via cloud computing.

Big data and data analytics have become one of the recent buzz in the information technology world. The promise of amazing insight and value that can be achieved via these advances in IT has led many organizations to aspire and consciously aim at gathering as much data from as many outlets as they can. In contrast to point one above where the main actor are the users who are by themselves generating all the SoCloMo data by their freewill, the Big Data view has the organization as the primary actor pushing for the generation and acquisition of data.

With the increasing popularity of *ecommerce*, businesses are eager to utilize any available opportunity to know more about their customers. Every data collected about an individual's transactional activities are considered mini gold mines. The underlying principles driving the ecommerce model is the notion that the better you know your customers the better you can better customize your offerings and position your products to motivate the customer to engage in business with you. The challenge however is the ownership debate about who really owns the data generated about the user. Additionally, the question remains as to what extent the data about a user can be utilized?

Furthermore, the issue of the *security* of the data stored by a user with an external provider remains a grey area particularly as it relates to the *trust* vested in these providers. This is even moreso with the recent Snowden revelations which largely diminished the level of trust associated with many top IT companies. This has ushered in an increasing awareness about the issue of the security and trust associated with the storage and collection of data from the users' perspective.

[6] SoCloMo - Social Media, Cloud Computing and Mobile

In this paper, we position *myCloud* conceptually to firstly describe the data generated by a user which is stored externally and secondly as data generated and stored about the user by other actors, all in the digital space. From the foregoing, *actors* involved in this discussion about the creation, access and utility of myCloud can be categorized into four. These are:

- Users – the subject of the data and who can also be the data creator.
- Businesses – the facilitator for the creation and/or the creator of the data.
- Governments – the mediator, regulator and/or policy maker.
- Others – external parties, hackers, friends…

Ethical Challenges

While most of the trends highlighted above are driving forces advancing the increasing generation of myCloud data, the ethical challenges surrounding such user generated data tends to be sources of hesitation to these trends (see figure 1). Some of the ethical challenges and questions about myCloud data include:

- Ownership – Who owns the data? The subject or the facilitator of the creation of the data? (Users versus Business?)
- Privacy - Who has access to what part of myCloud? Just the user, those the user willingly shares with, the businesses, the government, or other actors?
- Utility – How is myCloud data used? For commercial purposes or non-commercial, to study the user as an individual or as part of an aggregate group?
- Data life – Can a user truly terminate the existence and use of his/her data/digital life?

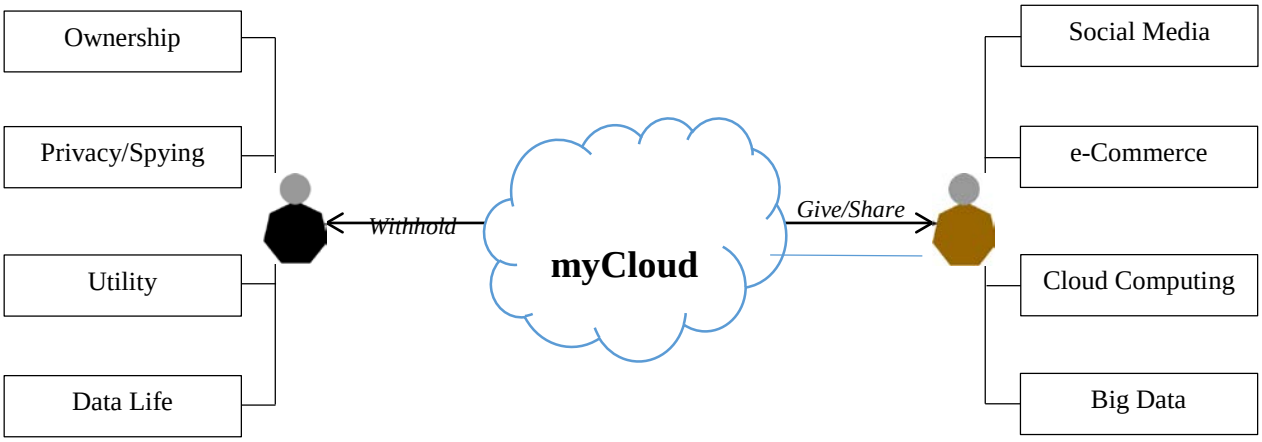

Figure 1: A framework showing trends *for* and challenges *against* the evolution of user data.

Scenario Model – myCloud User Options

Considering the unanswered questions and open ethical issues in the discussion about user data, it is logical to expect that there would be different possible stands a user can take. Due to the interlaced nature of the generation and utility of the data by both the user and the underlying technology/business, the users' eventual stand can be largely influenced. Based on the social, economic and technological relationship in the mix, four likely scenarios can be deduced. These are: the *phobia*, *transparent*, *compromise* and the *generous* scenario. These four scenarios are illustrated in four quadrants in the model in figure 2.

Phobia Scenario: This is a scenario that typifies what we call the 'Snowden model'. In this scenario there is a complete lack of trust in most providers of facilities that enable myCloud either via social media, ecommerce, cloud computing (file storage, email…) among others. This

is a possible scenario when users consider that they are either being socially manipulated or they realize that supposed privacy agreements have not been honored either for profit or other reasons.

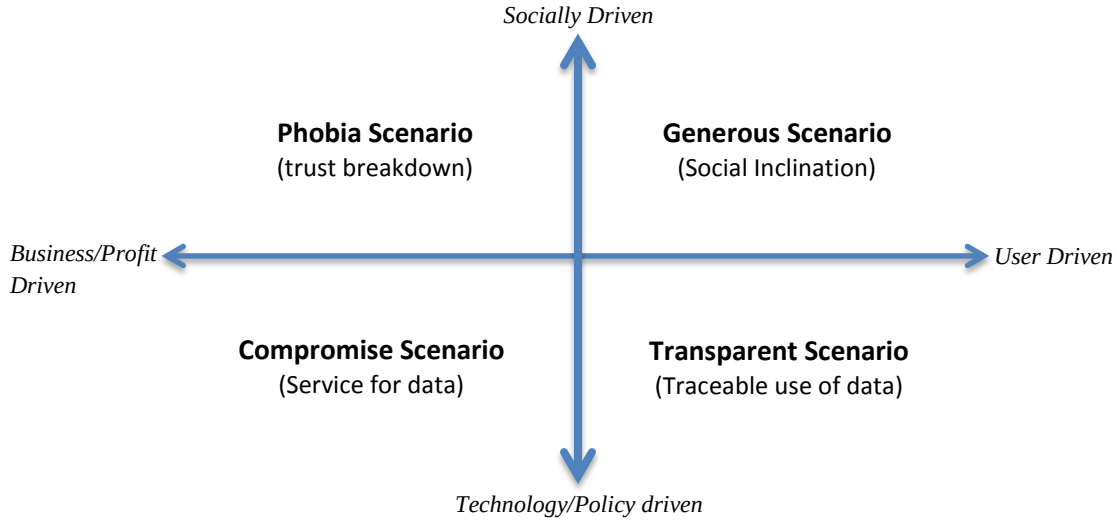

Figure 2: A scenario model of possible user options

Compromise Scenario: In this scenario which we have tagged the 'Google model', the myCloud setup is driven by business and technology decisions that have been laid out such that users have to provide their data to be able to utilize the service offered by the technology.

Transparent Scenario: For this scenario, the users are the key drivers. This is a sort of 'Privacy Respect model' where the user has the right, the power and the necessary facility to monitor the data generated about him/her and also possesses good control over the usage of data where he/she is the principal subject.

Generous Scenario: This is a scenario patterned after the 'Facebook model' where users although users are aware of the privacy loopholes and ethical issues, they nonetheless still willingly provide data about themselves and allow the generation and use of such data.

Ethical Issues of Cloud Computing Use by SMEs

Ishan Senarathna[1], Matthew Warren[2], William Yeoh[3] and Scott Salzman[4]

School of Information and Business Analytics, Deakin University, Australia
[1]ishan@deakin.edu.au
[2]matthew.warren@deakin.edu.au
[3]william.yeoh@deakin.edu.au
[4]scotts@deakin.edu.au

ABSTRACT: *The ethical issue has been a controversial and much disputed subject within the field of Cloud Computing as it holds confidential personal data with third party service providers. The key aspects of these issues can be cross boarder of transfer of personal data and other circumstances. This paper attempts to show fundamental nature and the context of ethical issues of Cloud Computing.*

Keywords: Cloud Computing, Ethics, Privacy, Small and Medium-sized Enterprises (SMEs).

INTRODUCTION

Cloud Computing is an increasingly important area in the development of business services. One of the most significant transitions in computer industry occurs in the last 20 years is reallocating from desktop and server based software into Cloud Computing. It is a service that delivered through the internet, with a fewer number of software and hardware having with user.

The Australian Bureau of Statistics (ABS) defines a small business as having fewer than 19 employees, whereas micro businesses have fewer than 4 employees. Medium-sized enterprises are defined as businesses with from 20 to 199 employees (DIISR, 2011). The Cloud Computing is an emerging technology that many Small and Medium-sized Enterprises (SMEs) are concerned in because of the benefits of elasticity, pay-as-you go and reduced hardware investment. Cloud based services in generally reduce large up-front licencing and server cost, offer reduces installation and consulting fees and finish off the endless upgrade usually associated with traditional software. This also offers anywhere accessibility, a high level of ease of use, and independent of the operating system. But questions are remaining over its security. SMEs typically face the same fright as large organisations and also lack the same level of expertise and other security resources. Cloud Computing raises issues associated with entrusting a third party with confidential personal data. One of the most significant current discussions in legal and moral philosophy of the computing industry will affect too many aspects of computing.

ETHICS OF CLOUD COMPUTING

Ethic is a very problematical term with a large number of meanings and consequences. Paul and Elder in 2006 define ethics as "a set of concepts and principles that guide us in determining what behaviour helps or harms sentient creatures". In this paper we discuss moral principles that govern especially on personal data in Cloud Computing. This paper does not intended to be reviewing this rather very briefly describe the arrears that ethics will emerges in Cloud Computing. The user outsources his data and computation in the cloud that he cannot be controlled directly by the user (Haeberlen, 2010). The loss of user control can be problematic in the situations such as unauthorised access, data damage or misuse, infrastructure failure, or unavailability (Paquette et al., 2010). In case of data damage or misuse it can be difficult to discriminate who has caused the problem and it is nearly impossible to identify the location of the root cause (Haeberlen, 2010).

Multiple services across the Cloud Computing are interconnected at different levels of functionality to provide a specific service to an end-user. Hence, in Cloud Computing a specific service delivered to a user cannot be segregated function wise and it may depends on another systems. So, this complex structure of cloud services can make it difficult to determine who is responsible for specific service in case something undesirable happens (Pieters, 2009).

The data are stored in multiple physical locations and transfer across the boarders around the world in various servers possibly owned and administrated by many different organisations. So this type of outsourcing data also raises the questions of what legislations are applied with the data, what can the cloud services providers do with this information (Grimes et al., 2009; Murley, 2009). Unnecessary dependency is created with lack of user control and freedom in the Cloud Computing (Grimes et al., 2009). This unwanted dependency on cloud service providers are enforced by possible vendor lock-ins. The service provisioning can make it hard for users to migrate from one provider to another thereby introducing a dependency on a particular cloud provider (ENISA, 2009).

Destruction and de-identification data outsourcing (DFD,2012), multi-sharing on number of cloud service providers (Johnston, 2008) have been identified as impending solutions for being unethical.

PRIVACY

Ethical issues arise in particular on confidential and personal data (Van den Hoven, 2008) which is considered as in terms of privacy. Most of the cloud service providers catch sensitive personal information, which is then stored in data centres in countries around the world. This will affect the development and acceptance of Cloud Computing and how users, companies and countries operate and address privacy issues (Nelson, 2009).

In the case of personal data stored in the cloud, it can be harmful as data is no longer stored locally and control over the data is with the service providers. Different service providers have different opinions on privacy to the customers and it will not always be clear with which service provider is dealing. In general ethics on privacy based on personal data and prevent to acquire and use information about other persons. But privacy protection is still unclear though there are many arguments on the justification of privacy (Van den Hoven, 2008).

As data storage and services can be located at any part of the world, users of the Cloud services will have to deal with the different cultures prevailing specific locations. Privacy aspects relate to different countries differently because of the legal systems. Capurro in 2005 argues that the privacy is affected by cultural differences. On the other hand, Ess accepts that there are irreducible differences between diverse cultures (Ess, 2008). These differences may lead to deep conflicts and divergences of global ethics and thus the development of a global account of privacy (Ess, 2008). But this doesn't mean that there is no hope for intercultural practices with respect to dealing with ethical differences (Moor et al., 2004; Ess, 2008).

CONCLUSION

Cloud Computing has brought great benefits to the SMEs, but it also raises many issues. However, this should not be dissuaded the use of Cloud Computing as the benefits most definitely outweigh the negative issues. Even though, the paper highlights the emerging arrears of ethics, there are very few answers at the moment. For instance, there should be a unified governing body to develop and impose standards to answer all of these concerns.

REFERENCES

Capurro, R. (2005). Privacy: An intercultural perspective. In *Ethics and Information Technology,(*7), pp. 37–47.

DFD. (2012). Privacy and Cloud Computing for Australian Government Agencies, Better Practice Guide, Australian Government Information Management Office.

DIISR. (2011). key statistics: Australian small business: Australian government.

Ess, C. (2008). Culture and Global Networks, Hope for a Global Ethics? In Information Technology and Moral Philosophy, pp. 195-225.

ENISA - The European Network and Information Security Agency (2009) , Cloud Computing, Benefits, risks and recommendations for information security. From: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment.

Grimes, J. M., Jaeger, P.T., and Lin, J. (2009) Weathering the Storm: The Policy Implications of Cloud Computing. http://nora.lis.uiuc.edu/images/iConferences/CloudAbstract13109FINAL.pdf.

Haeberlen (2010). A case for the accountable cloud. *SIGOPS Operations Systems Review.* (44:2), pp. 52-57.

Johnston, S. (2008), Cloud Computing and Privacy, Retrieved from www.circleid.com/posts/89163.

Moor, J. H., Mizutani, M. and Dorsey, J. (2004). The internet and Japanese conception of privacy. Ethics and Information Technology. (6:2), pp.121-128.

Murley, D. (2009). Law Libraries in the Cloud. Law Library Journal, (101:2). Available at SSRN: http://ssrn.com/abstract=1335322

Nelson, M. R. (2009). The Cloud, the Crowd, and Public Policy. Issues in Science and Technology (2009). From: http://www.issues.org/25.4/nelson.html.

Paquette, S., Jaeger, P.T., Wilson and S.C. (2010). Identifying the security risks associated with governmental use of Cloud Computing. Government Information Quarterly, (27:3), pp. 245 – 253.

Paul, R., Elder, L. (2006). The Miniature Guide to Understanding the Foundations of Ethical Reasoning. United States: Foundation for Critical Thinking Free Press. ISBN 0-944583-17-2.

Pieters, W., and van Cleeff, A. (2009). The precautionary principle in a world of digital dependencies. IEEE Computer, (42:6), pp. 50–56.

Van den Hoven, J. (2008). Information Technology, Privacy and the Protection of Personal Data. Information Technology and Moral Philosophy, pp. 301-321.