Dealing with Ethical Issues among Internet Users: Do We Need Legal Enforcement?

Ali Salman[1], Suhana Saad[1] & Mohd. Nor Shahizan Ali[1]

[1] Faculty of Social Sciences & Humanities, Universiti Kebangsaan Malaysia, Bangi, Malaysia

Correspondence: Ali Salman, School of Media & Communication Studies, Faculty of Social Sciences & Humanities, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia. E-mail: asalmanphd@gmail.com

Abstract

Information and communication technologies (ICTs), in particular of the Internet and of the World Wide Web, have paved the way for numerous ICT related development and initiative. In as much as there are beneficial usage of the Internet, there is also unethical usage and abuse. The Internet is like a double edge sword and care must be taken when indulging in this vast ocean of knowledge and information. Studies on ethical issue have centred much on internet security like hacking of personal information and data theft, including in business. This paper will look at the recent trends related to the ethical usage of the Internet, especially involving social media usage and hacking of government websites and legal enforcement that can be used to address ethical issues among Internet users. Data is derived from secondary sources. From the secondary data or literature, hacking has been a subject of concern following the hackings of website of government departments by the group anonymous. There are some cases of internet abuse, especially social media involving scams and personal relationship. There is also the use of social media to incite hatred, especially against authorities leading to widespread unrest. Hence, this implies, putting in place some guiding principles and more stringent legal enforcement to curb the unethical use and abuse of the Internet.

Keywords: internet, ethical usage, internet security, internet usage, social media, legal enforcement

1. Introduction

The digitization of information and communication technologies (ICTs), the world-wide extension of ICT-based networks, services and applications, and in particular of the Internet and of the World Wide Web, have paved the way for numerous ICT related development and initiatives. The web and the Internet have also changed the way we communicate and interrelate, both in our private sphere and at work place (Lagraña, 2010).

During the past decade, electronic mail (e-mail) has become the most popular communication tool outpacing fixed and mobile telephony. Some 96% of organizations declared that they offered access to e-mail in the workplace to their employees, 91% to a conventional fixed-line telephone line, and 86% to a professional mobile phone. On the user side, 99% of employees declared they were using e-mail professionally, against 80% for fixed-line telephony and 76% for mobile phone use (Dimension Data, 2007).

In Malaysia the situation is not different. The government aims to have 90 per cent of its services online by 2015. At present only 35 per cent of the government services are currently available online via the "myGovernment" portal. This included services for pensioners and senior citizens to access their various benefits online, quit rent payments, renewal of licenses, permits and summons payments at local council sites. It also uses social media -- such as Facebook and Twitter -- in day-to-day activities and operations to enhance productivity, with 242 agencies actively using social media to connect with communities. The government sees the need to upgrade the use of ICT in the socio-economic sphere to spur economic growth.

For Malaysia ICT complements the ongoing development strategies and actions which support the digital transformation, to boost socio-economic growth (New Straits Times, 2012). The United Nations e-Government

Survey 2012 that assessed the technical features of national websites as well as e-government policies and strategies applied by specific sectors, had ranked Malaysia 40th among its 193 member countries (ibid).

In as much as there are beneficial usage of the Internet, there is also unethical usage and abuse. The Internet is like a double edge sword and care must be taken when indulging in this vast ocean of knowledge and information in order to achieve the desired and meaningful digital inclusion.

The adoption of technologies is not morally neutral, and the emergence of the new electronic communication systems has come along with, or has favored new attitudes and behaviours, giving rise to new ethical concerns.

Recently there have been ethical issues arising from the usage of the Internet, especially involving social media and hacking of government websites. In the middle of 2011 Malaysia had to step up monitoring of government websites to stop a threatened hacking attack by Internet vigilante group Anonymous over government acts of censorship. The abuse of Social Media involves teenagers who meet strangers online.

Previous research on ethical issues, especially in e-business, mainly addresses the relation of e-businesses to their external environment. Issues such as data mining and profiling, customer and business-critical information protection and privacy, intellectual property rights in a digital economy, or advertizing and spamming, to name but a few, are well covered in the existing literature (Danna & Gandy, 2002; Davenport & Harris, 2007; Palmer, 2005; Roman, 2007; Stead & Gilbert, 2001). However, most of the issues explored relate to B2B or B2C relations, or to e-businesses within their strategic, regulatory and legal environments.

This paper will trace the recent trends related to the ethical usage of the Internet especially social media usage. The paper will also look into issues of hacking, in particular of government websites as experienced by Malaysia. This study used secondary data sources ranging from books to journal and newspaper articles.

2. Concept of Ethics

Ethics aims at providing tools to help discern what people should do and how they should behave or, in a simplified – and possibly simplistic – way, what is good and what is bad behavior. For that matter, the playing ground for philosophers and theologians are theoretical or fundamental ethics and indeed, the origin of ethical theory can be traced in various religious and philosophical views.

Ethics deals with behavior, e.g. with action rather than thoughts or feelings. Ethics is a practice rather than a science or an epistemology. Ethics is not a science since its ultimate purpose is not to develop knowledge (about virtues or virtuous behavior). Ethics is not an epistemology, which would consider each virtue as a science (by example the science of justice) and aim at developing knowledge about these virtues (Aristotle, 1994). Ethics deals with actual behavior: as one may feel like acting in a certain way, one may also analyze the ethical "quality" of such behavior, and then decide to act in a way or another. Only the eventual action will be considered from an ethical perspective, e.g. the action is considered from an ethical perspective rather than the thoughts, feelings or opinions.

Action or behavior must be voluntary. An action taken under constraint is not subject to ethical evaluation. Furthermore, as Aristotle points out in his *Eudemian Ethics,* "what he [a man] does in and by ignorance, he does it involuntarily" (Chapter 9, 3). For example, many e-mail users behave improperly because they do not understand the tool properly, and in such cases it is important to determine whether their action is voluntary or not. Even if their action is involuntary due to ignorance, however, we must also determine if their lack of knowledge is the result of their own negligence.

Ethics is about how we deal with each other and how we take care of common resources. Ethics entails demonstrating mutual respect, empathy, trying to understand each other and be understood and ensuring a proper working environment. For instance one is supposed to get one's right part of shared resources (such as Internet bandwidth) as distinct to overusing such resources for the fact that they are provided for free, is also part of ethical behavior (Hardin, 1968; Huberman & Lukose, 1997).

Ethics is diferent from culture (including philosophy and religion). What is acceptable behavior in one culture might be unethical or illegal in another. Legal behavior is a behavior abiding the laws in force in a specific jurisdiction (typically a national or regional territory where the behavior actually occurs). Ethical behavior is a behavior respecting the moral rules shared by a specific community (culture, philosophy, religion, nation, etc.). In our collective societies, where laws are made to protect the common good and the smooth operation of the communities, what is illegal is generally considered as unethical (Aristotle, 2008). On the other hand, the opposite is not directly true, such as employee monitoring by example, which is legal but consider by many as being unethical (Miller and Weckert, 2000).

Ethics also needs to take into consideration what can possibly be done technically or not, since some behaviors depend upon technological development. It is therefore useful to understand the technical setting before addressing the correlated ethical issues (Langford, 1996). Ethics evolve with technology and in particular, since the development and usage of ICTs, new ethics issues have surfaced up. This is obvious with many issues relating to social media which leads to immoral (considered unethical) acts.

3. Case Study on Ethical Issues and the Internet

The advent of the Internet and its related application, especially web 2.0 has tremendously changed the way we interact and do things. That said, of late, there have been calls for puting some kind of control on the Internet due to cases involving demonstrations and protests where Social Media (SM) was blamed as the cause. There are also cases involving relationship built over SM which subsequently led to abuse. In fact governments and companies websites around the world were not spared either as they came under attack by hackers.

In the United Kingdom (UK) following the London riots where SM was blamed by the government for inciting and fuelling the riots. This became serious because the rioters were simply seen as looters and they were mainly teenagers and young adults who were just out to loot and create unnecessary unrest. Following the riots, the House of Commons's shadow secretary of culture, Ivan Lewis, said that the house, "supports the government's decision to undertake a review of whether measures are necessary to prevent the abuse of social media by those who organize and participate in criminal activities (The Guardian, August 2011)."

There were other similar attempts such as the one by UK Home Secretary, Theresa May, who was scheduling meetings with Facebook, Twitter and Research In Motion (RIM) to "discuss their responsibilities in this area." Suggestions have ranged from banning suspected rioters from social media networks to the wholesale shutdown of social media in times of unrest without regard to individual freedoms in order to "catch the bad guys (Rutledge, 2011)."

In a Thursday speech to Parliament, the British Prime Minister David Cameron remarked, "Everyone watching these horrific actions will be struck by how they were organized via SM. Free flow of information can be used for good. But it can also be used for ill. And when people are using social media for violence, we need to stop them." The crust of the matter is based on the premise that people should and can not use SM to create unrest. Therefore, the Prime Minister reiterate the government and the police are going "to look at whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality."

The Prime Miniters received the backing of even the opposition Labour Party on the matter. For Ivan Lewis, the Labour Party's shadow secretary of culture in the House of Commons, "Free speech is central to our democracy, but so is public safety and security. We support the government's decision to undertake a review of whether measures are necessary to prevent the abuse of social media by those who organize and participate in criminal activities (Mick, 2011)."

Malaysia has its share of the ethical issues involving internet usage. Despite the developments in the adoption of Internet, there are challenges and Malaysia is not spared from such challenges. Common among these challenges are cyber attacks and hackings, which are worrying. Like any other country, Malaysia also bears the brunt of the new media by way of cyber attacks at the time the authorities were pushing for stringent piracy laws.

In the middle of 2011 Malaysia had to step up monitoring of government websites to stop a threatened hacking attack by Internet vigilante group Anonymous over government acts of censorship. The hacker group targetted the Malaysian government's online portal as a protest against censoring whistle-blower site WikiLeaks, in an attack codenamed "Operation Malaysia." Malaysia was the latest among countries in a cyber-war waged by the activists, who gained prominence when they temporarily crippled the websites of MasterCard and Paypal (Reuters, 2011).

In the course of the attacks almost 41 Malaysian government websites were hacked into overnight. However, no personal or financial data were lost. In the attacks, 51 websites were hit and at least 41 of these sites were disrupted (Communications and Multimedia Commission, 2011). On top of the list of hacked websites was www.malaysia.gov.my. Other sites which suffered similar faith belong to the Information Ministry (kpkk.gov.my), the Fire and Emergency Services Department (bomba.gov.my), the Land Public Transport Commission (spad.gov.my), and Parliament (www.parlimen.gov.my). Other related agencies sites which were down included Sabah Tourism (www.sabahtourism.com) and Construction Industry Development Board (www.cidb.gov.my). It also included Asean Connect, Treasury, Jobs Malaysia, and National Sports Council

among others. All the sites, except CIDB, became completely inaccessible. These sites were allegedly experiencing DDoS (Distributed Denial-of-Service) attacks or switched off by website administrator.

Personal relationship is also being affected by the Internet, especially social media. What is particularly worrying, however, is the involvement of teenagers who at times fall victims of internet abuse. Imagine a teenager meeting a stranger online and subsequently fall in love. Recently a 13-year-old girl (Form One student) defiantly stood by her decision to continue seeing her 16-year-old boyfriend who she met through Facebook. The girl's parents decision to go to the press was to create awareness on what is happening to our youths these days. This incident is alarming bearing in mind that it invloves our youth couple with the rise in the number of cases (The Star Online, 2012).

4. Discussions

The foregoing case studies have presented situations of unethical usage of the Internet. They show how the Internet was used for inciting and fuelling riots, threatening of government websites by hackers and last but not least affecting personal relationship, especially among teenagers through SM. This goes to show that despite all the advantages of using the internet, there are also disadvantages.

This presents a dilema as the Internet has been hailed for revolutionising how we do things and interact with one another. The challenge facing us now is how to safeguard the Internet from abuse and at the same time educate users, especially our youngsters on the negative side of this media.

Social unrest can easily spread via internet resulting in damage to properties and even in some cases life. This calls for checks on the usage of internet, especially SM to avoid a bigger damage to economy which can affect development process.

Governments even from the West who are known to be very liberal are now calling for control of the Internet. What this means is that the unethical use of internet is viewed as serious, especially as it can be hijacked and misuse for personal ad even criminal reasons. This could be one of the main reasons why Malaysia has proposed a legal enforcement by amending the Evidence Act of 1950.

4.1 Addressing Ethical Issues through Legal Enforcement

In Malaysia the government is taking the legal way out by bringing into force an act aiming at amending the Evidence Act 1950. This move is faced with strong objections and concerns from the fraternity of the online community and civil advocates. It is largely seen as curtailing freedom of expression. In fact section 114A of the Evidence Act was gazetted Mohamed Nazri Abdul Aziz, who is seen as the minister responsible for matters related to law and has been in operation since July 31 of 2012 (Asohan, 2012).

There were calls for more discussions prior to gazetting the Law. Among the prominent ones, is the call by the Centre of Independent Journalism (CIJ) which presented a petition with more than 3,000 signatures. There were further moves coordinated by CIJ known as the Internet Blackout Day as part of the "Stop 114A" campaign. It urged Internet users accross the country to registed their displeasure by blackening out their websites and profile pictures in protest of the amendment (Regina, 2012).

Following these developments, the Prime Minister Najib Abdul Razak's announced a cabinet review of Section 114A of the Evidence Act. The Evidence Act 1950 [*Act 56*], which is referred to as the "principal Act" in this Act, is amended in section 3 by substituting for the definition of "computer" the following definition:

> *"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;'*

New section 114A- The principal Act is amended by inserting after section 114 the following section: "Presumption of fact in publication" 114A.

1) A person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or re-publish the publication is presumed to have published or re-published the contents of the publication unless the contrary is proved.

2) A person who is registered with a network service provider as a subscriber of a network service on which any publication originates from is presumed to be the person who published or re-published the publication unless the contrary is proved.

3) Any person who has in his custody or control any computer on which any publication originates from is presumed to have published or re-published the content of the publication unless the contrary is proved.

4) For the purpose of this section;

(a) "network service" and "network service provider" have the meaning assigned to them in section 6 of the Communications and Multimedia Act 1998 [*Act 588*]; and

(b) "publication" means a statement or a representation, whether in written, printed, pictorial, film, graphical, acoustic or other form displayed on the screen of a computer."

However, the Evident Act (amendment 2012) should be viewed positively by new media practitioners, especially those who use social media to spread information. Despite the opposition, the existence of this act is important in reducing cyber crime. By engaging cyber ethics of writing and communication, Internet users will be more responsible and mature in delivering edicts and giving opinions. In addition, this Evidence Act can also help maintain privacy of ownership and internet usage.

5. Conclusion

As government services go online, the need for security becomes even more crucial. It might be catastrophic whenever vital data is lost, especially when it has to do with national security. Moreover, abuse of the Internet involving personal relationship is quiet alarming as well. Hence, more needs to be done by way of creating awareness of the pros and cons of using internet; and putting in place some guiding principles and security measures to safeguard the Internet from abuse bearing in mind that not all that glitters on the Internet is gold. At present countries of the world are vying for digital inclusion. Therefore legal enforcement such as Act 114A is a vital factor in addressing ethical issues related to internet and cyber crime.

References

Aristote. (1994). *Ethique à Eudème.* Translation by P. Maréchaux. Paris, France: Editions Payot & Rivage.

Aristote. (2008). *Sur la justice. Ethique à Nicomaque.* Translation by R. Bodéüs. Paris, France: Editions Flammarion.

Asohan, A. (2012). *Govt stealthily gazettes Evidence Act amendment, law is now in operation.* Retrieved November 29, 2012, from http://www.digitalasia.com

Brown, P. (2011, August 14). Emotion is contagious; social media is not. *Psychology Today*.

Danna, A., & Gandy, O. H. Jr. (2002). All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining. *Journal of Business Ethics, 40*, 373-386. http://dx.doi.org/10.1023/A:1020845814009

Davenport, T. H., & Harris, J. G. (2007, May). The Dark Side of Customer Analytics. *Harvard Business Review*.

Dimension Data and Datamonitor. (2007). *Dimension Data Unified Communications Study.* Retrieved August 10, 2012 from http://www.dimensiondata.com/uc

Hardin, G. (1968). The tragedy of the Commons. *Science, 162*.

Huberman, B. A., & Lukose, R. M. (1997). *Social Dilemmas and Internet Congestions*. Retrieved September 13, 2012, from http://ssrn.com/abstract=41207

Lagraña, F. A. A. (2010). Ethical Issues Arising from the Usage of Electronic communications in the Workplace in Ethical Issues in E-Business: Models and Frameworks. Daniel E. Palmer (Ed.). Hershey-New York: IGI Global.

Langford, D. (1996). Ethics and the Internet: Appropriate Behavior in Electronic Communication. *Ethics and Behavior, 6*(2), 91-106. http://dx.doi.org/10.1207/s15327019eb0602_2

Lee, R. (2012). *Websites show support for Internet Blackout Day.* Retrieved November 29, 2012, from http://thestar.com.my/news/story.asp?file=/2012/8/14/nation/20120814122218&sec=nation

Mick, J. (2011). *Britain Blames Social Media For Class Riots, Looks to Censorship.* Retrieved September 14, 2012, from http://www.dailytech.com/Britain+Blames+Social+Media+For+Class+Riots+Looks+to+Censorship/article22435.htm

Miller, S., & Weckert, J. (2000). Privacy, the Workplace and the Internet. *Journal of Business Ethics, 28*, 255-265. http://dx.doi.org/10.1023/A:1006232417265

New Straits Times. (2012, July 4). 90pc of govt services to go online by 2015.

Palmer, D. E. (2005). Pop-Ups, Cookies, and Spam: Toward a Deeper Analysis of the Ethical Significance of Internet Marketing Practices. *Journal of Business Ethics, 58*, 271-280. http://dx.doi.org/10.1007/s10551-005-1421-8

Reuters. (2011). *Hackers disrupt 41 Malaysian government websites.* Retrieved January 1, 2012, from http://in.reuters.com/article/2011/06/16/idINIndia-57724420110616

Reuters. (2011). *Malaysia tries to stop threatened cyber attack.* Retrieved January 1, 2012, from http://www.reuters.com/article/2011/06/15/us-cyber-malaysia-idUSTRE75E05N20110615

Roman, S. (2007). The Ethics of Online Retailing: A Scale Development and Validation from the Consumers' Perspective. *Journal of Business Ethics, 72*, 131-148. http://dx.doi.org/10.1007/s10551-006-9161-y

Stead, B. A., & Gilbert, J. (2001). Ethical Issues in Electronic Commerce. *Journal of Business Ethics, 34*, 75-85. http://dx.doi.org/10.1023/A:1012266020988

The Star Online. (2012, June 6). *We're in love, says runaway.* Retrieved September 9, 2012, from http://thestar.com.my/news/story.asp?file=/2012/6/6/nation/11421791&sec=nation