Corporate Social Media Use Policy: Meeting Business and Ethical Responsibilities

Don Gotterbarn

Corporate Social Media Use Policy: Meeting Business and Ethical Responsibilities

Don Gotterbarn

Centre for Computing and Social Responsibility, De Montfort University, Leicester, England
don@gotterbarn.com

Abstract. Rapidly developing social media technology has made obsolete many corporate computer use policies. New types of policies need to be developed which address the blurring of the distinction between corporate and personal computing. The gradual change in whose smart technology is used, and how it is used in the service of employers needs to be controlled to promote possible positive effects for the employer and reduce potential negative issues. The development of these policies raises significant ethical tensions in potentially controlling and limiting employee rights. These changes in technological convergence add new ethical requirements for an adequate policy. The lines between "business ethics" and "personal ethics" intersect here, and the ethical foundations of these need to be articulated in developing and/or promoting these policies. A technique is suggested as a starting point for companies to use in addressing these new ethics requirements for adequate social media policies.

Keywords: ethics, moral responsibility, social media policy, socio-technical isues

1 Introduction to ICT Governance

The rapid changes in information and communication technology (ICT) have always presented a problem for industry in determining how to use and manage the new technology in achieving its goals. Attempts to do this have led to the development of ICT governance. ICT governance is an attempt on the part of business to deal with the impacts of major software system failures on business. ICT governance is both proactive and reactive. It is proactive in providing the structure for determining organizational objectives and monitoring performance to ensure that objectives are attained, and it is reactive in providing a standard approach to computing accountability in industry. The increase in the speed and types of technological convergence makes it especially difficult to specify a single framework to help with decisions, articulate rights, and specify accountability. ICT governance requires a specific strategy providing direction, policies setting boundaries, and writing procedures and guidelines providing clear details of accountability clarifying roles and responsibilities.

adfa, p. 1, 2011.

1.1 Early Corporate Computer Use Policies

Prior to the current technology shift, computing devices were corporate assets and employees used those assets. Those assets' communication capabilities and external networking infrastructure were paid for by the corporation.

Policy justifications: ownership and employment. A corporation's computer use policies were justified by simple principles about business requirements and the financial relationship between employer and employee. The physical computing hardware was a corporate asset which operated on a network paid for by the employer. Following these policies, employees should not attend to personal tasks during working hours. The organization owns the computers and the data on them, and these devices should not be used for personal communications. These claims were used to justify Internet and corporate IT policies such as restricting employee computer use only to business functions, and corporations' monitoring email on the corporate computer for legal compliance. Because all email was of a business nature, employees were aware of the normal business protocol of polite speech.

Social media policy and the law. Laws eventually supported these claims based on the ownership of assets by industry. Some of these claims have been upheld in United States (US) court cases and also used to justify inspection and restriction/censorship of employee email on corporate machines. One problem with using laws to judge the use of computers at work is that technology moves faster than the law. This means that laws appropriate to an earlier generation of technology are used to adjudicate current technology issues, in effect, trying to apply policy designed for one technology to new technologies and to social changes. Inappropriate employee communication was easily controlled both by employer computer use policy and mechanical restrictions on the employer's computers. These computer use policies were about the use of computers at work and were based on at least two presumptions: the financial/work agreement between employer and employee, and the computers in question were corporate assets. The ICT equipment was the corporation's, and the company supplied staff to maintain it.

Negative impacts of social media on corporate survival. The relation between the employer and the employee was an implicit contract that the corporation provides fair pay for a focused fair amount of work to support the corporation. Companies needed to control the amount of time devoted to work to meet project plans. The company's survival also depended on protecting trade secrets and business plans, and complying with financial regulations and environmental controls.

1.2 Mediamorphosis: Blurring the Lines between Home and Work

Improvements in technology (such as wireless communication and miniaturization), and the change in the ways we communicate (generally referred to as 'social media'),

have caused many new and significant problems for employers. The boundaries between computing and communication have been blurring and raise questions such as: Is an Internet search on the phone while at work business or personal use of a computer? These changes blur the lines between personal and corporate computer use. Our concepts are further muddied by employees bringing their own computers, in the form of smart phones and other devices, into the work place.

Acceptability of disruptions and distractions. These technological changes have also facilitated radical changes in the acceptable use patterns of technology outside of the work place. Individuals are now in almost continuous contact through social media. Both the technology and its usage patterns in social media require careful ethical evaluation. Among the problems generated by social media are: a failure to see that the nature of the medium sometimes significantly distorts the messages; not realizing that built-in phone tracking may make it wrong to transmit messages from some locations: equating the degree of repetition with truth; the failure to understand the impact of messages beyond their video screen representation; and the career impacts of widespread digital information.

Prior to the development of digital media, in many cases work was partially defined geographically; people went to work, left one place for another where they worked. This difference in place made it easy to distinguish acceptable behaviors in work places and home. In the work place the employer's restrictions on computer use applied, and at home they did not. The information was also geographically distinct. Work-related information was stored at work on the corporate machine.

The convergence of technologies, such as the use of smart phones at home or work, for personal or work-related activities, has added to the difficulties of using geographical and ownership criteria to help employer management of employee computer use. Some have tried to maintain this simple physical separation model by having employees only use corporate supplied devices for their work activities just like the ones their employees own. Now employees are tethered to two separate, sometimes identical devices, one that they use for work and one that they use for personal activity. But both devices can be brought to work or home and used at either place. This weakens the geographical basis for distinguishing between personal and business computing. The clear geographical distinction was reduced to a distinction between the ownership of the tools. This was later replaced by the use of the employee personal smart device but with corporate software and an electronic partition of corporate data on the employee device. This physical blurring of the distinction between home and work tools is also the beginning of the blurring of when one is 'at work' and is 'doing work'.

Mediamorphosis. The blurring of distinctions within and across technologies is called "converging technology". Different technologies were enhanced and made more marketable by also performing tasks from other technologies. Computers were tools to do spreadsheets while telephones were used for verbal communications. These separate technologies now share resources and interact. It is now commonplace for individuals and organizations to deliver all forms of material over both wired and wireless communications. This has been called "mediamorphosis" [1].

2 Consequences of Convergence

The convergence affecting work, and the relationship of employers to their employees, is due to the connection of computing with other information technologies, media content, and communication networks. They form the activities, products and services that have emerged in the digital media space on information and communication technology devices (ICTDs).

There are numerous examples of the impact of the proliferation of ICTDs. Many employees own their own smart ICTDs using the associated social media. The introduction of smart technologies – such as iPods, iPads, and iPhones – has permeated society. The technology encourages and legitimizes their communicating on the Internet as soon as they are thinking it. These devices have introduced broad social changes. The impact of some of these changes has been addressed in legislation.

The systems developed for these technologies, such as aggregated searches, Facebook, LinkedIn, and Twitter have complicated the question of how to manage social media and maintain a necessary distinction between business and personal activities. Both businesses and individuals have accounts on Facebook. Individuals' LinkedIn connections can be used to make business contacts or to look for another job.

2.1 Social Media Policy: Requirements

Employers need to change the model of ICT governance, its justifications and its focus on internal corporate issues to address the changes in business context caused by converging technology. The new model of governance in its simplest form is a corporate social media policy. An effective policy must maximize the positive possibilities for the corporation to take advantage of social media and minimize its negative impact while, having a consistent ethically responsible policy for its employees.

Employer benefits. Employers need to consider what this change means for them. This change seems to introduce possibilities of employees using their own ICTDs to accomplish employer tasks while 'at work' reducing corporate IT expenses for new equipment and the upgrade of devices and ICTD support staff. The phrase 'at work' begins to lose its geographical connotation and just describes the relation of the activity to the interest of the employer. Convergence opens up the possibility of a 24/7 work week. Since devices belong to the individual, it will be less likely that they will be subject to negligent wear and tear. From an employer perspective these possibilities are positive; however, there are also negative issues.

Need to address unintentional harm. Employees using their own devices open up the whole question of how to monitor and control the work-related activity on these devices and whether activity on these devices can be monitored without negatively impacting employee privacy. In some contexts personal interactions assume a much less structured, and casual, form than business communications. Companies are finding it necessary to remind employees about proper business protocols when

talking to a client. A policy needs to fulfil this reminder function because some employees are not mindful of these communications breaches but, once reminded, an employee cannot engage in unregulated, unmanaged use of social media.

A social media policy is an attempt to deal with the impacts of unregulated use of social media on business and it must include in its scope a broader context than is circumscribed by the physical work place. Sometimes, the problems are simply that employees have operated in a normal mode of sharing information but in an unthinking way. For example, a waiter used his cell phone to post a picture of a credit card receipt showing a very large tip from an American footballer. The waiter was elated at the extent of the tip and wanted to share the information with his friends; an almost 50% tip on a several hundred dollar bill. The picture went viral [2]. This waiter perhaps did not intend anything negative, but it would seem that he broke the trust between the establishment and the clientele, and this had consequences.

The waiter was fired for several reasons. The waiter violated company policy; the restaurant which often serves celebrities has a strict policy that their private dining experiences stay private. The picture he posted shows the footballer's signature used on licensed merchandise, and shows the last four digits of a credit card number, which in some circles are used for identity verification purposes. The footballer makes part of his living doing advertisements for a particular credit card company, had the footballer used a different credit card from the one he advertised then the footballer's livelihood could have been impacted by the waiter's posting the picture. The waiter does not own the credit card receipt, the company does and it is part of its confidential business information. The negative impact on the restaurant probably was not intentional. There are however uses of social media that can intentionally harm companies.

Need to address intentional harm. The Internet has been used to record consumer complaints and record likes or dislikes, so some people have used it to develop corporation-critical websites such as www.walmartsucks.org/, IHateBarclaysBank, Starbucked, AOLsucks, and Noamazon.com. Some websites are designed to facilitate corporate criticism. Sucks.com is a micro-review site that does not require a name, email or a registration to express an opinion. Policies have to address these risks to corporate reputation. They need to address these attacks as well as employees' use of their own machine at home or at work, and employees' activities at home and work which might get then in trouble at work. One of the difficulties for a social media policy is that many employees consider social media use to be a purely personal behavior and reject as improper corporations' attempts to control it.

2.2 Inadequate Policies

Earlier employee computer use policies are inadequate and inappropriate for convergent social media. The basis for managing working time now has to include reference to usage of personal computing devices and social media accounts inside and outside of the workplace, and to corporate brand and image protection. Such policies can no longer simply rely on claims about corporate ownership of the computer and commu-

nications being done during working hours. Some problems for social media policies arise in part because an individual's use of social media blurs the distinction between public and private information, and between work information and personal information. Notes on LinkedIn, MySpace and Facebook are a blend of private and public information. These social media can be used to promote, criticize, or not mention a corporation. There is a need to balance the positive and negative effects of the policy.

Sample policy problem. In 2010 a company, American Medical Response of Connecticut (AMRC), fired an employee who had made untoward remarks about her manager on her personal Facebook account from her home computer. AMRC's policy stated that "Employees are prohibited from making disparaging, discriminatory or defamatory comments when discussing the Company or the employee's superiors, co-workers and/or competitors." In the United States of America (USA), the National Labor Relations Board (NLRB) brought a suit for the employee against AMRC to see if this policy violated employee rights and free speech standards.

The AMRC policy included the following restrictions: "Employees are prohibited from posting pictures of themselves in any media, including but not limited to the Internet, which depicts the Company in any way, including but not limited to a Company uniform, corporate logo or an ambulance, unless the employee receives written approval … in advance of the posting;" and "Employees are prohibited from making disparaging, discriminatory or defamatory comments when discussing the Company or the employee's superiors, co-workers and/or competitors."

The NLRB settlement required AMRC to: (1) revise its overly broad rules; (2) ensure that its rules do not improperly restrict employees from discussing their wages, hours and working conditions; and (3) not discipline or discharge employees for engaging in such discussions. The NLRB concluded that such provisions interfere with an employee's right to engage in protected activity but it is reasonable to prohibit employees from revealing confidential, proprietary or trade secret information about the company. Employers may also incorporate anti-harassment and discrimination policies into social media policies and otherwise legitimately curtail employees' use of social media as it relates to the workplace.

3 Business Use of Employee Devices: New Requirements for Social Media Policies

The potential savings of having employees do additional work at home, be available outside of the normal work day, and use their own devices to do business has appealed to organizations. However, there are significant issues that a social media policy must address to facilitate a "Bring Your Own Device" (BYOD) environment.

Manage the data on employee devices. The first puzzle is how to manage these devices. As in any work situation, the organization must be observed to direct and allocate rewards and encourage improvement of the work. Work must also be

monitored so as to detect non-work activity. There are also security requirements that must be met, and the use of personal devices must meet the same standards as those of corporate devices. These standards include client confidentiality, protection of data, financial security protection, and legal notification. The policy must provide for ways to remove confidential data from employee devices and procedures to safeguard the data when and if it leaves the premises with the employee.

Manage the software on employee devices. There is a need to control the types of software used on these systems. For example, some document-reading software has known but not fixed weak spots [3]. There are legal issues for a company if the employee device has and uses pirated software. Because of compatibility issues, once acceptable software has been tested and approved by the organization, the types of devices that can be used/owned by the employees will be limited.

In the USA more than half of the federal agencies encourage staff to bring their own devices. More than 50% of federal employees do this. The major puzzle for any social media policy which incorporates a BYOD option is "How do you control someone else's device?" This has been answered on a technical level using mobile device management (MDM) software, which enables corporate IT departments to manage the many mobile devices used throughout the enterprise.

Software is placed on employee devices. Policy enforcement typically calls for a small client to be installed on the device, and managed from a central server using over-the-air management. Functions such as policy enforcement and remote wipe are now standard. If a phone is lost or stolen, and this is discovered in time, confidential data can be wiped off the device. To protect the data they use a "sandbox approach" – they store enterprise data, including email and applications, in a distinct area of the device, and encrypt and password protect only that data. All other files including personal data are available to the employee.

These solutions are not available to smaller companies even though they are increasingly compelled to support mobile devices with fewer resources for managing all of them. A technical solution addresses some of the issues raised by social media in the workplace; restricting the applications that can be used in a sandbox (located on an employee's smart device) does not address how they use those systems and what they do when outside their smart device sandbox while at work. A corporate trade secret could be photographed and posted to "friends" using other applications on a phone. MDM software does not address the employee's relation to and comments about the company on social media. What is needed in a social media policy? The technical solutions and the justifications used to control employee computing are no longer adequate. A social media policy requires something more.

4 Social Media Policy

The basic positive goals of the policy should be to promote the business, maintain a positive social media presence, and promote the brand. The defensive functions of such a policy should be to reduce the impact of social media attacks on the Internet.

An overriding goal of all corporate policies is to be fair and supportive to an employee's productivity in an ethically and legally responsible way. MDM, and similar technological solutions, do not accomplish this. A specific policy is required to help employers and employees make good, ethical decisions. The differences among cultures make it difficult to see common ethical principles that would cover the handling of social media. Some policies in fact render the lines between home and work less distinct because corporations have their own social media accounts on Facebook or LinkedIn. Corporations want to promote company-supportive use of social media, but the same channels can be used to corporate disadvantage.

4.1 The Goals of a Policy

Social media policy for organizations (a policy which has broad application to public, private and governmental sectors) should be easy for employees to agree to and understand why following it is important and reasonable; so giving (light) philosophical and practical justification for the policy is useful. The goal is to develop a policy that organizations can use, starting with behavioral regulations that is justified by high-level ethical/normative standards that address (i.e., include) business ethics issues.

Include business goals. A possible strategy to develop such a policy is to start by identifying the business principles that need to be protected, encouraged, and enforced by the policy guidelines/rules. The policy needs to cover both positive and negative elements, for example, "don't say bad things about your company on social media" or "without revealing corporate secrets indicate the virtues of working for the company and the joys of using corporate media to communicate on social media."

Consider ethical issues. After this we need to identify the categories and ethical principles that the policy must address. There needs to be an identification of the ethical principles that a corporate social media policy may be in tension with, for example, "free speech" and restricting employees from mentioning their work on social media, "the right to form a union", and "trade secrets". Some companies, like Telstra [5], limit the scope of its policy to the work environment. The policy developers need to identify what should be contained in the policy statement. It is imperative that they then do a preliminary ranking of the principles by significance (to an organization) including why it would value these principles, because it may not be possible to advocate all of these principles in a single consistent policy.

With these preliminaries out of the way, developers then need to address the internal consistency of the different social media guidelines/rules and conformance with basic ethical principles. Such issues might include how to articulate and address tensions between the control desired by business and freedom desired by individuals.

Given a general satisfactory set of initial principles, we may try to move from general rules to rules for several business models such as public, private and non-profit, and then examine sector-specific rules. Areas such as the law need to include rules to restrain staff from giving legal advice. Sectors like health care and insurance need to

have specific rules about privacy and confidentiality. Be sure to identify and include other elements needed in other cultures. What parts of the policy will only require a minor change to make it relevant as it moves to different cultures? We should test what we do by asking how it would change when it is embedded in other cultures.

4.2 Requirements of a Policy

A social media policy has both business and ethical requirements, discussed below.

Business requirements for a social media policy. There are a number of employee rights which should not be restricted including: the right to organize and discuss working conditions, the freedom to depict the company in any way without permission and from making disparaging remarks when discussing the company or supervisors, and the terms and conditions of their employment. As a practical matter, the policy should define its scope to include all sorts of social media in any sort of devices. In the USA, under Federal Trade Commission (FTC) requirements, the policy should require employees to communicate that they are an employee of their employer when communicating information about the employer and make it clear that the comments reflect their own opinions and not those of their employer. The policy should make clear what information is restricted including employer's and customer's information but they may discuss their terms and conditions of employment.

Policy examples. Many companies have started to rewrite their social media policies [6]. Policies vary from encouraging web participation to helping a company to promote its image to developing more restrictive policies, in CISCO, for example. IBM [7] emphasizes that companies should develop supportive social media policies, and it used a blog to develop its own policy. Kodak's [8] policy includes training in all forms of social media. Several of the more inviting policies still require permission and do not conform to the National Labor Relations Board (NLRB) recommendations above. Most of the policies predate the NLRB decisions of early 2011.

None of the policies speaks of the above-identified problems with social media. The convergence of communications and computers and social media systems has combined to modify the socio-technical context of work. This revised context requires attention to be focused on explicit ethical issues; yet the closest that existing policies come to address ethical issues is to say "be polite" and "use common sense". Intel's policy talks of "respect" [9]. Its primary focus seems to be on protecting and supporting the company. These policies could be significantly improved with some discussion of ethics and the moral responsibility of the user.

Ethical requirements for a social media policy. Social media policies tend to have a narrow scope that focuses on the relation between employees and corporations. Policy makers focus on how to reduce problems for industry caused by its use. They tend to focus on a limited set of stakeholders, and pay limited attention to those others who

will be impacted. Stakeholders who are addressed in social media policies are the user and the company or, at most, those who have a financial interest in the company. Best Buy, for instance, has a clear social media policy [10], but with a limited view of who the stakeholders are. If you violate the Best Buy policy you could: "Get fired (and it's embarrassing to lose your job for something that's so easily avoided); Get Best Buy in legal trouble with customers or investors; Cost us the ability to get and keep customers. Remember: protect the brand, protect yourself."

Corporations tend to have a narrow a view of the stakeholders as being those with a financial interest in the system – the company and its customers. Corporations need to address a broader range of stakeholders impacted by their employees' social media use. The extended stakeholders are all those who are affected by the use of social media. In addition, a wider range of risks – social, political, and ethical – have to be addressed by any social media policy. Unfortunately, international standards are making the same mistake of focusing just on "evaluating and directing the plans for usage of [SM][1] within the organization and monitoring this use to achieve those plans" [11].

5 Concluding Discussion

As technology has converged there has been a gradual blurring of the distinction between working life and private life. Traditionally, the computer-use policy generally only needed to address managing employee use of computing while on employer premises. With the development of telecommuting, the policies were redefined in terms of ownership of the computing and networking equipment and of the data. Policies could be adequate if they focused primarily on the interaction and impacts of the relation between employer and employee. The current degree of technological convergence has introduced new requirements for any computer-use/social media policy. The whole range of social media is used by employees and the impacts of all of these social media need to be addressed.

Overly constraining policies tends to violate employee rights and causes resentment by employees. Such constraining policies also limit potential employer benefits from positive social media use of their employees. Technical management of social media used by employees is limited in scope to those employee personal devices that are known about by the employer. One of the critical weaknesses in many current policies is the limited view of who is impacted by employee computer use; also lacking is an attempt to develop buy-in by employees as responsible computer users.

5.1 Addressing the Ethical Responsibility of Social Media

In 2010 an Ad Hoc Committee for Responsible Computing was formed to develop a set of rules describing the Moral Responsibility for Computing Artifacts [12]. The rules currently consist of five rules as a normative guide for people who design, develop, deploy, evaluate or use computing artifacts. The document focuses on "the importance of moral responsibility for these artifacts" and encourages "individuals

[1] Social media.

and institutions to carefully examine their own responsibilities with respect to computing artifacts." The document includes a preliminary definition of "moral responsibility" as indicating "that people are answerable for their behavior when they produce or use computing artifacts, and that their actions reflect on their character… 'Moral responsibility' includes an obligation to adhere to reasonable standards of behavior and to respect others who could be affected by the behavior" [13].

These rules capture some significant common elements of ethical action in different business sectors and across divergent cultures. Although they were not developed to explicitly address the specific problems identified above, they have identified some essential elements of moral responsibility that could help address some of the issues about social media. This can be seen by some minor modifications of these rules so as to show their relevance to the development of an effective social media policy.

Rule 1: The people who communicate via social media are morally responsible for that communication and for the foreseeable effects of it. This responsibility is shared with other people who have affected and contributed to that communication as part of a sociotechnical system.

This identifies moral responsibility both for those who create the message for its unintended but foreseeable effects, and for those who use a system to wrongfully harm others.

Rule 2: The shared responsibility of a social media communication is not a zero-sum game. The responsibility of an individual is not reduced simply because more people become involved in designing, developing, deploying or using the artifact. Instead, a person's responsibility includes being answerable for the behaviors of the artifact and for the artifact's effects after deployment, to the degree to which these effects are reasonably foreseeable by that person.

This emphasizes the relevance of all participants – tweeters, followers, re-tweeters, mis-tweeters, bloggers, and subscribers for the effects of a message. The one who unthinkingly re-tweets every message is responsible for its increased credibility. The one who designs or modifies the Page Rank algorithm is responsible for the censorship and impressions it produces. The use of the word 'foreseeable' indicates that a morally responsible person should pause and think about the consequences of each use of social media.

Rule 3: People who knowingly use a particular computing artifact are morally responsible for that use.

The moral responsibility of a user includes an obligation to learn enough about the social media and its effect to make an informed judgment. Claims about others on Facebook have had notorious consequences. The seemingly mundane playing of a video game at work may delay the delivery of a safety-critical product.

Rule 4: People who knowingly design, develop, deploy, or use a computing artifact can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded.

This requires that a person tries to understand the relevant system and how the nature of the system and its context will impact others.

Rule 5: People who design, develop, deploy, promote, or evaluate a computing artifact should not explicitly or implicitly deceive users about the artifact or its fore-

seeable effects, or about the sociotechnical systems in which the artifact is embedded.

Incorporating the sense of these rules in a social media policy would help address the socio-technical problems of social media identified above, and an awareness of these rules would help provide a reason to adhere to a social media policy which is not primarily based on corporate self-interest[2]. No corporate social media policy will be effective without the moral support of those whose actions are within the scope of the policy. This will be possible by using and promoting these rules as part of that policy or part of the education in support of the policy.

References

1. Fidler, R.: Mediamorphosis: Understanding New Media. Pine Forge Press, Thousand Oaks (1997)
2. Gibson, D.: Angus Barn's Eure: Peyton Manning check posting 'horrible'. Triangle Business Journal, March 7 (2012), http://www.bizjournals.com/triangle/blog/2012/03/peyton-leaves-whopper-tip-at-angus-barn.html
3. Lemos, R.: Espionage network exploiting Adobe Reader flaw. Infoworld, December 9 (2011)
4. http://www.informationweek.com/news/government/mobile/232600428
5. http://www.telstra.com.au/abouttelstra/download/document/social-media-company-policy-final-150409.pdf?red=/at/m/d/smcpf150409pdf
6. Boudreaux, C.: Social Media Governance, Policy database 2009-2011 (2011), http://socialmediagovernance.com/policies.php (last accessed on 10.06.2011)
7. IBM, http://www.ibm.com/blogs/zz/en/guidelines.html
8. Kodak, http://www.kodak.com/US/images/en/corp/aboutKodak/onlineToday/Social_Media_10_7aSP.pdf
9. Intel, http://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html
10. Best Buy, http://forums.bestbuy.com/t5/Welcome-News/Best-Buy-Social-Media-Policy/td-p/20492
11. ISO 38500, 2008, AS8015, 2005 http://www.iso.org/iso/catalogue_detail?csnumber=51639
12. Miller, K.: Ad Hoc Committee for Responsible Computing. Moral Responsibility for Computing Artifacts: Five Rules, Version 27 (2010). https://edocs.uis.edu/kmill2/www/TheRules/moralResponsibilityForComputerArtifactsV27.pdf (last accessed on 10.06.2011)
13. Davis, M.: 'Ain't no one here but us social forces:' Constructing the professional responsibility of engineers. Science and Engineering Ethics (2011), http://ethics.iit.edu/publication/E-0077 (last accessed on 04.05.2012)
14. Gotterbarn, D.: Tweeting is a beautiful sound, but not in my backyard: Employer Rights and the ethical issues of a tweet free environment for business. In: Bissett, A, et al. (eds.), Ethicomp 2011, Conference Proceedings. Sheffield Hallam University Press, Sheffield, UK (2011)

[2] This use of moral rules was first addressed in an earlier work, see reference [14].