International Journal of Data Analysis and Information Systems
Volume 9 • Number 1 • June 2017

Accounting Information Systems - Crucial Frontier in Business Ethics

Silvia Romero*, Ronald Strauss and Agatha Jeffers
Montclair State University, Feliciano School of Business, 1 Normal Avenue, Montclair, NJ 07043
E-mails: ^{1*}romeros@montclair.edu; ^{2}Strauss@montclair.edu; ^{3}jeffersa@montclair.edu

ABSTRACT

In recent years the exponential growth of Big Data captured in the Accounting Information Systems of firms, has produced new ethical dilemmas that need to be studied and evaluated. Given the experience from the past, action has to be taken before the damage extends to the overall economy. At different times in history, ethical issues have affected reporting in general and accounting in particular. These situations were mostly addressed by regulation (e.g. the Securities Act of 1933, the Sarbanes-Oxley Act of 2002, and the Dodd-Frank Consumer Protection Act of 2010). In all of these scenarios, policy setters reacted after the ethical issues damaged different stakeholders and the economy, and the purpose of the rules was to avoid harm in the future. In this paper we discuss the new environment of Accounting Information Systems (AIS), and the need to proactively address the ethical aspects of these new developments in Big Data. Our discussion can be useful to the leaders of corporations, their stakeholders, lawmakers and others as they grapple with cyber-security and the other problems posed by Big Data.

Keywords: AIS; IT; Big Data; Hacking; Normative Ethics; Kantian Ethics; and Stakeholder Theory.

INTRODUCTION

Modern big business has adapted, albeit slowly, hesitantly and at times incompletely, to societal demands for corporate accountability and responsibility including safe products, fair labor conditions, environmental protections, reliable financial statements and effective corporate governance. In the current period, forces have emerged that spark important questions regarding examining the self-interests of firms and the interests of a broader group of stakeholders, including society at large. In Accounting Information Systems (AIS), these forces involve the tension between gathering and protecting private individual data with the ability of firms to extract instead of value of all this vast data. Margaret Lynch states “information is a source of power and, increasingly, the key to prosperity among those with access to it. Consequently, developments in information systems also involve social and political relationships— and so make ethical considerations in how information is used all the more important. Electronic systems now reach into all levels of government, into the workplace, and into private lives to such an extent that even people without access to these systems are affected in significant ways by them. New ethical and legal decisions are necessary to balance the needs and rights of everyone.” (Lynch, 2016).

With respect to public corporations, CFOs and Controllers are keenly attune to the needs and sensitivities of the public capital markets as their responsibilities include the integrity of timely public financial disclosures and balancing these disclosures with judgments regarding a firm’s private information. Many of these individuals are CPAs (Certified Public Accountants) who are well schooled in the public interest focus. In addition, given evolving forms of cybercrime, that for very large and important companies has a significant impact to the public welfare, the business must also be constrained by considerations of public interest. These developments present accounting organizations and leaders with radically new and expanded challenges compared with the far simpler time of recording and reporting upon a finite set of transactions whose details were ensconced on a firms’ mainframe computer or even on paper in a bygone era. These are new challenges, but not the first the accounting profession has had to resolve. At different points in time, ethical issues affected accounting. In 1930, the financial crisis resulted in the birth of Auditing and the enactment of the Securities Act of 1933 followed by the Securities Act of 1934; the crisis of confidence of 2000 led to the Sarbanes-Oxley Act of 2002; and the crisis of 2008 resulted in the Dodd-Frank Consumer Protection Act of 2010. A common element of all these crises affecting business ethics is that policy-setters reacted after the damage was inflicted. With the widespread challenges posed by the new AIS environment, perhaps it is time to take a more proactive approach to look for solutions involving regulation, monitoring or enforcement rather than waiting until after the economy and the public trust are destroyed. In this paper, we discuss some of the challenges and ethical issues posed by Big Data and present several possible solutions for corporations.

The advent and proliferation of powerful, important and revolutionary technological developments that enable corporate entities to amass, analyze and share vast amounts of granular customer, supplier, employee and investor data in sophisticated 4th generation AIS poses complex new challenges. As a consequence of collecting, storing and using Big Data, these challenges include understanding, from an ethical perspective, the duties, responsibilities and implications faced by corporate entities and their senior executives. This raises many questions, several of which are as follows: 1) Whose interests are paramount - a corporate entity in search of a competitive advantage by collecting and mining data or an individual who wishes to keep her data private? 2) What safeguards must a firm put in place to ensure that the data is safe from cyber hacking? 3) What responsibilities and leadership role in a firm should CFO's and Controllers have in ensuring that the data they "own" in the AIS is safe from abuse? 4) Should CFO's and controllers cede responsibility for these matters to technology executives, information system and marketing executives or do the senior leaders of accounting organizations have a responsibility to take on an active leadership role as these challenges are addressed? In this paper we raise these and other questions and bring to the forefront the ethical dimensions of this new paradigm with a particular focus on the leadership of accounting organizations.

BACKGROUND

Development and Expansion of AIS systems - key technological advances and trends

Accounting records can be traced back over 70,000 years in Africa, and to 3000 BC with Mesopotamian record keeping (Sy & Tinker, 2006) The system of notched sticks and carved stones representing tallies in the agrarian age, evolved to Pacioli's double entry bookkeeping in the mercantile age (Brown & Johnson, 1963), to enterprise resource planning (ERP) systems in the last decades, and to finally include the use of cloud computing in the current times. Regarding the amount of data handled by accounting systems, Pacioli's double entry bookkeeping produced an increase in the amount of information collected, but it is not comparable with the increase produced by the development of information technology. While double entry bookkeeping included only accounting data, current ERP systems collect non-accounting data as well. Furthermore, the negligible cost of data storage as well as the development of e-business has produced an increase of data collected by companies with no specific immediate purpose. For example, companies are collecting data about customers and their preferences with a marketing purpose, but many times without having tools or specific plans for analyzing such big data. Another example is the overwhelming existence of medical centers developing their own portals and requiring users to open an account to access their appointments, examination results, etc. As Cukier & Mayer-Schoenberger (2013) state: "Today, when we gather all the data, we do not need to know beforehand what we plan to use it for." With new sources of data, and the possibility to access it in a browser, the risk of hacker attacks has increased (Cukier & Mayer-Schonberger, 2013). Warren, Moffitt, & Byrnes (2015) highlight how automatic sensor devices and machine to machine communications continuously increases the amount of data, and that organizations collected more data during the past two years than in the previous 2,000 years (Syed, Gillela, & Venugupal, 2013). This impressive increase in data requires new storage with higher capacity. Companies' storage in 2015 vary between dozens and hundreds of terabytes (Vasarhelyi, Kogan, & Tuttle, 2015).

Given the need to increase storage and processing capabilities, companies are currently adopting Cloud computing. The National Institute of Standards and Technology (NIST) defines Cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST, 2011). It generates additional problems because service providers do not have access to the physical security system of data centers, and they must rely on the infrastructure provider (Zhang, Cheng, & Boutaba, 2010).

Hence, Cloud Computing is also increasing the security risks of data collected by companies and thereby raising ethical questions related to extracting value from data versus more cautiously protecting privacy and security. Can both extracting Big Data while at the same time achieving privacy and security be achieved? Further, who, in an organization will be charged with balancing these choices? Cloud computing has been defined as both a threat and an irresistible opportunity (Weinman, 2012) and also seen as a provider of wide bandwidth and distributed storage (Moffitt & Vasarhelyi, 2013).

VULNERALITIES EXPOSED

During the last decade we have witnessed a proliferation of hacking attacks to personal data in corporate databases. A hacker is defined as someone who breaks in a computer system because of their knowledge to identify weaknesses in a system and their proficiency in programming (Lamprecht, 2004). According to Privacy Rights Clearinghouse (PRC), instances of hacking go back to 2005, when a laptop from Ameriprise Financial was stolen, giving illegitimate access to 220,000 customer records (Clearinghouse, 2016). That same year, different universities were hacked (e.g. University of California at San Diego, University of Northern Colorado), resulting in the stealing of student and employees data. The number of breaches to security reported in this period, only considering hacking and malware, was over 10 thousand. The most relevant cases during the 2005-2014 periods include the following: In 2006, the AOL Data Valdez scandal gave access to data from 650,000 members. In January 2007, the TJ Maxx companies were hacked and data from 45 million credit and debit cards were stolen. In January 2008, GE Money, a subsidiary of General Electric, reported a magnetic tape file missing which contained credit card information from 650,000 customers as well as 150,000 social security numbers. In January 2009, Heartland Payment Systems was the victim of a security breach at a global level. This was the largest at that time, with an estimate of 100 million cards compromised. In December, a Rockyou! Company's Password database was hacked and 32 million user names and passwords were stolen. In April 2010, General Motors reported that a file containing social security numbers, names and emails was mistakenly sent to an unauthorized party. In April 2011, ITunes users reported fraudulent purchases using their accounts. Simultaneously, Sony identified an external intrusion in their databases affecting 77 million users. In June of that same year, Citigroup reported a breach in their credit card operations affecting 210,000 users. In October 2012 it was discovered that since August of the same year, an estimated 3.6 million social security numbers were compromised from the South Carolina Department of Revenue. In 2013 Target Corporation disclosed that data from 40 million credit and debit cards was stolen. This was the largest breach since the TJMax's breach in 2007. Finally, in September 2014, Home Depot suffered a data breach of 56 million credit card numbers, and Staples of 1.16 million customer payment cards.

It is clear that over the last decade, data breaches have been rampant. In fact, cyber security attacks increased by over 50% in 2014 compared to 2013 (Hatstand, 2015). This display of breaches raises questions regarding the diligence of companies in securing customer's data, given that the threats now are more vicious and smarter than ever before. In their recent white paper, the financial technology firm Hatstand, states that "businesses need to have sound governance practices in place and recognize that cyber security is more than just an IT related issue" (Hatstand, 2015). The broader dissemination of hacking abilities has raised new ethical issues and responsibilities for firms. These breaches are costly for companies. For example, Data Valdez paid a $5 million settlement and Target's total cost related to its breach was over $146 million. We therefore contend that cybersecurity is not purely a matter of protection of the interests of the firm, but a broader interest of the corporation, which is to live up to the ethical responsibilities to customers and even society.

BIG DATA

Who are is guardians?

Of critical importance for the analysis is this paper, we argue that Big Data also changes managers' attributes from collectors of information about accounting transactions to guardians of personal data of third parties. The Stamford, Connecticut-based IT research firm Gartner Inc. defines "big data" as "high-volume, velocity and/or variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making and process automation."[1] Other experts point out that big data might include unstructured textual information from social media sites, machine-generated log data and a host of other information collected by cloud applications, on-premises applications and websites.

Big data can also be defined as data that "exceeds the reach of commonly used hardware environments and software tools to capture, manage, and process it within a tolerable elapsed time for its user population" (Gartner, 2011). Big data offers the potential of diverse, voluminous datasets that allow sophisticated analysis, and that will significantly impact accounting (Warren, Moffitt, & Byrnes, 2015). The amount of digital data companies handle increased from 25% in 2000 to over 98% in 2013 (Cukier & Mayer-Schonberger, 2013) and changed in format and quantity of data affected collection, storage, processing and reporting.

While big data can be defined in technical computer processing terms, big data can also be thought of in social rather than technical terms (Richards & King, 2014). Major transformations are projected to occur in society as a result of this transformative development. Successful, sustainable businesses operate within a framework of business ethics that instills customers, shareholders, employees and all stakeholders with confidence that the motivation of business managers is not purely their self-interest profit motive. The developments of Big Data in business may very well parallel the explosion of data in astronomy as described in the following quotation.

"When the Sloan Digital Sky Survey began in 2000, its telescope in New Mexico collected more data in its first few weeks than had been amassed in the entire history of astronomy. By 2001, the survey's archive teemed with a whopping 140 terabytes of information. But a successor, the Large Synoptic Survey Telescope in Chile, due to come on stream in 2016, will acquire that quality of data every five days." (Mayer-Schonberger & Cukier, 2014).

The advent of vast, searchable accumulations of data from customers, prospective customers, investors, etc. motivates analysis and deep thinking about the ethical implications of big data.

ETHICAL IMPLICATIONS OF AIS & BIG DATA

The implications of AIS and Big Data can be discussed in relation to various ethical theories, such as the pursuit of profits by Friedman, Kantian normative business ethics, and the Stakeholder Theory as discussed in the following paragraphs.

Different definitions of ethics are available in literature. Paul & Elder (2013) state that ethics is not a subjective matter and discuss its relationship with behavior. How the behavior of a group affects the well-being of other groups. The Oxford English dictionary (2017) defines ethics as: "The branch of knowledge or study dealing with moral principles." Similarly, Webster's Dictionary (2017) states it is "the discipline dealing with what is good and bad and with moral duty and obligation" as well as" a set of moral principles."

Pursuit of Profits – Friedman

The academic discipline of business ethics developed in recent decades as the classical economic norm, which embraced the unencumbered pursuit of profits, proved inadequate in keeping pace with abuses, scandals and societal outrage that accompanied the industrial and post-industrial eras. This economic norm was most famously championed by acclaimed economist Milton Friedman who stated in 1970 that "the one and only" social responsibility of business is to increase profits (Friedman, 1970) . Friedman's thesis is linked to and builds upon the laissez-faire philosophy of Adam Smith and posits that allowing producers to produce whatever they believe will earn them the most profit, while consumers are free to buy the products they value the most, provides the best outcomes for society (Smith, 1976). According to this view, the free market is most effective for the allocation of scarse resources and improving the general welfare. Business firms have an important and unique role to play in this free-market process. In the pursuit of profits, firms productively use labor, capital, natural resources, and human knowledge to create wealth for society (Friedman, 1970). The more profits businesses earn, the more wealth they create for society. Conversely, firms that do not create social value are vulnerable to going out of business when there is no demand for their goods and services. Applied to the current challenges and risks, information must now be added to the core ingredients of labor, capital and natural resources. A free market approach to the widespread proliferation and value of data capture, use and sharing, may result in simply allowing the unfettered use of data by firms for their own self-interest and waiting for market influences to dictate actions and consequences. For example, if the Target Company fails to protect customer data and then cyber hackers steal such data, then Target will suffer the consequences. They will then address such problems, and others will learn and move on. As described above, this reactionary approach is quite risky for society and we argue that a deeper analysis of the way the business should think proactively about the impact of the data housed in accounting information systems on stakeholders and society at large is needed.

Business Ethics Normative - Kantian

At the forefront in the development of business ethics from a normative perspective was Norman Bowie, a leading business ethicist, whose seminal work applies the philosophies of Kant to business. He started a stream of research which analyzes questions by focusing and clarifying the way business ought to be conducted, generally basing analysis and arguments upon core ethical philosophies. Kantian moral calculus centers on rational motivation and duty. Human actions are judged to be moral if they are based on a rational motivation which is derived from one's sense of duty (N Bowie, 1998; N.E. Bowie, 1999). Duty, in part, is rooted in universal acceptance. Similarly, legitimacy theory supports the existence of a "social contract" by which companies behave in such a way so that society recognizes them as socially responsible (O'Donovan, 2002). When the society perceives that a company's behavior is not adequate, a legitimacy gap may develop (Branco & Rodrigues, 2006).

This normative approach suggests that companies will protect the data they hold because it is their duty, and if data are not adequately taken care of, the legitimacy gap will produce a lack of confidence in the company, with the subsequent loss in profitability.

Stakeholder Theory - Freeman

A seminal work by Ed Freeman in 1984 introduced the concept of stakeholders and stakeholder theories to business. This theory states that business must not operate solely for the profits to be earned by shareholders but in the best interests of a broad range of stakeholders including customers, employees, suppliers etc. Hence, a broad cross-section of interests must be considered by business organizations in the pursuit of profits.

With respect to AIS, the constituencies are quite diverse. First and foremost are the interests of the firm, the corporate entity.

Working with stakeholder theory as a primary grounding for the arguments in this paper, we also draw upon the work of French (1979), who constructs a model for the concept that corporations are moral agents, i.e., the corporations themselves are responsible, and not purely the individuals involved.

While it is generally accepted and understood, as an aspect of moral philosophy and ethics, that individuals have moral responsibility for their behavior, accepting the moral responsibly of institutions, continues to be the subject of ongoing analysis. Soares (2003) has argued that consideration of the interests of society must be recognized by institutions, given the complexity of modern economic activity. Such institutions need to recognize their moral responsibilities. He argues that corporations have a collective or corporate social responsibility to take into account society and its problems.

As the literature examining corporate moral responsibility evolves, substantial research has moved beyond the basic question of whether corporations have moral responsibility, to discussing the nature of such moral dimension (Wettstein, 2010). Philosophical or conceptual aspect of corporate morality is the link between the operating practices of corporations, including financial institutions, and their corporate morality that provides the means for converting moral hazard into real hazards for stakeholders including society at large. The operating means exist in corporations to implement decisions, and French (1979) posits that it is precisely the corporate organization's structures which enable implementation of decisions, and such decision-support structure provides an important basis for applying moral agency to corporations (French, 1979). The focus here is particularly on the accounting organizations, the accounting information systems and the leadership of these activities.

In addition to the corporate entity, other stakeholders impacted by the moral calculus involving data housed in large organizations, includes private individuals. These are citizens whose personal data may have been collected and housed in the AIS of a firm by virtue of the fact that the individual is a customer, shareholder, employee or supplier of a firm.

The fundamental questions raised in this paper relate to clarifying the ethical aspects of the judgments involved in balancing protocols, protections, and limitations as firms pursue extracting value from the vast data that they possess.

ETHICAL ANALYSIS

A fundamental component in the ethical analysis of an Accounting Information System relates to privacy.

Privacy

Privacy has previously been described as: "an interaction, in which the rights of different parties collide" (Noam, 1997). It is not about secrecy, but about control of personal information. Who will have control over the access to an individual's private information? Under what conditions and circumstances does a firm have the ongoing right to access and use the private information, gathered from a customer, employee, supplier etc.?

In a frequently quoted statement by a Supreme Court justice on the subject of privacy, Justice Brandeis's dissent in Olmstead v. U. S. (1928) included the following:

"The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men… Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language . . . " (Brandeis, 1928).

This quote is frequently cited in discussions regarding privacy and is a cornerstone concept in the US democracy where the right to be left alone is constitutionally protected. Does this right extend to private information? Is it morally wrong for a firm to use for their benefit the data provided by customers, suppliers, etc.? Under what circumstances and with what protocols would it be acceptable for firms to use private data?

Kantian moral calculus centers on rational motivation and duty. Human actions are judged to be moral if they are based on a rational motivation which is derived from one's sense of duty (N Bowie, 1998; NE Bowie, 1999). Duty, in part, is rooted in universal acceptance and in this regard people are to be treated as means, not ends. In the case of the use of private information by corporate entities, unauthorized uses of private information foster misalignment of interests between customers, shareholders, employees and a firm. It raises questions as to whether executives' short-term self-interests have overtaken customer interests. An important series of questions must be answered by each firm with respect to the personal data that it collects and houses, from customers, suppliers, investors, etc.

As new uses for data develop, current privacy protection laws that emphasize "notice and consent" may prove inadequate. Developed in an era when the data from customers was merely captured and retained in hard wired computers. With the new frontier in AIS, how can adequate privacy consent be provided by an individual if the ways in which the data will be used has yet to be determined? Some may argue that these are questions of law and technology, yet we argue here that it is financial executives who have a unique and important perspective to contribute to this evolution. Given the factors that need to be considered when making judgments regarding the value of mining big data, it is crucial that the executives involved have a deep knowledge and understanding of the public's interest. In this regard, the focus of CFO's and Controllers, particularly of public firms, who are generally CPAs must be the concept of the "public interest." In fact, as part of their core values and training, CPAs are required to abide by the AICPA Code of Conduct which includes the following with respect to the public interest:

> ".01 The public interest principle. Members should accept the obligation to act in a way that will serve the public interest, honor the public trust, and demonstrate a commitment to professionalism.
>
> .02 A distinguishing mark of a profession is acceptance of its responsibility to the public. The accounting profession's public consists of *clients*, credit grantors, governments, employers, investors, the business and financial community, and others who rely on the objectivity and integrity of *members* to maintain the orderly functioning of commerce. This reliance imposes a public interest responsibility on *members*. The public interest is defined as the collective well-being of the community of people and institutions that the profession serves."[2].

There are methods that have been developed to better protect the data from misuse and abuse. Included among these is the process of de-identification. It has been defined as:

> "The process of altering and/or removing identifiers from personal information prior to its use or disclosure. It enables the protection of individual privacy while also permitting other secondary uses of the de-identified information. De-identification involves removing direct identifiers, variables that provide an explicit link to a person and can directly identify an individual, for example name, email address, home address, telephone number, health insurance number and social insurance number. However, removing only direct identifiers is insufficient to ensure that the information truly protects individual privacy. It is also important to deal with quasi-identifiers." (Design, 2015)

Another alternative for controlling personal information is self-determination. In 1983 Germany introduced the important concept of information self-determination into the formal government census, as individuals were resistant to complying with the data requests included in the census. It reinforces the individual's right to control the dissemination and use of private information (Hornung & Schnabel, 2009).

CYBER SECURITY

Clearly, breaches of security with hackers penetrating computer security systems raises issues and threats that firms must address. In fact, the way that businesses are run has to be altered in the best interest of the owner (the shareholders). These include Codes of Ethics for Information System (IS) practitioners, issues of privacy and security, combating of cybercrime, intellectual property disputes, free and open software, hacking, and the digital divide as a form of social exclusion. Issues such as these are discussed in existing literature (for example, Himma & Tavani, 2008; Tavani, 2007; van den Hoven & Weckert, 2008), but much of this work is not published nor widely cited in the mainstream IS literature. Indeed it can be argued that the core IS field, based on publications in journals such as MIS Quarterly, is under representative of ethics and IS, bearing in mind the importance of this subfield.

IMPLICATIONS

We argue that the proliferation of sophisticated technology that allows for massive, interconnected systems that house and analyze individual customers, suppliers, employees, and investors data, throughout the accounting information systems of a firm, must have a profound and fundamental impact on the role and responsibilities of firms and senior accounting personnel to carefully guard and protect such data, as well as understand the social and ethical implications of such power. We argue that there is a need to focus, examine, explore and clarify the ethical responsibilities that accounting organizations and their leadership, namely CFO's and controllers have as a result of "owning" such data; data that is housed in a firm's accounting information systems.

Furthermore, CFO's and controllers need to urgently leverage and expand their expertise and develop a deep understanding of the ethical responsibilities that firms have as a result of the complexity, vulnerability and importance of data captured and housed in AIS. Not only must firms now continue to be supremely competent on matters of internal control, treasury, financial reporting and the like, but these firms must fully understand and inculcate an ethic that takes responsibility and addresses the new challenges that have surfaced for the operations of the AIS under their control.

CONCLUSION

In this paper, we undertake a discussion related to the ethical implications of the responsibility of Corporations and the new AIS environment in light of various ethical theories. We contend that Corporate CFO's and Controllers must increase their competence in a host of IT related areas and must be cognizant of their duty to protect their stakeholders and the general public. Furthermore, laws related to the protection of the information of consumers were developed in response to certain specific financial crises and are now incapable of addressing the new Big Data environment. It is therefore incumbent on corporations, regulators and standard setters to be more proactive rather than reactive in addressing the challenges posed by the current crucial frontier in AIS as it relates to the protection of the information of customers, suppliers, financial statement users and the general public. By doing so, the interests and privacy of the people who corporate executives are charged with serving will be safeguarded.

REFERENCES

[1] Bowie, N. (1998). A Kantian theory of capitalism. *Business Ethics Quarterly*, 8, 37-60.

[2] Bowie, N. E. (1999). *Business ethics: A Kantian perspective*. Malden, Mass: Blackwell.

[3] Brandeis, L. (1928). *Olmstead v. United States, 277 U.S. 438*. Retrieved from http://www.fjc.gov/history/home.nsf/page/tu_olmstead_doc_15.html.

[4] Branco, M. C., and L. L. Rodrigues. 2000. Corporate social responsibility and resource-based perspectives, *Journal of Business Ethics* 69(2): 111-132.

[5] Brown, R. G., & Johnson, K. S. (1963). *Pacioli on accounting*. New York: McGraw-Hill.

[6] Clearinghouse, P. R. (2016). Data Breaches Retrieved October 23, 2016, from http://www.privacyrights.org/data-breach.

[7] Cukier, K., & Mayer-Schonberger, V. (2013). The rise of big data. *Foreign Affairs*, May/June, 28-40.

[8] Design, P. (2015) Retrieved October 26, 2015, from: https://www.privacybydesign.ca/index.php/de-identification-centre/about-de-identification/.

[9] Friedman, M. (1970). The social responsibility of business is to increase its profits, *The New York Times*.

[10] Gartner. (2011). CEO advisory "big data" equals big opportunity. *Gartner Web Site* Retrieved October 5, 2015, from www.gartner.com/id=1614215.

[11] Hatstand. (2015). Demonstrating cybersecurity readiness to regulators. *Web Site* Retrieved October 10, 2015, from: www.automatedtrader.net/news.at.154381/demonstrating-cybersecurity-readiness-to-regulators-hatsand.

[12] Himma, K. and Tavani, H. (2008). *The Handbook of Information and Computer Ethics*. Wiley.

[13] Hornung, G., & Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law and Security Review: The International Journal of Technology and Practice, 25*, 84-88. doi: 10.1016/j.clsr.2008.11.002.

[14] Lynch, M. (2016). Ethical Issues in Electronic Information Systems. Retrieved from http://www.colorado.edu/geography/gcraft/notes/ethics/ethics_f.html.

[15] Mayer-Schonberger, V., & Cukier, K. (2014). *Big data: A revolution that will transform how we live, work and think*. New York: Houghton Mifflin Harcourt.

[16] Moffitt, K., & Vasarhelyi, M. (2013). AIS in an age of big data. *Journal of Information Systems, 27*(2), 1-19.

[17] NIST. (2011). The National Institute of Standards and Technology definition of cloud computing. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[18] Noam (1997) available at: http://www.citi.columbia.edu/elinoam/articles/priv_self.htm.

[19] O'Donovan, G., (2002). Environmental disclosures in the annual report: Extending the applicability and predictive power of legitimacy theory. *Accounting, Auditing and Accountability Journal* 15(3), 344–371.

[20] Richards, N. M., & King, J. H. (2014). Big Data Ethics. *Wake Forest Law Review,* 49(2), 393-432.

[21] Smith, A. (1976). *An Inquiry into the Nature and Causes of the Wealth of Nations* Chicago: University of Chicago Press.

[22] Soares, C. (2003). Corporate versus individual moral responsibility. *Journal of Business Ethics* 46.2 (2003): 143-150.

[23] Sy, A., & Tinker, A. (2006). Bury pacioli in africa: a bookkeeper's reification of accountancy. *Abacus*, 45, 105-127.

[24] Syed, A. R., Gillela, K., & Venugupal, C. (2013). The future revolution in big data. *International Journal of Advanced Research in Computer and Communication Engineering, 2*(6), 2446-2551.

[25] Tavani, H. (2007). *Ethics and Technology: Controversies, Questions and Strategies for Ethical Computing.* Wiley Global Education.

[26] van den Hoven, J. & Weckert, J. (2008) *Information Technology and Moral Philosophy.* Cambridge University Press. New York, NY.

[27] Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big Data in Accounting: An Overview. *Accounting Horizons*, 29(2), 381-396. doi: 10.2308/acch-51071.

[28] Warren, D., Moffitt, K., & Byrnes, P. (2015). How big data will change accounting. *Accounting Horizons, 29*(s), 397-407.

[29] Weinman, J. (2012). *Cloudonomics:The business value of cloud computing*": John Wiley & Sons.

[30] Wettstein, F. (2010) The Duty to Protect: Corporate Complicity, Political Responsibility, and Human Rights Advocacy. *Journal of business ethics* 96:33–47.

[31] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state of the art and research challenges. *Journal of internet services and applications,* 1(1), 7-18.