JOURNAL OF INFORMATION SYSTEMS
Vol. 31, No. 2
Summer 2017
pp. 65–81

American Accounting Association
DOI: 10.2308/isys-51265

Accounting Information Systems and Ethics Research: Review, Synthesis, and the Future

Binod Guragai
Nicholas C. Hunt
University of Nevada, Reno

Marc P. Neri
Texas Christian University

Eileen Z. Taylor
North Carolina State University

ABSTRACT: The rapid evolution of technology and the increasingly integrated nature of Accounting Information Systems (AIS) in business provide opportunities for those who interact with these systems to act unethically. Accountants, as the managers of accounting information systems and gatekeepers of assets, records, and reporting, have a responsibility to understand and address ethical dilemmas related to these responsibilities in their organizations. A summary of AIS and ethics research calls attention to gaps in the literature and provides directions for future research. The ETHOs framework, which categorizes factors as environmental, technological, human, and organizational, provides a model for researchers to examine ethical issues related to the AIS functions of recordkeeping, reporting, and control.

Keywords: accounting information systems; ethics; data management; judgment and decision making; outsourcing; privacy; security; information technology.

I. INTRODUCTION

This paper examines the intersection of accounting information systems (AIS) and ethics by reviewing existing literature, proposing a research framework, and suggesting future research ideas. AIS, a critical component of business operations, comprise many interrelated elements (i.e., people, procedures, data, software, hardware, and controls) that identify, collect, store, manage, and communicate accounting data. These recordkeeping functions enable organizations to report data and information to internal and external parties, and to control activities (e.g., safeguard assets, limit individuals' actions). The foundation of ethics is the understanding of how our behavior affects the well-being of others (Paul and Elder 2013). Because people are key elements in AIS, and because managers, regulators, investors, and others use information from AIS to make decisions that affect others (e.g., contracting, hiring, investing, purchasing, and selling), virtually every aspect of AIS has ethical implications.

Although many think of AIS primarily as automated, whenever people interact with a system, from development through use, unethical decisions and behavior are a risk. There are several links between AIS and unethical behavior. First, accountants may use systems to engage in (i.e., commit, convert, and conceal) occupational fraud.[1] Second, accountants may use systems to

We thank Roger Debreceny, Mary Curtis, anonymous reviewers, and participants at the 2015 Midyear Meeting of the Accounting Information Systems Section of the AAA for their helpful suggestions and comments.

Supplemental material can be accessed by clicking the link in Appendix A.

Editor's note: Accepted by Roger S. Debreceny.

Submitted: October 2014
Accepted: August 2015
Published Online: August 2015

[1] According to the Association of Certified Fraud Examiners (ACFE), occupational fraud includes asset misappropriation (e.g., fraudulent billing, payroll fraud, and expense reimbursement fraud), corruption, and fraudulent financial reporting (i.e., intentional manipulation of reported information, either its content, or its form, or both).

violate individuals' privacy by collecting, storing, selling, and using these data for unauthorized, self-serving, or unethical purposes. Third, technology-based systems may enable individuals to engage in unethical practices over others, such as unauthorized monitoring. Last, systems themselves, even the mere existence of a system (Hannan, Rankin, and Towry 2006), can lead to deskilling or may bias an accountant's moral judgment, by either clouding their awareness of wrongdoing or altering their evaluation of what is right or wrong. Systems, especially computer-based systems, may precipitate unethical outcomes by allowing individuals to distance themselves from their actions, obfuscating ethical aspects and enabling unjust rationalizations for unethical actions. The more technology evolves, the farther the actor is removed "from the consequences of organizationally sanctioned" actions (Dillard 2003, 13), reducing personal responsibility and enabling neutralizations. In other words, systems legitimize individual wrongdoing by allowing people to focus on their duties within the system, without consideration of the moral impact of their actions (Adams and Balfour 1998). A striking example of this occurred when a German subsidiary of IBM helped Hitler's Third Reich carry out the Holocaust by providing technology that allowed the Germans to catalog Jewish and other citizens through people counting and registration technologies (Black and Wallace 2001; Dillard 2003). By treating people as inventory, the Third Reich dehumanized them, allowing Nazis to distance themselves from their actions of mass extermination.

More recently, individuals acting for themselves and individuals acting as organizational agents have used AIS to violate individual privacy, misappropriate business assets, and falsify accounting data to meet organizational goals and market expectations. In the late 1990s and early 2000s, executives at WorldCom pressured accounting staff to use their AIS to perpetrate financial statement fraud, misclassifying expenses as assets, and hiding hundreds of entries from the internal and external auditors (Cooper 2009). Satyam Computer Services used its AIS to create ghost employees and falsify sales orders in order to conceal a massive accounting fraud perpetrated by its executives (Rai 2014). Last, United States (U.S.) government employees (i.e., Veteran's Administration managers) entered false data within their systems, altering waiting times for military veterans' healthcare appointments to portray more favorable statistics and earn performance-based bonuses (Bronstein, Griffin, and Black 2014). These examples demonstrate the harm enabled by modern AIS.

The link between AIS and ethics, in which AIS enable individuals to act unethically, is heightened by two aspects. They are the increasingly integrated role of AIS in organizations, and society's expectations that professional accountants will act in the public interest (Copeland 2005). AIS have grown from simple bookkeeping tools to integrated enterprise resource planning (ERP) systems. The focus of AIS has gone from making existing processes more efficient, to designing systems to take strategic advantage of IS/IT capabilities, to addressing risks associated with managing, retaining, and securing the data that organizations collect and report (Brancheau and Wetherbe 1987; Brancheau, Janz, and Wetherbe 1996; Beard and Wen 2007; AICPA 2013b). While earlier systems were relatively limited recorders and reporters of data, due to rapid technological advances, AIS are now powerful systems that integrate myriad functions within a business (e.g., accounting, human resources, production, and supply chain). Early ERP systems focused on resource optimization and transaction processing. ERP II expands these functions to leverage information from business-to-business (B2B) and business-to-consumer (B2C) electronic commerce (Bond et al. 2000).[2] Because ERP II systems increase the touchpoints where individuals interact with them, they enable new opportunities for individuals who design, implement, and interact with them to intentionally and to unintentionally cause harm. In short, the integration and reach of modern AIS enable unethical behavior.

Understanding the link between AIS and ethics is particularly important for accountants, as they have a role as protectors of the public interest. Accountants of all types have a long history of being the designated recordkeepers and asset guardians for businesses and governments alike (Soll 2014). Per the Institute of Internal Auditors (IIA) Code of Ethics, internal auditors have an obligation to maintain integrity, abide by the laws, act in an ethical manner, and exercise objectivity in reporting. External auditors abide by a Code of Professional Conduct that places the public interest at the forefront (AICPA 2013a). Audit committees, which typically comprise accountants, are responsible for enterprise risk management, for reporting to external parties, for the control environment and control activities, as well as for monitoring activities (COSO 2013). Further, audit committees now, more than ever, are overseeing controls related to compliance and operational matters (Deloitte 2014), as well as matters of risk oversight (Rapoport and Lublin 2015). The designated role of accountants as controllers necessitates our involvement, as AIS researchers and professionals, in understanding and addressing these issues.

After a brief history punctuated by rapid change, AIS are at an unavoidable crossroads with ethics. Given AIS's ubiquity and power, and accountants' roles as recordkeepers, reporters, and asset protectors, academics, as creators of knowledge and investigators of social phenomena in the accounting and information systems' space, have an obligation to examine and work to understand these issues. Further, using technology to perform tasks has been found to influence peoples' ethical decisions in both positive and negative ways (Hunt and Iyer 2015). We cannot afford to ignore their potential for harm, both intentional and

[2] All major ERP vendors (e.g., SAP, Oracle, PeopleSoft) have adopted the concept of ERP II to help customers meet today's business challenges (Møller 2005).

unintentional. This paper aids in our understanding of the implications of AIS on ethical issues by cataloging the existing research on AIS and ethics, identifying gaps in the literature, creating a framework for the study of AIS and ethics based on a four-factor categorization, and posing relevant questions for future research.

II. DEFINING THE BOUNDARIES OF THE PAPER

Ethics

Ethics encompass an individual's values, integrity, and courage. Values guide a person's moral decisions, integrity is the consistency with which they apply their values (i.e., relative to time, place), and courage is the ability to convert values to actions, notably in the presence of threats, both physical and intellectual (Gentile 2012; Kidder 2005). We define ethics using a universal approach. Unethical actions are those judgments and behaviors enacted by humans (individuals or groups) that "inherently deny another person or creature some inalienable right" (Paul and Elder 2013, 14). Human rights include life, freedom, and security (among others), to all, without distinction of any kind (e.g., race, color, sex, religion, status) (United Nations 1948).

The purpose of ethics, and of making ethical decisions, is to help, rather than harm others, making it a social construct (Paul and Elder 2013). As part of their express duties toward citizens, governments typically regulate acts that are unethical in and of themselves (such as murder, fraud, and intimidation). However, social norms, which may vary between communities, also play a part in communicating ethical standards. For example, professional accounting societies and regulatory bodies enact differing codes of conduct governing the duties of a professional, such as the duty of accountants to serve the public interest, and the general expectation (in the U.S.) of accountants to maintain client confidentiality (AICPA 2014). More recently, governments have been called to respond to technological developments that enable companies to infringe on the rights of private citizens. For example, the Court of Justice of the European Union upheld the complaint of a Spanish citizen's objection to Google including sensitive information about this person in its search results. The court affirmed European Union citizens' "right to be forgotten" (i.e., the ability to remove their digital footprint from the internet) over the objections of internet companies' worries of extra costs (Chee 2014).

This paper broadens the concept of ethics in two ways. First, it considers not only individual decisions and actions, but also includes organizational decisions and actions because AIS' development, implementation, and use are often the result of a group effort and are dependent on the institution's existing structure. Thus, individuals at times act unethically for their own direct personal benefit; at other times, they act on behalf of their organizations, or as part of a group, indirectly for their own personal benefit (Cohen, Manzon, and Zamora 2015). Second, it categorizes violations of generally accepted social norms as unethical, recognizing that professional standards may go beyond basic human rights, but are legitimately valid considerations within the profession. For example, there is an expectation that a professional accountant has a higher standard to protect the public interest than does any individual citizen.

Accounting Information Systems

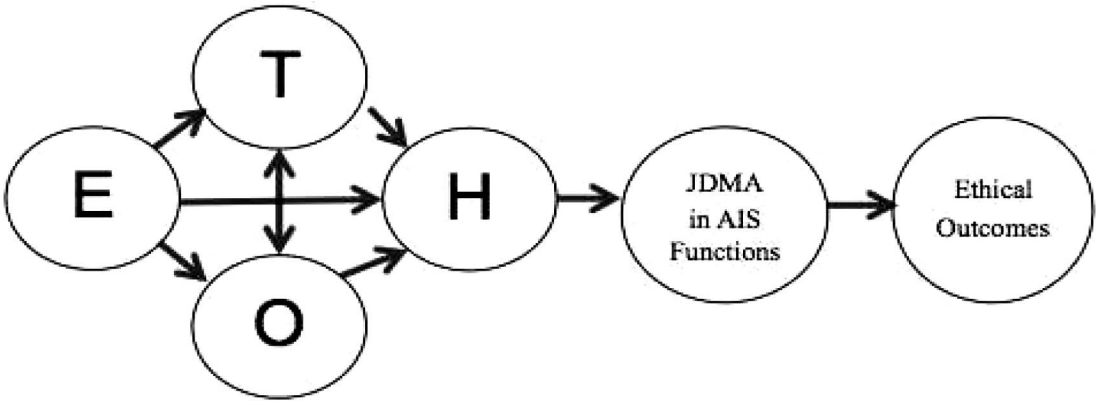
We organize the paper using Romney and Steinbart's (2015) textbook definition: accounting information systems (AIS) are systems that identify, collect, store, manage, and communicate accounting data and information for the purposes of reporting and control. Recordkeeping encompasses the first four activities, while reporting is the communication of data and information to internal and external stakeholders. These reports, generated by AIS, include financial information (e.g., balance sheet and income statement, C-suite compensation, and cost per unit) and nonfinancial information (e.g., number of employees, patents awarded, hours worked). Organizations also use AIS and the processes embedded within them to control both people and assets. Accounting, through its recording function, enables management to identify and hold individuals accountable for their actions. AIS also enable and limit who can engage in certain transactions (e.g., access controls to physical assets and to electronic data and approvals). These controls allow organizations to safeguard assets, produce valid information, and carry out activities efficiently and effectively.

Factor Categories: ETHOs

We classified the existing AIS/Ethics research using a framework (see Figure 1) that includes four types of factors: *environmental, technological, human, and organizational* (ETHOs).[3] *Environmental* factors include standards, rules, expectations, and norms imposed by governments, professional organizations, industry groups, self-regulatory bodies, and

[3] We develop and use the acronym ETHOs (*environmental, technological, human,* and *organizational*) throughout the paper when referring to these factor types.

FIGURE 1
ETHOs Model for AIS/Ethics Research



communities. For example, regulatory factors refer to governments enacting laws influencing the design, use, and governance of AIS, overseeing the implementation of these laws, enforcing these laws, and educating the public about these laws (Boritz and No 2011). *Technological* factors refer to AIS inputs, systems and tool design, and outputs (Neely and Cook 2011). These include hardware, software, and communication tools and their features and capabilities. *Human* factors include people's attitudes, perceptions, culture, group membership, and other individual characteristics that influence their behavior (Pavlou 2011). *Human* factors are influential in ethical decisions regarding privacy, equity, personal responsibility, and identity issues encountered when interacting with AIS (e.g., Clarke 1999; Glass and Wood 1996; Harrington 1996; Sipior, Ward, and Rongione 2004). Last, *organizational* factors "include organizational strategy, structure, and the internal and external business environment," as well as how organizations interact with their environment (Mauldin and Ruchala 1999, 324). They also include decentralization, ethical climate, culture, and approach to self-regulation. Researchers may use the ETHOs framework to both understand existing literature and to identify, develop, and examine relevant research questions related to AIS and ethics.[4]

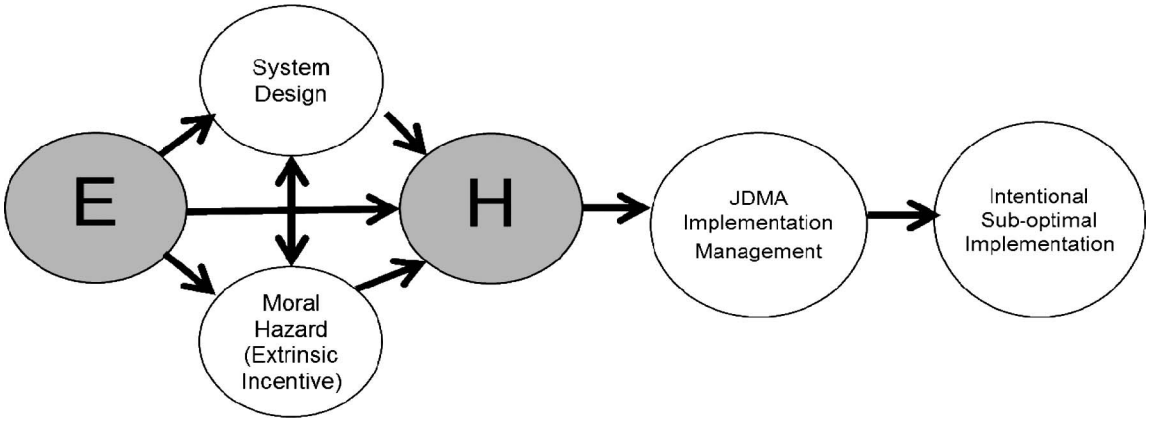
The ETHOs factors influence judgment, decision making, and the actions (JDMA) individuals make when carrying out the AIS functions of recordkeeping, reporting, or control. Recall that these individuals may make these JDMA with the goal of personal, direct benefit (as in asset misappropriation through false billing), or to gain an indirect benefit through the organization, (as in fraudulent financial reporting to meet analyst expectations, eventually resulting in individual benefits including bonuses, stock options, and promotions). We go beyond judgment and decision making, which academics typically use as their dependent variable, to include actions as well.

Ethical outcomes are the measured dependent variables resulting from individuals' JDMA. Note that this is a subjective measure, depending on one's own determination of what is ethical and what is unethical. While there will be general agreement about the ethicality of some outcomes (asset misappropriation [theft] resulting in loss of cash from an organization is unethical), there are other areas that may stimulate valid disagreement. Some could consider income smoothing ethical, as it reduces market volatility, thus lowering transaction costs, and improving efficiency. Others may seriously object to all forms of income smoothing, deeming it unethical and a violation of generally accepted accounting principles. One contribution academics can make is to evaluate outcomes from multiple perspectives, which should lead to a better understanding of their ethical implications.

To show how the ETHOs framework applies to a particular paper, Figure 2 includes an interpretation of Tuttle, Harrell, and Harrison (1997). This study examines the effects of incentives and system design on system implementation. System design is a *technological* factor. Company-provided extrinsic incentives (in this study, bonuses for on-time and within-budget delivery) are an *organizational* factor, which creates a moral hazard for the decision maker. Judgment surrounding the implementation of a new system is affected, resulting in an ethical dilemma: implementation of a suboptimal system. This study does not examine *environmental* and *human* factors that may mitigate the effect of incentives on system implementation decisions. Therefore,

[4] Thanks to Andrea Kelton for proposing this graphical representation in her discussion of this paper at the Midyear Meeting of the 2015 Accounting Information Systems Section of the American Accounting Association.

FIGURE 2
Example of ETHOs Model
Tuttle et al. (1997)



professional standards, experience, and level in the organization are among a number of factors that might be included in future research.

The review proceeds as follows. The next section details our methodology. The following sections address recordkeeping, reporting, and control. In each subsection, we define the area, review relevant ethics-related AIS research and its connection to ETHOs factors, and provide suggestions for future research to fill existing gaps in the literature. Existing research, with variables categorized by ETHOs factor, is available in the online supplemental material (see Appendix A for the link to downloadable Word document).

III. METHODOLOGY

All literature reviews are constrained by limits of space and the qualitative preferences of their authors; this review is intended to be as comprehensive as is possible. We began by reviewing all *Journal of Information Systems* (*JIS*) articles from January 2000 to December 2013 and categorizing these into general areas of AIS research. We then used these areas to develop a list of keywords to categorize the research streams and searched each of these terms in conjunction with the keyword "ethics."

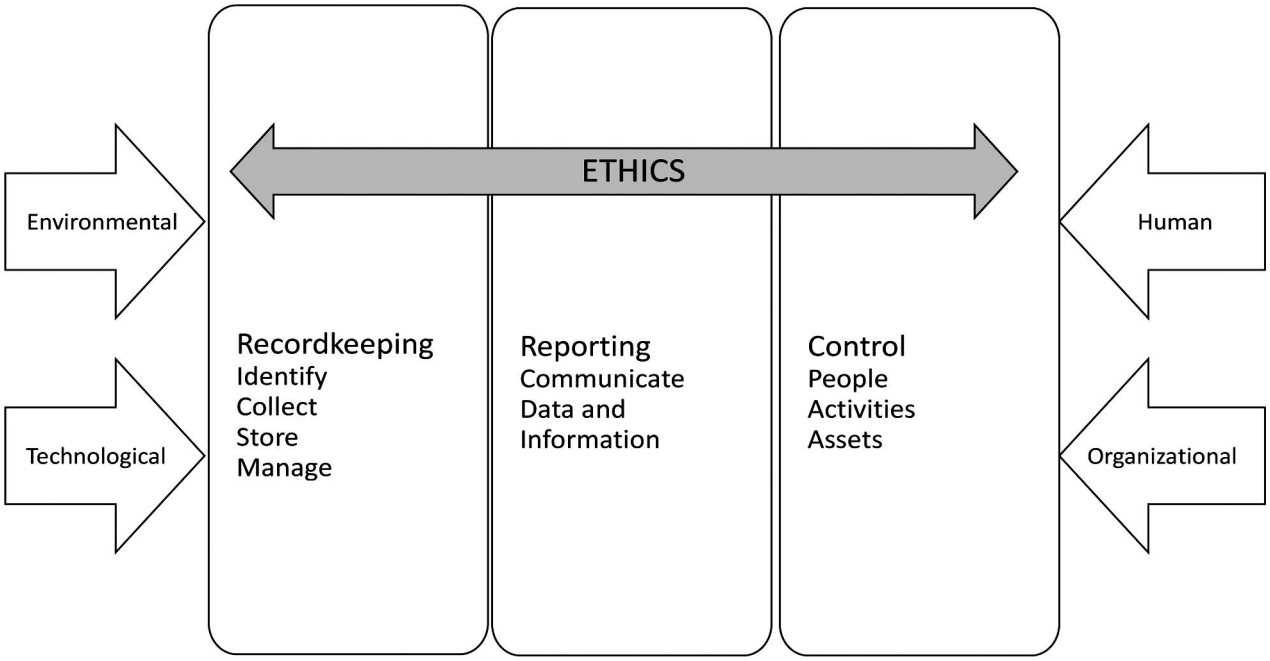
One limitation of this approach is that not all ethics-related research explicitly uses the word "ethics." In fact, throughout our search, ethics is often an implicit, rather than explicit motivation for AIS research. That is, researchers state that they have identified a process, decision, policy, or behavior that is unfair, unjust, biased, obfuscates results, and/or manipulates or takes advantage of individuals, but they do not use the word "ethics." While not all research is ethics related, (some identifies ways to improve efficiency or effectiveness), much research has some underlying motive to reduce harm to others. One early recommendation of this project is that researchers explicitly identify and explain how their research relates to ethics. This action (uncovering and explicating the ethics connection) will make ethics a more salient aspect in AIS research and, like Dorothy realized at the end of her stay in Oz, we will be reminded of something that was there the whole time.[5]

Since AIS research is often interdisciplinary, we expanded the literature search beyond *JIS,* and following Webster and Watson (2002), used online search tools (including Google Scholar and university library search engines) to capture relevant studies. We comprehensively searched the last 14 years of literature from specific journals expected to include a large amount of AIS-related research (e.g., *JIS, MIS Quarterly, Information Systems Research,* and *International Journal of Accounting Information Systems*) and ethics-related research (e.g., *Journal of Business Ethics, Ethics and Information Technology*).

We then developed an understanding (see Figure 3) of what AIS are and do using the elements of AIS described by Romney and Steinbart (2015), set under the ethics umbrella. Using this understanding, we established an overall structure for the review and created subheadings related to the major concepts or themes identified within each element of AIS. We then grouped each article based on the AIS functional area, identified ETHOs factors, and we present them in the online

[5] We acknowledge the above limitation of using the term "ethics" in our search, and include any research identified that investigates ethics and AIS even if the study does not specifically use "ethics" in the text.

FIGURE 3
Relationship of AIS Functions, Ethics, and ETHOs Factors



supplemental material available in Appendix A.[6] This listing includes findings and highlights gaps by factor category. We continued our search process throughout the writing stage, discovering new streams of research, using reference lists and citation cross-referencing tools to find additional sources, per Webster and Watson (2002).

IV. RECORDKEEPING

Recordkeeping, as shown in Figure 3, includes identifying, collecting, storing, and managing data. While recordkeeping has always been at the heart of accounting, computer technology has fundamentally broadened and deepened its reach. Our review finds sparse research explicitly investigating the ethical implications of recordkeeping, although Desai and Embse (2008) identify six key ethical issues regarding electronic information. These issues include what data to collect, how they are collected, processed, and presented, what purpose they are used for, and the extent of their impact on individuals and organizations.

Identify and Collect Data

Organizations identify and collect data as part of recording normal accounting transactions, making decisions about these actions an accounting issue. Firms may also internally generate or purchase external data. Addressing ethical issues related to data acquisition is important because once collected, data are no longer in the control of those who provided them. Thus, it is a gatekeeper decision for all future decisions regarding collected data.

The increased reach and virtually infinite capacity of AIS bring the issue of data identification and collection to the forefront. Integrated systems provide "organizational-wide access and analysis capabilities by standardizing data capture and providing seamless interfaces across functions, responsibility centers, and locations" (Dillard and Yuthas 2006, 203). This integration led to the rise of Big Data[7] and results in firms acquiring more data from more sources than ever before. The accompanying ethical issues primarily focus on personal privacy issues, a *human* factor. Exposure and misuse of personally

[6] Articles appear in the online supplemental material only if they test or propose theories directly related to AIS and ethics. Not all articles are discussed within the text. Other citations appear throughout the text that are not included in the online supplemental material because they are not AIS/ethics papers, or because they refer to current events or reports.

[7] Big Data refers to the 2.5 quintillion bytes of data that are created and stored every day (IBM 2014).

identifiable information (PII) is a real threat. For example, it takes only four credit card transactions to identify 90 percent of individuals, despite using data scrubbed of all personal identifying information (de Montjoye, Radaelli, Singh, and Pentland 2015). Individual identification through Big Data analytics exposes people to identity theft, unwanted targeted marketing, location tracking, and other invasions of personal privacy.

While research in this area is sparse in the AIS literature, one approach put forth by Kauffman, Lee, Prosch, and Steinbart (2011) explores the relationships among stakeholders and each groups' involvement to understand related ethical issues. Their review suggests that stakeholders' concerns can differ based on which ethical issues associated with data collection and identification are the most important. For example, businesses may perceive the sale of personal data as part of daily operations and try to assuage privacy fears by securing the data and creating protocols to govern the transfer of information. Individuals may view the same sale of data as a privacy infringement and be more concerned with whether they consented to their information being used for purposes other than their transaction with that business. Governments may believe that they need to regulate the sale of personal data in order to safeguard the privacy of their constituents. Understanding these relationships seems especially important consider the pace at which technology is advancing.

Mason (1986) argues that using IT (*technological* factors such as facial recognition or GPS locators) to collect personal attributes enables the invasion of privacy of one stakeholder by another. For example, Murphy (2011) discusses how mobile advertising can pinpoint users' locations at any given moment in time. Ethical issues regarding data collection, such as tracking, abound when dealing with devices that are "always on." Stone and Stone-Romero (1998) argue that information collection poses moral dilemmas for organizations: How do they protect the interests of consumers and employees while collecting enough information to facilitate decision making? Additionally, consumers are often unable to acquire goods or services without providing personal information the firm considers necessary (Shapiro and Baker 2002). Relevant *organizational* factors include industry and products offered. Levin and Nicholson (2005) contend that privacy laws, an *environmental* factor, should reflect concerns about private sector abuse of personal information and enable individuals to set limits upon both public and private use of their information. Different stakeholders likely have diverse concerns over the appropriateness of what data are collected and for what purposes.

Generally Accepted Privacy Principles[8] (GAPP, AICPA/CICA 2009) list many negative outcomes to organizations from misjudging individuals' (and regulators') perceptions and expectations about data identified and collected. Many of these, such as reputational damage, legal liability, and loss of customer trust and business, come from the perceived harm resulting from these misjudgments. A possible mitigating factor is whether the firm transparently communicated a valid reason for collecting the data.

Based on a review of the literature, there is relatively little research investigating the identification and collection aspect of AIS. Much of the literature is theoretical in nature and focuses on privacy issues surrounding data capture. This literature provides directions for future research investigating how ETHOs factors influence data collection. For example, Kauffman et al. (2011) discuss privacy rights, policies, and procedures. Researchers may investigate how *environmental* factors such as regulation and industry standards, and *technological* factors, such as automated collection, miniaturization of data collection tools, and connectedness (e.g., the Internet of Things) enable or limit unethical collection practices. Further, research may examine whether *human* factors influence user acceptance, consent, and/or attitudes toward different types of notices contained within privacy policies.

Data Management: Storage and Security, Quality, and Use

Data management includes storage and security, quality maintenance (including data accuracy and reliability), and proper use. Integrated applications such as ERP and ERP II allow organizations to store and use data from various, disparate business units. Furthermore, organizations, through their AIS, build and maintain extensive centralized databases housing huge quantities of data, including PII. Because PII has been used to identify, discriminate, persecute, punish, and silence people in the past (Parson 1966; Lwin, Wirtz, and Williams 2007; Bansal, Zahedi, and Gefen 2010), the right to privacy appears to be a basic human right, and thus control over PII is an ethical issue. The determination of PII ownership is an area ripe for analysis, as it poses serious ethical concerns.

Organizations are morally and legally responsible for managing the data they collect. GAPP (AICPA/CICA 2009) recommends entities only use data for the purposes identified in the notice and for which individuals have provided explicit or implicit consent. COBIT asserts that privacy issues are a growing concern and that organizations need to manage them if people are to trust IT systems. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides guidance on maintaining the privacy and security of personally identifiable health information (U.S. Department of Health and Human

[8] This framework was created in 2009 by the AICPA (American Institute of Public Accountants) and CICA (Canadian Institute of Chartered Accountants) in response to privacy concerns associated with PII (personally identifiable information).

Services [HHS] 2003). HIPAA ensures patients' rights to examine and obtain a copy of their health records and to request corrections. Organizations also collect personal information from employees through the human resources function. Federal and state privacy laws, as well as organizations' own policies, govern the storage, security, quality, and use of employee information.

Data Management (Storage and Security)

Because individuals and organizations can use data for unethical purposes (e.g., identity theft, unfair competitive advantage, unwanted targeted advertising), their security is paramount. Yet within the AIS domain, there is little published research in this area. In an interview with 103 IT managers, Dhillon and Torkzadeh (2006) identify specific *organizational* factors (e.g., employer trust, and authority structure) and *human* factors (e.g., individual lifestyle, personal financial situation) affecting data security effectiveness. Biot-Paquerot and Hasnaoui (2009) emphasize *organizational* factors, noting that strong corporate governance with clear codes of ethics ensures clarification of fundamental values and reinforces self-regulation within organizations.

Sykes and Matza (1957) argue that people psychologically enable themselves to commit rule-breaking or any antisocial actions by applying the techniques of neutralization.[9] Siponen and Vance (2010) find that neutralization is a major predictor of employees' intention to violate IS security policies. Similarly, Harrington (1996) shows that individuals with a denial-of-responsibility attitude are less likely to judge computer abuse as wrong and are more strongly influenced by ethical codes. These findings suggest that the *human* factor, rationalization, holds in IT cases as well as in other occupational fraud.

While protecting data from unauthorized access is necessary, certain security measures, such as authentication,[10] pose ethical dilemmas of their own. Sutrop and Laas-Mikko (2012) compare the ethical issues raised by first- and second-generation biometrics, both authentication systems. Ethical issues related to first-generation biometrics are privacy, autonomy, bodily integrity, dignity, equity, and personal liberty. The difference between first- and second-generation biometrics lies in the individuals' awareness that a third party is collecting data from them. Second-generation biometrics, therefore, raises new ethical issues because it devalues the principle of informed consent, which may lead to less respect for individual moral autonomy and to the loss of public trust.

Data Management (Quality)

Companies collect, store, and analyze information from multiple sources using less structured and informal data processing systems (O'Leary 2013). However, these approaches may pose major security and privacy breaches if the data involved are sensitive for reasons of privacy, enterprise security, or regulatory requirements (Villars, Olofson, and Eastwood 2011). Additionally, since Big Data allows for information inputs from multiple sources, there is a higher likelihood of collecting data with potential errors, incompleteness, or differential precision (O'Leary 2013). Nunan and Domenico (2013) point to the memory power of Big Data, passive data collection, and ownership of the data as major ethical issues associated with Big Data.

Database quality begins with a high-quality implementation. Many organizations implement information systems (IS) when there are clear signs that quality problems exist and that the system will not perform up to its expectations (Tuttle et al. 1997). Using IS professionals as participants, Tuttle et al. (1997) document that incentives to shirk and privately held information motivate IS professionals to place their own interests over their organizations' interests.

Data Management (Use)

Increasing use of electronic databases poses a major threat to data privacy, as the data within them are searchable, downloadable (possibly undetected), and at risk for illegitimate and unethical uses. In order to reduce the risks associated with misuse, organizations must address privacy issues throughout the database design process and teach designers to treat privacy as an integral database issue (Appel 2006). Culnan and Williams (2009) note that stakeholders are vulnerable in their dealings with businesses due to their inability to control subsequent use of their personal information. The authors suggest that organizations create a culture of privacy through tone at the top. *Organizational* factors, such as ethical climate and strategy, and *environmental* factors, such as industry standards, are likely influential here and motivate further study.

Morris, Kleist, Dull, and Tanner (2014) note that interorganizational information sharing may help organizations (e.g., solve complex problems, reduce uncertainty, and improve decision making). To address privacy and security concerns in information sharing, Morris et al. (2014) propose a Secure Information Market (SIM) model where organizations contribute

[9] In accounting, this falls into the same category of rationalization.

[10] Authentication is the process of confirming that an individual accessing the system is, in fact, who he says he is.

data to the electronic market and the market makes the information available to organizations or to preapproved information buyers. Industry and availability of certain technologies likely influence SIM adoption and may be fruitful areas of investigation.

As companies are increasingly networked via outsourcing and other joint venture agreements, data sharing becomes more common and ethical concerns more prevalent. Major public and private organizations such as General Electric, Ford, American Express, Citibank, British Petroleum, and Hewlett-Packard have outsourced parts of their accounting function to third-party providers (Elharidy, Nicholson, and Scapens 2013). Although AIS outsourcing is common, very limited research exists on its related ethical issues. Elharidy et al. (2013) find that legal and professional bodies enforce the ethical duties of outsourcing suppliers, whereas religion and traditional customs and values influence the importance of integrity and ethical dealings. In a related study, Cullinan and Zheng (2015) find that mutual funds consider potential cost savings as an important factor in their AIS outsourcing decisions. The authors also document that funds using more complex valuation processes and older fund families are less likely to outsource their AIS functions.

Based on the review of articles related to data management and ethics, *technological* and *environmental* factors appear infrequently. Prior literature does not examine how *technological* factors (e.g., technological complexity, integrated information system, and emergence of Big Data) and *environmental* factors (e.g., industry standards, regulations, and competitive pressure) affect the ethical generation and use of information. Also missing in this literature are the interactive effects of ETHOs factors. Further research to investigate how *human* factors such as fear-based persuasive communication and cross-cultural differences interact with *technological* factors (Crossler et al. 2013) to enable security breaches is appropriate.

Researchers may also investigate whether models such as SIM, proposed by Morris et al. (2014), effectively address privacy and ethical concerns. Although organizations continue to implement information systems with known quality problems, little is known about the ethics-related factors that affect these choices. Future research may focus on whether *organizational* factors, such as ethical climate, time pressure, risk preference, or system complexity, influence the implementation of faulty systems.

V. REPORTING

As Figure 3 indicates, reporting involves communicating information to stakeholders. The chief outputs of AIS are financial and nonfinancial reports, which assist internal and external users in evaluating performance and in making decisions. Reporting represents a critical and everyday intersection of AIS and human judgment as both the form and presence of reports potentially bias user judgment. This intersection has moral implications and exposes two types of biases: those that arise by design or those that occur accidentally, *ex machina*.

Commonly cited characteristics of information related to its usefulness include accessibility, relevance, understandability, timeliness, reliability, completeness, and verifiability (Romney and Steinbart 2015). These characteristics provide a framework for discussing AIS reporting and ethics.

Access (Accessibility)

Access concerns the availability, transparency, and disclosure of information from AIS to users (Turilli and Floridi 2009). Ethical issues include considerations of how and when organizations make AIS output available to users. Although information asymmetry is often seen as a negative, Turilli and Floridi (2009) include a valuable discussion of organizations' duties to secure certain confidential information from disclosure.

In addition to shareholders of listed entities, there is a host of potential internal and external users of accounting information (Young 2006). One method for examining access issues is to consider the distinct information needs of different stakeholders (Dillard and Yuthas 2002). ETHOs factors likely influence decisions about when and to whom information from AIS is available. Both individuals and organizations make access decisions. This is an ethical judgment, because these disclosures (or lack of them) can unfairly advantage (or harm) certain stakeholders. Technology can deliver better information to all stakeholders, yet evidence suggests that technology may also exacerbate information asymmetry. Although the SEC (2014) established Regulation FD[11] to level the playing field for all investors by regulating corporate disclosures, Patterson (2014) finds that high-frequency traders purchase market reports ahead of public release in order to gain a competitive advantage in stock trading. While in this case a third party acts as a conduit for information, this situation draws attention to the

[11] Regulation FD provides that when an issuer discloses material nonpublic information to certain individuals or entities—generally, securities market professionals such as stock analysts or holders of the issuer's securities, who may well trade on the basis of the information—the issuer must make public disclosure of that information (SEC 2014).

role that information intermediaries play as an interface with the organization's AIS and how their involvement has ethical implications.

Human and *organizational* factors may inhibit sharing of financial information with external stakeholders, despite the promise of transparency enabled by advances in technology. Accessibility to information involves an interaction of human judgment and technology, and thus is subject to *human* and *technological* factors. In field research, Gowthorpe (2004) reports that senior corporate offices intend to use internet reporting to address extant information inequalities, but haphazard implementation can result in a failure to identify stakeholder needs adequately, leading to unintended negative consequences. In experimental research, Hassink, Bollen, and Steggink (2007) find many firms are reluctant to respond to investor-initiated requests for financial information over the internet, even though there are positive consequences from greater access (e.g., lower cost of capital, greater liquidity, and a larger analyst following Kirk and Vincent [2014]). Therefore, management may view communication through new technology as inherently different from traditional forms of communication, which may be due to concerns over misuse or to how technology removes the actors from the actions taken (Dillard 2003). Researchers have not yet exhaustively examined the uses of AIS in stakeholder relations.

Future research should focus on how new technologies influence access to reports and whether they mitigate or exacerbate information asymmetry and/or information processing. As evident from the article list in the online supplemental material (see Appendix A), there are few studies, if any, considering the ethical implications tied to *technological* factors. While an increasing amount of research investigates human factors in financial reporting, there are significant research gaps around possible interactions between human factors and new technology such as XBRL, social media, and real-time analysis. For instance, do the frequent updates of the XBRL taxonomy enable managers to obfuscate financial disclosures? How might managers seek to use social media to exploit *human* factors and exacerbate information asymmetry in spite of a general assumption that the internet improves access? Snow's (2015) analysis of retail investors' perceptions of financial disclosures on Twitter versus the World Wide Web is just one example.

With regard to *environmental* factors, whether and how accounting and financial regulation can keep up with innovation in the integration of reporting with new technology, such as social media, is an area ripe for investigation. Researchers may also explore *environmental* factors (e.g., regulation) across different countries and investigate whether there are significant interactions with *human* factors such as culture.

Judgment Bias (Timeliness, Understandability, and Relevance)

AIS provide input for individual judgment and decision making (JDM) (O'Donnell and David 2000). Technology can greatly enhance the timeliness, understandability, and relevance of reports; however, it also enables organizations to exploit individual judgment biases, an ethical concern. Heuristics and biases influence moral judgment just as they influence other forms of accounting judgments (Jones, Massey, and Thorne 2003; Bailey, Scott, and Thoma 2010; Neri 2015). AIS research into general judgment biases suggests two areas that merit further investigation in relation to moral judgment: the effect that the existence of AIS have on JDM and the effect that the presentation format of reports has on JDM.

Effects of the Presence of AIS

Researchers find that the mere existence of an information system can affect moral judgments, such as manager intentions to be honest (Hannan et al. 2006). The existence of computer-mediated reporting technology may increase manager perceptions of scrutiny, which results in more honest reporting. On an individual level, AIS can help improve JDM; however, AIS might also create dysfunctional behavior, such as over-reliance on systems, reduced accountability, and acceptance of authority, even malicious obedience (Dillard and Yuthas 2002). These behaviors reduce users' perceived need for and exercise of professional judgment. Some researchers express concern that the advent of risk management and related systems actually supplants managerial moral judgment (Power 2009); moral questions may become subject to a question of "risk appetite" rather than to adherence to a universal human value.

Researchers raise concerns that an auditor's inadequate understanding of system limitations when using expert auditing systems may result in reduced audit quality (Sutton, V. Arnold, and T. Arnold 1995; Sutton and Byington 1993). Longer exposure to decision aids may actually result in deskilling, which could affect an auditor's professional judgment resulting in diminished fraud detection and reduced audit quality.

Effects of Presentation Format

Organizations can present financial information in verbal, numerical, or graphical formats. Vohs, Mead, and Goode (2008) suggest presenting information in a "money" context changes behavior. Kelton, Pennington, and Tuttle (2010) and O'Donnell and David (2000) review experimental research that demonstrates that presentation style affects individual JDM. Dilla and

Stone (1997) find that presentation of financial information in numerical rather than verbal form affects auditors' inherent risk judgments. In a field study, Dull, Graham, and Baldwin (2003) find that investors' JDM differs depending on whether organizations present financial disclosures in interactive, drill-down menus or in conventional, static web pages.

Our review suggests this area of research is already quite mature; however, future research can combine existing ETHOs factors in new ways to identify important interactions. There are also many judgment biases that have not yet been considered with regard to ethical judgment. O'Donnell and David (2000) provide a framework to help researchers identify the ways in which AIS bias JDM in general. Ethics researchers could then layer the ETHOs framework to identify ways in which AIS might bias moral judgment specifically. *Environmental* factors include the decision-making environment, *technological* factors include features of the AIS, and *human* factors include the individual's problem-solving skills or their processing strategy. To date, researchers have studied only three factors in depth: presentation format, decision support system use, and the level of information load involved in particular judgments (O'Donnell and David 2000).

Financial Reporting Quality (Reliability, Completeness, and Verifiability)

Preventing and Detecting Fraudulent Financial Reporting and Errors

At the organizational level, *control* over financial reporting is a clear purpose of legislation (e.g., SOX) and profession-sponsored frameworks (e.g., COSO) (Drennan 2004). However, legislation alone does not prevent major fraudulent practices (H. Rockness and J. Rockness 2005). Rather, strong ethical corporate culture, internal controls, laws, rewards, and penalties must work together to provide ethical and transparent financial reporting. Thus, *environmental* factors, in conjunction with technology, organization, and *human* factors, influence control effectiveness.

The automation inherent in modern AIS enables management to adopt continuous monitoring and auditing to reduce fraudulent financial reporting. Organizations can use continuous monitoring to help make specific components of AIS, such as the purchasing system, compliant with SOX regulations (S. Chang, Wu, and I. Chang 2008). Continuous auditing also has the potential to yield better testing and online communication and less expensive and timelier audits (Kogan, Sudit, and Vasarhelyi 1999). However, the introduction of these tools raises ethical concerns, including auditor over-reliance and negative effects on auditor knowledge and skills development (J. Daigle, R. Daigle, and Lampe 2008; Dillard and Yuthas 2001).

XBRL, a technology-based standard, promises more reliable, standardized financial reporting, yet also introduces ethical concerns. While XBRL is a computer-readable format, the SEC requires auditors to provide assurance on a manual version of the financial reports generated from it.[12] However, Boritz and No (2009) and Bartley, Chen, and Taylor (2011) point out serious shortcomings in XBRL's early regulation and implementation. XBRL's complexity, along with the individuals' inexperience auditing and interpreting XBRL filings, provides managers an opportunity to misrepresent these disclosures with a lower chance of detection. On the other hand, investors may be able to use XBRL disclosure analysis tools to locate specific information more easily, improving detection of accounting irregularities by making it more difficult to "hide information in plain sight" (Cohen, Schiavina, and Servais 2005). Whether XBRL enables more or less misstatement is a question for future research.

AIS technology enables management to conduct sensitivity analyses to gauge the effect of transactions on quarterly and annual earnings quickly and easily, increasing the opportunity for earnings management. Malenko and Grundfest (2014) provide evidence of firms managing EPS numbers reported by U.S.-listed corporations.[13] While there is evidence that accruals-based earnings management (EM) is on the decline post-SOX, it remains prevalent (Dichev, Graham, Harvey, and Rajgopal 2013), and real activities EM[14] may be on the rise (Cohen, Dey, and Lys 2008). Arguably, advances in AIS facilitate EM. Using computer programs and digital data, managers can run virtually unlimited simulations to identify the accounting strategy with the best (or most desired) financial statement outcome making EM faster and easier than ever before.

Much of the existing research into new reporting technologies considers their impact on capital markets. Future research should examine how *technological* factors, such as advances in audit software, continuous monitoring, and XBRL interact with human factors, such as age, experience and functional area, or with *organizational* factors such as ethical climate (Martin and Cullen 2006) or industry to enable or discourage fraud or deception. *Environmental* factors, such as new regulation, seem particularly relevant since present research has primarily considered regulation of conventional, paper-based media.

[12] The SEC and PCAOB developed XBRL guidelines (R. Plumlee and M. Plumlee 2008) to address adoption and assurance issues.

[13] Quadrophobia, "a fear of four," is the phenomenon that the number four occurs statistically less frequently than other numerals in the first post-decimal digit of EPS data. The claim is that this occurs because firms manage reported EPS so that it is rounded up more often than it is rounded down. For instance, Dell is cited as rounding up EPS for 48 straight quarters, which is statistically improbable.

[14] Real activities earnings management involves manipulating the operations of the business, such as inventory levels or sales, through "channel stuffing" (Roychowdhury 2006).

VI. CONTROL

AIS encompass controls over the activities of both people and systems to enhance organizational efficiency and effectiveness and safeguard assets (see Figure 3). Ethical issues arise when people, like other business assets, are monitored and controlled (Romney and Steinbart 2015).

Control implies managers, including accountants, have moral obligations when allocating resources and prioritizing stakeholder claims.[15] Yet, controls designed to manage organizational efficiency and effectiveness can have a detrimental effect on moral judgment at the human level (Abernethy and Brownell 1997). Research outside AIS finds that formal control systems[16] may be positively associated with employee moral awareness and behavior (Rottig, Koufteros, and Umphress 2011), but that over-reliance on rules-based systems may also be detrimental (Stansbury and Barry 2007), as when individuals blindly follow rules despite changes in context. These discoveries are highly relevant to AIS research related to internal control, management accounting, and audit.

A major aspect of organizational control is the control over employees through electronic monitoring. Electronic monitoring of employees in the workplace has deep ethical implications with respect to workplace outcomes such as employee perceptions of privacy and fairness, quality of work life, and stress-related illness (Tabak and Smith 2005). Using the concepts of formalism and utilitarianism, Alder, Schminke, Noel, and Kuenzi (2008) argue that an employee's prior beliefs and ethical orientation, both *human* factors, affect his or her reaction toward electronic monitoring. Similarly, continuous monitoring introduces the ethical question of whether greater surveillance of workers and their work is at all times and in all places acceptable and desirable. Monitoring may have unintended consequences through its effects on individual judgment and behavior.

In addition to control over people and their activities, AIS include controls over assets. While information technology may positively affect organizational development and growth, its widespread use also increases opportunities for occupational fraud (Kesar 2006), which costs about 5 percent of an organization's total revenue (Association of Certified Fraud Examiners [ACFE] 2014). Although employee dishonesty and fraud are clearly not new issues, use of integrated information technology creates fruitful ground for new forms of employee dishonesty (Todd 2004). Further, considering Ariely's (2008) finding that cheating is easier when the actor is a step removed from the cash, technology may have the unintended consequence of increasing unethical behavior by creating illusory distance between individuals and the cash they misappropriate.

Lynch and Gomaa (2003) suggest that information technology enables fraud. Based on Ajzen's (1991) theory of planned behavior, they posit a framework for considering the likelihood of fraud in an environment that includes integrated information systems, a *technological* factor. In a survey of IT managers, S. Behling, Floyd, Smith, Koohang, and R. Behling (2009) find that even when employee fraud detection controls are in place, they are not fully effective due to *organizational* factors such as limited staff, shrinking budgets, and time constraints. Wells (2007) posits that technology controls are not always enough to prevent employee fraud because they are designed to provide reasonable, but not absolute, assurance. Furthermore, employees with sufficient motivation can override most controls since employees are usually more aware than are outsiders of flaws in the system (Wells 2007; Kesar 2006). *Human* factors such as the ability to rationalize and financial pressures are relevant here.

Based on our review of articles related to the control function of AIS, *technological* and *environmental* factors are under researched. Prior literature does not examine how *environmental* factors (e.g., local laws and industry standards) affect the acceptance of employee monitoring and employee satisfaction. Although limited research indicates that AIS technology facilitates fraud, more research is needed to validate this argument. Understanding whether and how technological complexity and certain AIS features facilitate (or mitigate) occupational fraud is a fruitful path to explore. Also important is to investigate whether and how *organizational* and *technological* factors (e.g., decision aids, AIS features, tracking tools, remote access, formal ethical infrastructure, and continuous monitoring practices) negatively influence critical thinking, induce employees toward checklist mentality in ethical decisions, and contribute to increased occupational fraud.

VIII. CONCLUSION

This review outlines major areas of interest related to AIS and ethics based on the primary AIS functions of recordkeeping, reporting, and control. We define ethics as issues that infringe upon universal human rights and expand the definition to include

[15] Otley (1999, 365–366) suggests that management control includes identifying organizational goals leading to an organization's overall future success: adopting strategies, processes, and activities that enable an organization to achieve its goals; defining levels of performance in each strategy area that allow an organization to set performance targets to assess the achievement of its goals; defining the rewards (penalties) that managers will receive for achieving (failing to achieve) organizational performance targets; and creating information flows (feedback and feed-forward loops) that allow the organization to learn from its experience and adapt its current behavior to reflect what it has learned.

[16] Consistent with Weaver, Trevino, and Cochran's (1999) conception of formal ethics programs, Rottig et al. (2011, 163) defines a multifaceted formal ethical infrastructure as one "consisting of formal communication, recurrent communication, formal surveillance, and formal sanctions."

issues related to the public's expectations of accounting and other business professionals. AIS affect peoples' lives; these effects are magnified by systems' ubiquitous integration into all areas of organizations and by their expanding technological capabilities (i.e., ability to collect, store, disseminate, and process data faster and further, with minimal cost). It is imperative that individuals and groups acknowledge the harm and risk of harm that inevitably come with AIS. This review suggests that overreliance on AIS potentially provides individuals a convenient source of rationalization for unethical behavior.

We discuss the current state of research in each of the AIS functional areas, summarizing findings and linking them to ETHOs factor categories, and suggest future research within each category. Within recordkeeping are privacy issues associated with data collected, stored, and used by organizations. The discussion expands beyond consideration of customer data to include other stakeholders' data such as that belonging to employees, vendors, and other third parties. A central concern is the determination of who owns data and how organizations may use these data to harm others.

The next area is reporting, a key function of AIS. As AIS are the primary source of financial disclosures, it is important to understand their technological capabilities and how these may lead to unethical acts. One example is the ease with which managers can use scenario analysis to manage earnings faster and more precisely than ever before. Another example is the ability to alter presentation format to influence moral judgments (e.g., minimizing effects of employees' layoffs by scaling graphs to overstate benefits or to obscure costs to individuals).

Control issues, namely how managers use AIS as a tool to control people and assets, are the final area explored. Employee monitoring, decision automation, and dehumanization of processes all affect human rights. Monitoring, both with and without consent, evokes fears of "Big Brother" and may impede productivity and innovation. Systems enable individuals to distance themselves both physically and psychologically from their actions, facilitating occupational fraud by enabling rationalizations. Control issues are inextricably linked with AIS and ethics.

In the process of preparing this review, we were encouraged by the attention a small contingent of AIS researchers has paid to ethics. However, there are significant gaps in the literature. While much AIS research has ethical implications, researchers rarely explicitly tie their research questions and motivations underlying ethical goals. Preventing harm to others is a noble endeavor, and we recommend researchers acknowledge this as a purpose of their research when appropriate.

Accounting is a moral discipline; people designed, developed, and control it for the benefit of themselves and others. There are no scientific laws of accounting, thus we are ultimately responsible for its development and for its effects on society. Universal ethics demand that professionals and academics alike take on the responsibility of understanding how AIS not only help, but also potentially harm others. It is a challenge we are fully capable of meeting.

REFERENCES

Abernethy, M. A., and P. Brownell. 1997. Management control systems in research and development organizations: The role of accounting, behavior and personnel controls. *Accounting, Organizations and Society* 22 (3): 233–248.

Adams, G. B., and D. L. Balfour. 1998. *Unmasking Administrative Evil*. Thousand Oaks, CA: Sage Publications.

Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 50 (2): 179–211.

Alder, G. S., M. Schminke, T. W. Noel, and M. Kuenzi. 2008. Employee reactions to internet monitoring: The moderating role of ethical orientation. *Journal of Business Ethics* 80 (3): 481–498.

American Institute of Certified Public Accounts (AICPA). 2013a. *Code of Professional Conduct and Bylaws*. Available at: http://www.aicpa.org/research/standards/codeofconduct/downloadabledocuments/2013june1codeofprofessionalconduct.pdf

American Institute of Certified Public Accountants (AICPA). 2013b. *2013 North American Top Technology Initiatives Survey*. Available at: http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/TopTechnologyInitiatives/DownloadableDocuments/north-america-tti-survey.PDF

American Institute of Certified Public Accountants (AICPA). 2014. *Code of Professional Conduct*. Available at: http://pub.aicpa.org/codeofconduct/Ethics.aspx

American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA). 2009. *Generally Accepted Privacy Principles: CPA and CA Practitioner Version*. New York, NY: AICPA/CICA.

Appel, F. 2006. The study of database design must address privacy concerns. *Journal of Information, Communication and Ethics in Society* 4 (3): 155–161.

Ariely, D. 2008. How honest people cheat. *Harvard Business Review* 86 (2): 24–24.

Association of Certified Fraud Examiners (ACFE). 2014. *Report to the Nation: Occupational Fraud and Abuse*. Austin, TX: Association of Certified Fraud Examiners.

Bailey, C. D., I. Scott, and S. J. Thoma. 2010. Revitalizing accounting ethics research in the neo-Kohlbergian framework: Putting the DIT into perspective. *Behavioral Research in Accounting* 22 (2): 1–26.

Bansal, G., F. Zahedi, and D. Gefen. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems* 49 (2): 138–150.

Bartley, J., A. Y. S. Chen, and E. Z. Taylor. 2011. A comparison of XBRL filings to corporate 10-Ks: Evidence from the voluntary filing program. *Accounting Horizons* 25 (2): 227–245.

Beard, D., and H. J. Wen. 2007. Reducing the threat level for accounting information systems. *The CPA Journal* 77 (5): 34.

Behling, S., K. Floyd, T. Smith, A. Koohang, and R. Behling. 2009. Managers' perspectives on employee information technology fraud issues within companies/organizations. *Issues in Information Systems* 10 (2): 76–81.

Biot-Paquerot, G., and A. Hasnaoui. 2009. Stakeholders perspective and ethics in financial information systems. *Journal of Electronic Commerce in Organizations* 7 (1): 59–70.

Black, E., and B. Wallace. 2001. *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. New York, NY: Crown Publishers.

Bond, B., Y. Genovese, D. Miklovic, N. Wood, B. Zrimsek, and N. Rayner. 2000. *ERP Is Dead—Long Live ERP II*. New York, NY: Gartner Group.

Boritz, J. E., and W. G. No. 2009. Assurance on XBRL-related documents: The case of United Technologies Corporation. *Journal of Information Systems* 23 (2): 49–78.

Boritz, J. E., and W. G. No. 2011. E-commerce and privacy: Exploring what we know and opportunities for future discovery. *Journal of Information Systems* 25 (2): 11–45.

Brancheau, J. C., and J. C. Wetherbe. 1987. Key issues in information systems management. *MIS Quarterly* 11 (1): 23–45.

Brancheau, J. C., B. D. Janz, and J. C. Wetherbe. 1996. Key issues in information systems management: 1994–1995 SIM Delphi results. *MIS Quarterly* 20 (2): 225–242.

Bronstein, S., D. Griffin, and N. Black. 2014. *VA Deaths Covered Up to Make Statistics Look Better, Whistle-Blower Says*. Available at: http://www.cnn.com/2014/06/23/us/phoenix-va-deaths-new-allegations/

Chang, S. I., C. C. Wu, and I. C. Chang. 2008. The development of a computer auditing system sufficient for Sarbanes-Oxley Section 404—A study on the purchasing and expenditure cycle of the ERP system. *Information Systems Management* 25 (3): 211–229.

Chee, F. Y. 2014. *European Court Says Google Must Respect "Right to Be Forgotten."* Available at: http://www.reuters.com/article/2014/05/13/us-eu-google-dataprotection-idUSBREA4C07120140513

Clarke, R. 1999. Internet privacy concerns confirm the case for intervention. *Communications of the ACM* 42 (2): 60–67.

Cohen, E. E., T. Schiavina, and O. Servais. 2005. XBRL: The standardized business language for 21st century reporting and governance. *International Journal of Disclosure and Governance* 2 (4): 368–394.

Cohen, D. A., A. Dey, and T. Z. Lys. 2008. Real and accrual-based earnings management in the pre- and post-Sarbanes-Oxley periods. *The Accounting Review* 83 (3): 757–787.

Cohen, J., G. B. Manzon, Jr., and V. L. Zamora. 2015. Contextual and individual dimensions of taxpayer decision making. *Journal of Business Ethics* 126 (4): 631–647.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2013. *Internal Control—Integrated Framework*. New York, NY: AICPA.

Cooper, C. 2009. *Extraordinary Circumstances: The Journey of a Corporate Whistleblower*. New York, NY: John Wiley & Sons.

Copeland, J. 2005. Ethics as an imperative. *Accounting Horizons* 19 (1): 35–43.

Crossler, R. E., A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. 2013. Future directions for behavioral information security research. *Computers and Security* 32: 90–101.

Cullinan, C. P., and X. Zheng. 2015. Outsourcing accounting information systems: Evidence from closed-ended mutual fund families. *International Journal of Accounting Information Systems* 17: 65–83.

Culnan, M. J., and C. C. Williams. 2009. How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *Management Information Systems Quarterly* 33 (4): 6.

Daigle, J. J., R. J. Daigle, and J. C. Lampe. 2008. Auditor ethics for continuous auditing and continuous monitoring. *Information Systems Control Journal* 3: 1–4.

de Montjoye, Y. A., L. Radaelli, V. K. Singh, and A. S. Pentland. 2015. Unique in the shopping mall: On the re-identifiability of credit card metadata. *Science* 347 (6221): 453–580.

Deloitte. 2014. *The 2013 COSO Framework and the Audit Committee*. Available at: http://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-acbrief-march-2014.pdf

Desai, M. S., and T. J. Embse. 2008. Managing electronic information: An ethics perspective. *Information Management and Computer Security* 16 (1): 20–27.

Dhillon, G., and G. Torkzadeh. 2006. Value-focused assessment of information system security in organizations. *Information Systems Journal* 16 (3): 293–314.

Dichev, I., J. Graham, C. R. Harvey, and S. Rajgopal. 2013. Earnings quality: Evidence from the field. *Journal of Accounting & Economics* 56 (2–3): 1–33.

Dilla, W. N., and D. N. Stone. 1997. Representations as decision aids: The asymmetric effects of words and numbers on auditors' inherent risk judgments. *Decision Sciences* 28 (3): 709–743.

Dillard, J. F. 2003. Professional services, IBM, and the Holocaust. *Journal of Information Systems* 17 (2): 1–16.

Dillard, J. F., and K. Yuthas. 2001. A responsibility ethics for audit expert systems. *Journal of Business Ethics* 30 (4): 337–359.

Dillard, J. F., and K. Yuthas. 2002. Ethics research in AIS. In *Researching Accounting as an Information Systems Discipline,* edited by Arnold, V., and S. Sutton, 181–206. Sarasota, FL: American Accounting Association.

Dillard, J. F., and K. Yuthas. 2006. Enterprise resource planning systems and communicative action. *Critical Perspectives on Accounting* 17 (2): 202–223.

Drennan, L. T. 2004. Ethics, governance and risk management: Lessons from Mirror Group newspapers and Barings Bank. *Journal of Business Ethics* 52 (3): 257–266.

Dull, R. B., A. W. Graham, and A. A. Baldwin. 2003. Web-based financial statements: Hypertext links to footnotes and their effect on decisions. *International Journal of Accounting Information Systems* 4 (3): 185–203.

Elharidy, A. M., B. Nicholson, and R. Scapens. 2013. The embeddedness of accounting outsourcing relationships. *Qualitative Research in Accounting and Management* 10 (1): 60–77.

Gentile, M. C. 2012. *Giving Voice to Values: How to Speak Your Mind When You Know What's Right*. New Haven, CT: Yale University Press.

Glass, R. S., and W. A. Wood. 1996. Situational determinants of software piracy: An equity theory perspective. *Journal of Business Ethics* 15 (11): 1189–1198.

Gowthorpe, C. 2004. Asymmetrical dialogue? Corporate financial reporting via the internet. *Corporate Communications: An International Journal* 9 (4): 283–293.

Hannan, R. L., F. W. Rankin, and K. L. Towry. 2006. The effect of information systems on honesty in managerial reporting: A behavioral perspective. *Contemporary Accounting Research* 23 (4): 885–918.

Harrington, S. J. 1996. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly* 20 (3): 257–278.

Hassink, H., L. Bollen, and M. Steggink. 2007. Symmetrical versus asymmetrical company-investor communications via the internet. *Corporate Communications: An International Journal* 12 (2): 145–160.

Hunt, N., and G. Iyer. 2015. *The Effect of Tax Domain, Income Class, and Personal Norms: An Analysis of Taxpayer Compliance Decisions Using Paper and Software*. Working paper, University of North Texas.

International Business Machines (IBM). 2014. *What Is Big Data? Big Data at the Speed of Business*. Available at: http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

Jones, J., D. W. Massey, and L. Thorne. 2003. Auditors' ethical reasoning: Insights from past research and implications for the future. *Journal of Accounting Literature* 22: 45–103.

Kauffman, R. J., Y. J. Lee, M. Prosch, and P. J. Steinbart. 2011. A survey of consumer information privacy from the accounting information systems perspective. *Journal of Information Systems* 25 (2): 47–79.

Kelton, A. S., R. R. Pennington, and B. M. Tuttle. 2010. The effects of information presentation format on judgment and decision making: A review of the information systems research. *Journal of Information Systems* 24 (2): 79–105.

Kesar, S. 2006. Legal issues alone are not enough to manage computer fraud committed by employees. *Journal of International Commercial Law and Technology* 1 (1): 25–40.

Kidder, R. M. 2005. *Moral Courage*. New York, NY: HarperCollins.

Kirk, M. P., and J. Vincent. 2014. Professional investor relations within the firm. *The Accounting Review* 89 (4): 1421–1452.

Kogan, A., E. F. Sudit, and M. A. Vasarhelyi. 1999. Continuous online auditing: A program of research. *Journal of Information Systems* 13 (2): 87–103.

Levin, A., and M. J. Nicholson. 2005. Privacy law in the United States, the EU and Canada: The allure of the middle ground. *University of Ottawa Law and Technology Journal* 2: 357.

Lynch, A., and M. Gomaa. 2003. Understanding the potential impact of information technology on the susceptibility of organizations to fraudulent employee behavior. *International Journal of Accounting Information Systems* 4 (4): 295–308.

Lwin, M., J. Wirtz, and J. D. Williams. 2007. Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science* 35 (4): 572–585.

Malenko, N., and J. Grundfest. 2014. *Quadrophobia: Strategic Rounding of EPS Data*. Available at: http://ssrn.com/abstract=1474668

Mason, R. O. 1986. Four ethical issues of the information age. *MIS Quarterly* 10 (1): 5–12.

Martin, K. D., and J. B. Cullen. 2006. Continuities and extensions of ethical climate theory: A meta-analytic review. *Journal of Business Ethics* 69 (2): 175–194.

Mauldin, E. G., and L. V. Ruchala. 1999. Towards a meta-theory of accounting information systems. *Accounting, Organizations and Society* 24 (4): 317–331.

Møller, C. 2005. ERP II: A conceptual framework for next-generation enterprise systems? *Journal of Enterprise Information Management* 18 (4): 483–497.

Morris, B. W., V. F. Kleist, R. B. Dull, and C. D. Tanner. 2014. Secure information market: A model to support information sharing, data fusion, privacy, and decisions. *Journal of Information Systems* 28 (1): 269–285.

Murphy, D. 2011. *The Geo-Targeting Revolution*. Available at: http://mobilemarketingmagazine.com/geo-targeting-revolution/

Neely, M. P., and J. S. Cook. 2011. Fifteen years of data and information quality literature: Developing a research agenda for accounting. *Journal of Information Systems* 25 (1): 79–108.

Neri, M. P. 2015. Moral intuition: A review for accounting research. *Proceedings of the 20th Annual Ethics Research Symposium of the American Accounting Association,* Chicago, IL, August 9.

Nunan, D., and M. D. Domenico. 2013. Market research and the ethics of Big Data. *International Journal of Market Research* 55 (4): 41–56.

O'Donnell, E., and J. S. David. 2000. How information systems influence user decisions: A research framework and literature review. *International Journal of Accounting Information Systems* 1 (3): 178–203.

O'Leary, D. E. 2013. Artificial intelligence and Big Data. *IEEE Intelligent Systems* 28 (2): 96–99.

Otley, D. 1999. Performance management: A framework for management control systems research. *Management Accounting Research* 10 (4): 363–382.

Parson, D. P. 1966. Individual right of petition: A study of methods used by international organizations to utilize the individual as a source of information on the violations of human rights. *Wayne Law Review* 13: 678.

Patterson, S. 2014. *Speed Traders Get an Edge*. Available at: http://online.wsj.com/news/articles/SB10001424052702304450904579367050946606562

Paul, R., and L. Elder. 2013. *The Thinker's Guide to Ethical Reasoning*. Tomales, CA: Foundation for Critical Thinking Press.

Pavlou, P. A. 2011. State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly* 35 (4): 977–988.

Plumlee, R. D., and M. A. Plumlee. 2008. Assurance on XBRL for financial reporting. *Accounting Horizons* 22 (3): 353–368.

Power, M. 2009. The risk management of nothing. *Accounting, Organizations and Society* 34 (6): 849–855.

Rai, S. 2014. *Despite Dramatic Half-Billion-Dollar Award in Satyam Scandal, "India's Enron," It May Be Years before Investors See a Dime*. Available at: http://www.forbes.com/sites/saritharai/2014/07/21/despite-dramatic-half-billion-dollar-award-in-satyam-scandal-indias-enron-it-may-be-years-before-investors-see-a-dime/

Rapoport, M., and J. S. Lublin. 2015. *Meet the Corporate Board's "Kitchen Junk Drawer"; Workload of the Audit Committee Has Expanded Well beyond Oversight of Financial Reporting*. Available at: http://blogs.wsj.com/cfo/2015/02/03/meet-the-corporate-boards-kitchen-junk-drawer/

Rockness, H., and J. Rockness. 2005. Legislated ethics: From Enron to Sarbanes-Oxley, the impact on corporate America. *Journal of Business Ethics* 57 (1): 31–54.

Romney, M. B., and P. J. Steinbart. 2015. *Accounting Information Systems*. Upper Saddle River, NJ: Prentice Hall.

Rottig, D., X. Koufteros, and E. Umphress. 2011. Formal infrastructure and ethical decision-making: An empirical investigation and implications for supply management. *Decision Sciences* 42 (1): 163–204.

Roychowdhury, S. 2006. Earnings management through real activities manipulation. *Journal of Accounting & Economics* 42 (3): 335–370.

Securities and Exchange Commission (SEC). 2014. *Fair Disclosure, Regulation FD*. Available at: http://www.sec.gov/answers/regfd.htm

Shapiro, B., and C. R. Baker. 2002. Information technology and the social construction of information privacy. *Journal of Accounting and Public Policy* 20 (4): 295–322.

Sipior, J. C., B. T. Ward, and N. M. Rongione. 2004. Ethics of collecting and using consumer internet data. *Information Systems Management* 21 (1): 58–66.

Siponen, M., and A. Vance. 2010. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34 (3): 487.

Snow, N. M. 2015. *Retail Investors' Perceptions of Financial Disclosures on Social Media: An Experimental Investigation Using Twitter*. Working paper, University of South Florida.

Soll, J. 2014. *The Reckoning: Financial Accountability and the Rise and Fall of Nations*. New York, NY: Basic Books.

Stansbury, J., and B. Barry. 2007. Ethics programs and the paradox of control. *Business Ethics Quarterly* 17 (2): 239–261.

Stone, D. L., and E. F. Stone-Romero. 1998. A multiple stakeholder model of privacy in organizations. *Managerial Ethics: Moral Management of People and Processes:* 35–59.

Sutrop, M., and K. Laas-Mikko. 2012. From identity verification to behavior prediction: Ethical implications of second generation biometrics. *Review of Policy Research* 29 (1): 21–36.

Sutton, S., V. Arnold, and T. Arnold. 1995. Toward an understanding of the philosophical foundations for ethical development of audit expert systems. *Research on Accounting Ethics* 1: 61–74.

Sutton, S. G., and J. R. Byington. 1993. An analysis of ethical and epistemological issues in the development and implementation of audit expert systems. *Advances in Public Interest Accounting* 5: 231–243.

Sykes, G. M., and D. Matza. 1957. Techniques of neutralization: A theory of delinquency. *American Sociological Review:* 664–670.

Tabak, F., and W. P. Smith. 2005. Privacy and electronic monitoring in the workplace: A model of managerial cognition and relational trust development. *Employee Responsibilities and Rights Journal* 17 (3): 173–189.

Todd, K. J. 2004. Using digital evidence to ferret out the dishonest employee. *Employee Relations Law Journal* 30 (2): 13–22.

Turilli, M., and L. Floridi. 2009. The ethics of information transparency. *Ethics and Information Technology* 11 (2): 105–112.

Tuttle, B., A. Harrell, and P. Harrison. 1997. Moral hazard, ethical considerations, and the decision to implement an information system. *Journal of Management Information Systems* 13 (4): 7–27.

United Nations. 1948. *Universal Declaration of Human Rights*. New York, NY: United Nations.

Unites States Department of Health and Human Services (HHS). 2003. *Summary of the HIPAA Privacy Rule*. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

Villars, R. L., C. W. Olofson, and M. Eastwood. 2011. *Big Data: What It Is and Why You Should Care*. White paper. Framingham, MA: IDC.

Vohs, K. D., N. L. Mead, and M. R. Goode. 2008. Merely activating the concept of money changes personal and interpersonal behavior. *Current Directions in Psychological Science* 17 (3): 208–212.

Weaver, G. R., L. K. Trevino, and P. L. Cochran. 1999. Integrated and decoupled corporate social performance: Management commitments, external pressures, and corporate ethics practices. *Academy of Management Journal* 42 (5): 539–552.

Webster, J., and R. T. Watson. 2002. Analyzing the past to prepare for the future: Writing a literature review. *Management Information Systems Quarterly* 26 (2): 3.

Wells, J. T. 2007. What is your fraud IQ? *Journal of Accountancy* 204 (6): 56–57.

Young, J. J. 2006. Making up users. *Accounting, Organizations and Society* 31 (6): 579–600.

APPENDIX A

Online Supplemental Material: http://dx.doi.org/10.2308/isys-51265.s01