

ETHICS OF BUSINESS CONTINUITY AND DISASTER RECOVERY TECHNOLOGIES: A CONCEPTUAL ORIENTATION

Christopher B. Davison

PhD Student, Capella University
Technology Manger, Rescue Project: University of California, Irvine, USA
cbdaviso@uci.edu

ABSTRACT

The ethical implications of business continuity/disaster recovery planning, and technology is rarely a topic discussed within the academic or practitioner literature. However, ethical decisions permeate such business continuity and disaster recovery areas as data custody, privacy, and security issues involved in the control and possession of business continuity data. In this paper, a discussion and analysis of the ethical considerations involved with business continuity and disaster recovery planning is presented. The ethical foundations of privacy are presented within the framework of the Kantian categorical imperatives, Christian golden rule philosophy, and Utilitarian philosophy. Building upon those foundations, a synthesis of the theoretical framework and arguments for data privacy and security is provided. This paper is relevant to both Information Technology practitioners as well as scholars in that it addresses ethical issues that are often overlooked in a predominantly technical domain.

Keywords: business continuity, disaster recovery, corporate ethics, privacy, data security.

1. INTRODUCTION

A multi-dimensional discussion and analysis of ethical considerations involved with business continuity and disaster recovery planning is presented in this paper. The goal of writing this paper is to provide a conceptual orientation that examines business continuity and disaster recovery science and practice through the lens of ethical theory. Information Technology (IT) continuity planning often involves movement and storage of others' personal data. Many times, this data is placed in the care of third parties. The concomitant ethical issues such as data privacy, customer expectations of privacy, and the trade-offs between ethics and efficiency are important issues worthy of analysis.

The first section of this paper is devoted to a discussion of the need for privacy framed within the context of the Kantian categorical imperatives, Christian golden rule philosophy, and Utilitarian philosophy. These philosophical arguments serve as the ethical and theoretical foundations for the need for privacy in free society. Following that discussion, a presentation of the theoretical framework for data privacy and security will ensue. This presentation will center on synthesizing the arguments for data privacy and security as well as the theoretical framework for data privacy and security. Next, a discussion of ethics in data custody, privacy, and security that presents issues involved in the control and possession of business continuity data will be provided. This discussion will focus on the hand-offs of data between various persons involved in continuity operations (specifically offsite personnel), the choice of encryption schemes for the data, and corporate ethics training. Following that discussion, the ideas regarding customer

expectations of privacy and customer expectations pertaining to corporate privacy policies are presented. Finally, a discussion of future ethical trends as well as the societal implications of technology within the context of data privacy and security will be offered.

This paper contributes to IT science and practice. Scholars will find the discussion of ethical theory applied to business continuity and disaster recovery systems and processes timely in that ethics and privacy are currently at the center of national research debate. Practitioners may note that the systems they build are designed to carry IP datagrams and not ethics. However ethics and privacy are ideas that impact the foundations of a democratic society.

A necessary condition of a democratic society is the freedom of citizens to exercise their autonomy (Johnson cited in Beauchamp & Bowie 2004). Privacy and the right to privacy is perhaps one of the largest ethical issues discussed in the IT research literature. The problem is that ethics are often less considered within IT practice. The intent is that this work will contribute to the considerations of ethics in relation to technology and the use of technology.

Computer ethicists such as Moor (1997) argue that as technologists struggle to make data access easier ("greased" (p. 27)) and data sharing more seamless, the unintended side effect is an increased risk of data loss or improper exposure of information. Unauthorized data, in the possession of unscrupulous hands, could threaten personal freedoms and the foundations of a democratic society.

Recently, the FBI admitted to making mistakes with regard to court-authorized wiretaps. These mistakes involved wiretaps, not necessarily of the roving kind, and Internet activity monitoring. The FBI mistakes resulted in 38,514 hours of untranslated telephone conversations and Internet logs. The FBI calls this data "collections of materials from the wrong source due to technical problems" (McNabb Associates 2005). The question remains if the data has been disposed of or archived.

2. ETHICAL FOUNDATIONS OF PRIVACY

The arguments for privacy could stem from Kantian philosophy, Christian golden rule philosophy, and Utilitarian philosophy. These foundational arguments, posited hundreds and even thousands of years ago, are relevant to the contingency planning discussion in that modern continuity technology and practices provide new avenues of encroachment into old ethical territory (i.e., privacy concerns). These arguments are explored in this section.

Immanuel Kant provides three versions of his categorical imperative. In the first version, Kant (1785/1964), states that we should "act only according to that maxim by which you can at the same time will that it would become a universal law." The second formulation of the categorical imperative is to "act in such a way that you always treat humanity, whether in your own person or in the person of any other, never simply as a means, but always at the same time as an end." Finally the third formulation compels us to "act as though you were through your maxims a law-making member of a kingdom of ends."

The Christian golden rule compels us to do unto others as we would have them do unto ourselves. It is similar to the formulations of the Kantian categorical imperative. Both of these maxims prescribe that we treat people and have them treat us in a manner that we would like to be treated. Using these ethical foundations, we would be compelled to respect others' privacy as we would have them respect our own.

Boatright (cited in Charters 2002) explains the Utilitarian foundation for the right to privacy as two-fold. The first is "the concern that the invasion of privacy can result in significant actual harm to individuals" (Charters 2002, p. 248). The collective benefit to society must outweigh the collective harm experienced by the individual in order to be considered ethical by Utilitarian philosophy.

The second Utilitarian foundation for privacy centers on the harm that privacy invasion can lead to in a larger sense. Boatright (cited in Charters 2002) explains that privacy is a necessary condition of some activities. The invasion of privacy harms the enjoyment of those activities. As such, the harm exceeds any perceived benefits from the invasion of privacy.

With regard to data privacy and security within business continuity planning, these formulations of the categorical imperative, golden rule, and Utilitarian philosophy would compel digital medium owners to treat the data contained on the medium as though it were their own personal data and respect the privacy needs of the individual. Thus, the following normative rule

for digital data is proposed: the personal data contained on the digital media is indeed the property of the individual to whom the data relates and only the digital medium is the property of the organization.

Personal information such as Social Security numbers and credit card numbers are not the property of the issuing authority or any organization that collects this information. Ultimately these numbers are the property of the individual. Responsibility for the use (and misuse) of these numbers falls upon the individual. Likewise the ownership rights fall upon the individual.

The arguments for ownership rights could be extended to digital representations of a person's face or other identifying pictures. As such, another normative statement is posited at this point: An individual's face (or other body parts) and voice should be treated as their property and any unauthorized representation, digital or otherwise, should be treated as conversion or copyright infringement. California Civil Code § 3344(a) contains an appropriation of likeness clause stating "Any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner or on or in products, merchandise, or goods, or for the purpose of advertising or selling, or soliciting purchases of products, merchandise, goods or services, without such person's prior consent ... shall be liable for any damages sustained by the person or persons injured as a result thereof." Interesting court cases could ensue from traffic light cameras or other forms of government surveillance including the FBI's mistaken wiretaps, especially if an individual took the time to successfully copyright and/or patent his likeness and voice.

3. DATA PRIVACY AND SECURITY THEORITICAL FRAMEWORK

There exists much literature that addresses the legal ramifications of data privacy and security. In the U.S., the Fourth Amendment, Gramm-Leach-Bliley Act, and California Civil Code 1798.80 – 1798.84 even codifies part of an individual's right to privacy. In Europe, the European Union's Data Privacy Directive provides regulations to protect the privacy of European citizens. While much overlap exists and the subjects are not cleanly differentiated, only the ethical issues involved in data privacy and data security will be addressed in this paper and not the legal aspects.

Moor (1997) discusses the ethical need for a person's right to privacy. He explains this right as an instrumental value (i.e., that which serves as a means to a good end) in that privacy enables us "to form intimate bonds with other people that might be difficult to form and maintain in public" (Moor 1997, p. 28). Secondly, if one accepts privacy as a necessary condition of freedom and democracy, then privacy is an intrinsic value (i.e., that which is good in itself). In the justification for privacy, which is often a central argument in the privacy debate, an intrinsic value is weighted more heavily than an instrumental value. Johnson (1994) believes privacy is an intrinsic value as a necessary condition of autonomy, assuming autonomy is an intrinsic value (e.g., being a necessary condition for free, democratic societies). However, Moor (1997) provides an interesting counter-example demonstrating autonomy without privacy.

Moor (1997) defends privacy rights on yet a third argument. He posits privacy as "the expression of the core value of security" (p. 30). Moor contends that security and protection are core values (i.e., those values that all normal human beings and cultures require for survival). He believes that as a society collects greater amounts of information, the need for protection against unethical use of this information manifests itself as a need for privacy. Therefore, Moor concludes that privacy is a plausible intrinsic value as it is an expression of the core value of security.

The intellectual linkage of privacy as an expression of security would propose a direct relationship between privacy and security. As people's privacy (in a highly computerized culture) increases so should their security. However, there are situations in which privacy and security have inverse relationships.

Consider the example of public parking structures. As people notice cameras and other monitoring devices, their perception of security increases and, presumably, so should their actual security increase. The perception of security increases even more if the person under surveillance believes that the video is being monitored by others such as the police or private security. This is a modern manifestation of the exchange of privacy (or freedom) for security.

Theories of privacy protection have evolved from Moor's (1990) restricted access view of privacy (i.e., levels of access) and Fried's (1984) control theory of privacy (i.e., controlling

information about ourselves). Emerging from these varying theories is Moor's (1997) situation dependant view of privacy that he terms the control/restricted access theory of privacy. This theory has the functionality of being able to fine tune levels of access to data that is appropriate for the situation. Moor gives the example of hospital data. The doctors have more access than nurses to hospital data. However, these doctors do not have complete access to all hospital data.

The control/restricted access theory of privacy (Moor 1997) is posited as a theoretical framework for information privacy. The theory is provided as a context-aware, situational dependant framework for protection of individual privacy in a computerized society. Philosophical debate continues on privacy as an intrinsic value or instrumental value and even on the definition of privacy. Whether or not philosophers and ethicists are able to define and categorize privacy, technologists should recognize that privacy is an important ethical consideration and societal value.

4. ETHICS IN DATA CUSTODY, PRIVACY, AND SECURITY

Organizations, the FBI included, should make ethical decisions with regard to storage and transportation of data. Take the example of storage and transportation of offsite backups. Many data centers chose a third party courier and storage solution for the purposes of data recovery during a disaster or unexpected IT infrastructure disruption. An ethical problem arises from the transfer of custody of the data.

It is not likely that the organization, contracting with a third party business continuity vendor, is aware of the entire chain of custody once the data leaves the premises. It is even less likely that the continuity vendor is aware of any organizational privacy policies that pertain to the data. Providing the name of the person last picking up the offsite backup materials would be a difficult challenge for many data center managers.

Data custody is further complicated by data communications networks. As Moor (1997) points out, technologists endeavor to make data more exchangeable as well as easier and faster to transport. These efforts have the potential side effect of making the unauthorized access of the data as easy and as fast. Internet Protocol (IP) is a protocol that is the accepted communication protocol of the Internet. However, IP was built with transmitting datagrams in mind and not ethical considerations of privacy.

Consider the example of performing data backups over the Internet. VPNs, encryption, and other methodologies exist to ensure data privacy and security. However, these technologies often add unwanted overhead in terms of costly equipment/software, computational requirements and network bandwidth. A trade-off between cost, speed and efficiency versus data privacy and security exists.

Any unencrypted IP datagrams, traversing multiple router hops on its way to delivery, could be easily monitored by anyone willing to sniff network packets. Even with encryption, the source and destination addresses (along with other IP datagram header information) must remain unencrypted in order to be delivered over the Internet. At the very least, the implication is that senders and receivers can have no reasonable expectation of temporal privacy. Who, when, and for how long, but not necessarily what, two organizations (dictated by unique IP address source and destination addresses) communicate is almost a matter of public record.

The same trade-off regarding encryption versus overhead could be extended to the creation of data storage. Whether creating tapes for offsite storage, or performing disk to disk file backups, an organization must decide on or against the use of encryption with the accompanying overhead. An unsecured, unencrypted data tape, leaving the premises for offsite storage, could be read by anyone in the chain of custody.

To further complicate the ethical issue of data privacy and security, consider paper files. Often, organizations such as healthcare providers are required to keep medical records for an extended period of time. Imagine the potential damage to individual privacy if those paper records were stolen or just lost from the back of a delivery truck on its way to long-term storage.

Corporate decisions to outsource add yet another layer of complexity to the ethics of data privacy and security. It is not clear how a company can control access to private customer information when call centers, helpdesks and the like are located overseas. Countries have varying degrees of emphasis on privacy and privacy laws. Furthermore, legal systems vary from country to county making prosecution and extradition non-trivial problems. U.S. privacy law may not be

applicable or extend to overseas contractors in many cases. As Klosek (2005) explains, it is important for organizations to understand the privacy, security, and legal implications of outsourcing decisions.

Corporate ethics and ethics training is another issue that may arise from outsourcing. Many companies are finding it in the best interests of all stakeholders and a strategic advantage to provide corporate ethics training (Childers 2005). This training should be serious ethics training with senior management support and not the "window dressing" (p. 380) variety reported in McKendall, DeMarr, and Jones-Rikkars (2002). While direct employees of corporations may be required to attend certain ethics training (e.g., California companies must provide their employees in supervisory roles with two hours of sexual harassment prevention training) this requirement may not extend to contractors. In the case of overseas contractors, it may prove impossible, or at least quite expensive, to provide ethics training; especially if that ethics training is located in a U.S. corporate office.

5. PRACTICALITY OF DATA PRIVACY AND SECURITY

Moor (1997) contends that Fried's control theory is impractical. Moore believes that in a highly computerized society, it is impossible to control personal information as it is communicated throughout the world. Moor's argument is centered on access control and informed consent of the individual.

Access control has its own myriad of complexities that ultimately could prove impractical. Referring back to Moor's (1997) hospital example, it is probable that the admitting personnel have the lowest access to all patient-oriented hospital data. Nurses would have the next highest access to all hospital data. Finally, doctors would have access to most hospital data. The highest level of access and ultimately to all hospital data is reserved for the database administrators. These people, not even in the chain of providing healthcare, have root and/or administrator access to all patient data and are charged with assigning access levels to the admitting personnel, nurses and doctors. Privacy violations at this level are quite possible and virtually impossible to detect.

Keeping within the example of hospital data, Moor (1999) contends that "computer programs that access these records can set access levels for different people (who, what, and when) and they can keep audit trails of users" (p. 261). While this is true in the general sense, the computer controlled access control mechanism is still ultimately controlled by database administrators, systems administrators, and any number of support personnel. Moor (1999) does agree that computers are not the entire solution to the data privacy dilemma. Part of the reason that this is true is due to systems architecture.

Just as technologists have "greased" (Moor 1997) information so that it can seamlessly move across platforms and technologies, the same technologists have greased the administration of the systems that contain the information. The technologists have architected systems that are completely exposed to any user, usually a systems administrator, with high enough access rights.

The idea of a super-user is built into Windows and Unix (including Linux variants) operating systems (OS) environments. The majority of computers housing information warehouses are of the Windows or Unix type using Oracle, DB2, MySQL, or Microsoft's SQL Server. Windows has an administrator account with complete access to any information stored on the machine. Likewise, the Unix root account has complete access to all system resources. Any user account granted administrator or root privileges (easily done by any competent systems administrator) has the same super-user access as the original. Additionally, anyone with the administrator or root password has complete control over the system including granting access privileges.

Users demand that system administrators fix problems ranging from email delivery, web content delivery, to database indexing. In order to cope with these varied demands and the demands of constant security patches and OS patching/upgrading, systems administrators need super-user privileges in order to efficiently perform their functions. Users also surrender super-user privileges to system administrators for protection purposes. In the first six months of 2005 there have been over 48 million customer data loss incidents resulting from security breaches (Newman 2005). Many of these incidents are perpetrated by systems administrators such as in the

case of Duronio and UBS. As such, this same super-user privilege nullifies the idea of effective automated access control posited by Moor (1999).

Audit trails are presumed to thwart super-user abuse by logging systems administrator and user activities. Recognized as one of the four main safeguards (Best, Mohay, & Anderson 2004), audit trail analysis (especially across heterogeneous computing environments) provides yet another set of research problems to be solved. While Moor (1999) contends that audit trail analysis can be utilized to detect system security activity, the feasibility of a knowledge based system for machine independent audit trail analysis has only been demonstrated (Best, Mohay, & Anderson 2004) and is far from being implemented in industry.

6. CONSUMER EXPECTATIONS OF PRIVACY

Anyone who has information about themselves stored on another party's digital medium is a consumer with expectations of privacy. At a minimum, there is an implied-in-fact contract that exists between the consumer and the owner of the medium. The consideration (i.e., compensation in return for goods or services) in the contract is monetary compensation or possibly a trade for goods in kind. In return for the compensation, the consumer has the expectation that not only the goods or services purchased will be rendered, but that the provider will protect any personal data collected. From the consumer's perspective the expectation can be articulated as "You, the provider, have my personal data and are entirely responsible for safeguarding and securing my personal data."

At a minimum, consumers of privacy should be informed of where, how and by whom, their personal information is stored, viewed, manipulated, shared, backed-up, and transported. Most companies have privacy policy statements which, in addition to attempting to communicate this information, try to balance their desire to collect marketable information with the desire to not alienate consumers. Markel (2005) describes the typical corporate privacy-policy statement as "full of misleading and deceptive rhetoric intended to cover up the gap between the company's privacy policy and the image it wishes to project" (p. 197). Markel's research on corporate privacy policies found that several large corporations' policies, as listed on their websites, were confusing and often times contradictory.

A well developed privacy policy statement and privacy practices could result in positive revenue for a company. According to Markel (2005), "the Pew Internet and American Life Project found that more than half of Internet users feel that collecting personal information invades visitors' privacy" (p. 198). A large majority seek an opt-in policy allowing the user to dictate what personal information is collected by which site (Merkow and Breithaupt, 2002). This expectation is comparable to standing at the checkout register of the grocery store where a consumer has the opt-in/opt-out ability of having his savings card scanned simply by not handing it to the cashier.

Complying with these customer desires could result in increased sales and, at the very least, a marketing strategy emphasizing the company's attention to data privacy and security ethics. However, it is disappointing to think that a well developed and adhered to privacy policy would evolve from marketing or sales strategies. As Markel (2005) describes it, "it would be more ethical if the company concluded that it should protect personal information because that is the right thing to do" (p. 213).

7. FUTURE ETHICAL CONSIDERATIONS

Moor (1999) points out that computers are quickly mapping the human genome. Computers are able to store and disseminate human genetic information at ever increasing speeds. Moore's Law has held true since it was first postulated in 1965. Potential privacy issues arise from genetic processing that impact many areas of human culture. From employment ramifications to selective marketing based on genetics, civilization should address ethical considerations in this area.

Another area that is gaining in popularity partly due to massive and inexpensive computational power is that of large-scale decision support systems. It is estimated that 95% of the Fortune 1000 companies either have a data warehouse in place or are planning to develop one (META Group 1996). Data warehouses are large (often in the terabyte range) repositories of data resulting from information being extracted, cleaned/scrubbed, and transformed from source systems (Gray and Watson 1998). The sales of data warehousing systems, software, and services

are expected to continue to grow (Eckerson, 1998). This increase in consumer data, and retail marketing of it in the case of Dun & Bradstreet among others, further illustrates the need for informed consent and an opt-in policy of data sharing.

Inexpensive, ubiquitous, and powerful sensing environments create further privacy challenges. Creating these multi-modal sensing environments is a popular research approach and also a popular security paradigm. In their research, Smith et al. (2005) promise to use RFID to "infer human activity directly from sensor readings" (p. 39). More cameras are being deployed in public spaces such as malls and traffic lights. After the London subway bombing, it was only a matter of days before the perpetrators were identified by cameras. This widespread deployment and usage of sensors imply large-scale ethical questions with regard to privacy. Exactly how much freedom will be surrendered for security and convenience is yet unknown.

Another pervasive sensing environment known as the Responsphere testbed is being created at University of California, Irvine. This author serves as the Technology Manager for the research project and thus the interest in the privacy implications of such technology. The Responsphere project seeks to instrument one third of the UCI campus with RFID, acoustic sensors, optical sensors, people counters, a variety of localization technologies, temperature sensors, accelerometers, motes, and other forms of multi-modal sensing. In addition to the hardware infrastructure, the Responsphere project provides a multi-agent simulator (MetaSim) which simulates crisis response activities within the testbed. While the project's main research thrust is in the disaster response domain, the privacy implications of technology is an active research area (Rescue Project 2006).

The Responsphere testbed is intended to be an open testbed for the purposes of testing IT solutions within a disaster response context (Responsphere 2006). Of interest to the Responsphere researchers are privacy preserving technologies that provide technological solutions to human privacy problems. The ideas of a privacy knob and a dynamic policy engine are among the research topics within the project.

A privacy knob is a concept that fits well with Moor's (1997) control/restricted access theory of privacy. Under normal circumstances, a privacy consumer within the Responsphere space would have his privacy knob set to the highest setting (e.g., set to 10 on a scale from 0 to 10). Provided that consumer has the proper credentials and is not in violation of any policy, the consumer's privacy should be protected. Protected privacy would include masking the consumer's image on the video sensors (Wickramasuriya, Alhazzazi, Datt, Mehrotra & Venkatasubramanian 2005), masking the RFID signature, as well as dropping his acoustic signature. Informed consent and control of private data appear to be achieved by this architecture if the privacy consumer is completely aware of all policies, restrictions, and consequences.

If the privacy consumer violates any predefined access control policy the privacy preservation technologies would cease and the consumer's information would no longer be masked or dropped. During the event of a disaster or medical related emergency, the privacy consumer would most likely prefer his privacy knob setting to go to 0, especially during an earthquake if he is trapped under a desk or having a heart attack. Allowing the pervasive sensing space to set the privacy knob to 0, in the event of an emergency, would reveal the consumer/casualty's location and possibly physical state to First Responders. This situation aware, adjustable policy structure is the concept behind the dynamic policy engine.

With the dynamic policy engine, privacy consumers would stipulate their privacy preferences. This would occur in cooperation with the infrastructure management, (i.e., those who own and manage the sensors). For instance, a privacy consumer would state that any cry containing "Help" would immediately set the privacy knob to 0. Additionally, the policy engine could contain language that instructs an email or phone call be made to some person of authority. Work continues at the project for specifying a language for privacy preservation and the dynamic policy engine.

8. SOCIAL IMPLICATIONS

Brin (2004) argues that society is at a crossroads. "Critical decisions during the next few years -- about research, investment, law and lifestyle -- may determine what kind of civilization our children inherit" (Brin 2004, p. 1). We may chose technology that creates an Orwellian nightmare of tyranny or chose technology that empowers the citizens to "watch the watchers"

(Brin 2004, p.5) in an egalitarian society. While these future choices have yet to be made, it is clear that technological advances will continue to occur at a rapid pace. There should not be and will not be any stopping of these sorts of scientific innovations and the privacy and ethical concerns these advancements bring about. No society or tyrannical regime has ever been successful in stopping these advancements. It would appear that society, the citizenry, and the scientific community should make ethics, responsibility, and accountability a focal point.

Consider the social implications of creating a privacy-aware packet routing network or business continuity system. No system has ever been built from the ground up as a privacy-aware, ethics-aware system. The ethical considerations of creating such a system would no doubt be a center of great debate. The issues of responsibility and accountability are a matter of great importance as well.

The initial thought when discussing such a system is that law breakers would feel free to do as they will. Law enforcement would feel powerless to track criminal behavior such as trading copyrighted materials as the privacy-preservation mechanisms would render tracking impossible. However, ethics-aware policies and the technology to empower such polices could make it possible to prevent such illegal activity from taking place. Instead of creating a situation where law enforcement could not track criminals, these types of technologies could prevent criminals from engaging in criminal activity. Such systems are, arguably, a distant future and a world of practicality away. However, they do appear possible or, at the least, imaginable.

9. CONCLUSION

The goal in writing this paper was to provide a conceptual orientation that examines business continuity and disaster recovery science through the lens of ethics. Theories as well as applied concepts were presented throughout the paper. Ethical considerations and practical considerations were synthesized and presented for evaluation.

The beginning section of this paper develops the need for privacy framed within the context of the Kantian categorical imperatives, Christian golden rule philosophy, and Utilitarian philosophy. The categorical imperatives and the golden rule compel humanity to act in a fashion as we would have others to act and to treat others as we would have them treat us. Coupled with the Utilitarian philosophy, these maxims would compel data medium owners to respect the property rights of others and treat the personal data contained on the medium as the property of others. Storage medium owners should treat the data as they would have others treat their personal information.

In the third section of this paper, the theoretical framework for data privacy and security was discussed. Moor (1997) argues that privacy is an instrumental value as well as an intrinsic value. Also, Moor argues that privacy is a core value of society. With this defense of privacy, Moor posits a control/restricted access theory of privacy as a theoretical framework for information privacy.

The next section of this paper was devoted to a discussion of ethics in data custody, privacy, and security that presents issues involved in the control and possession of business continuity data. The hand-offs of data between various persons involved in continuity of operations (specifically offsite personnel) was discussed. This discussion raised issue with chain of possession of backup data, the use of the Internet for data backups, as well as the choice of encryption schemes for the data. The impact of outsourcing on data privacy as well as ethics training was discussed as well.

Next, a discussion of the practicalities of data privacy and security was offered. Systems architecture with administrator and root accounts create difficulties (if not impossibilities) with regard to audit trails, access levels, and data privacy. Systems have been created that, while not making administration an impossible task, have complicated data privacy and security.

Following that, ideas regarding customer expectations of privacy and expectations regarding corporate privacy policies were presented. Research finds that corporate privacy polices are lacking clear explanation. Thus, the argument that companies should adopt and adhere to well-developed privacy policy statements was offered. If not because it is the right thing to do, at least because it could positively impact sales and the company's image.

After the privacy expectation discussion, a discussion of the future ethical considerations of data privacy and data security was presented. This discussion focused on human genome

mapping, trends in large-scale data warehousing, as well as the proliferation of multi-modal sensing environments. The research from the Responsphere project on the ideas of user controlled privacy knobs (in alignment with the control/restricted access theory) and the idea of a dynamic policy engine was presented. Work in the creation of a privacy policy language for pervasive sensing environments was presented as an area of ongoing and future research.

Finally, societal implications of technology were discussed. Technology will continue to advance rapidly and any attempt to halt this progression will be futile. The focus of the debate should not be the intrinsic nature (i.e., the goodness or evilness) of the technology but the responsibility and accountability (or lack thereof) enabled by the technology and wielded by the users of the technology. Ideally, ethical considerations could be a component of system design resulting in privacy-aware and ethics-aware systems. The concept of ethics as an integral systems design component is an opportunity for future research. Creation of such systems presents many research challenges for AI researchers, HCI researchers, software and hardware engineers, management scientists, and, of course, business continuity and disaster recovery scientists.

REFERENCES

- Beauchamp, T. and Bowie, N. (2004) *Ethical theory and business, 7th ed.*, Pearson, Upper Saddle River, New Jersey.
- Best, P. J., Mohay, G., and Anderson, A. (2004) 'Machine-independent audit trail analysis—a tool for continuous audit assurance', *Intelligent Systems in Accounting, Finance and Management*, **12**(2).
- Brin, D. (2004) 'Three cheers for the surveillance society' http://archive.salon.com/tech/feature/2004/08/04/mortal_gods/ (accessed December 27, 2006).
- Charters, D. (2002) 'Electronic monitoring and privacy issues in business-marketing: The ethics of the DoubleClick experience', *Journal of Business Ethics*, **35**(4), 243-254.
- Childers, D. (2005) 'Ethics as a strategy', *The Internal Auditor*, **62**(5), 34-37.
- Eckerson, W. W. (1998) 'Post-Chasm warehousing', *Journal of Data Warehousing*, **3**(3), 28-45.
- Fried, C. (1984) 'Privacy', *Philosophical Dimensions of Privacy*, Schoeman E (ed.), Cambridge University Press, New York.
- Gray, P. and Watson H. J. (1998) *Decision Support in the Data Warehouse*, Prentice Hall, Upper Saddle River, New Jersey.
- Johnson, D. G. (1994) *Computer Ethics, 2nd ed.*, Prentice Hall, Upper Saddle River, New Jersey.
- Kant, I. (1964) *Groundwork of the Metaphysic of Morals*, Harper and Row, New York. (Original work published 1785)
- Klosek, J. (2005) 'Data privacy and security are a significant part of the outsourcing equation', *Intellectual Property & Technology Law Journal*, **17**(6), 15-19.
- Markel, M. (2005) 'The rhetoric of misdirection in corporate privacy-policy statements', *Technical Communication Quarterly*, **14**(2), 198-215.
- META Group (1996) 'Industry overview: New insights in data warehousing solutions', *Information Week*, 1-27.
- McKendall, M., DeMarr, B., and Jones-Rikkers, C. (2002) 'Ethical compliance programs and corporate illegality: Testing the assumptions of the corporate sentencing guidelines', *Journal of Business Ethics*, **37**(4), 367-384.
- McNabb Associates (2005), 'Federal Bureau of Investigation', *Federal Crimes Blog*, <http://www.federalcrimesblog.com/2005/10/federal-bureau-of-investigation.html> (accessed December 27, 2006)
- Merkow, M. S. and Breithaupt, J. (2002), *The E-privacy imperative: Protect your customers' Internet privacy and ensure your company's survival in the electronic age*, Amacon, New York.
- Moor, J. (1990) 'Ethics of privacy protection' *Library Trends*, **39**(1), 69-82.
- Moor, J. (1997) 'Towards a theory of privacy in the information age', *Computers and Society*, **27**(3), 27-32.
- Moor, J. (1999) 'Using genetic information while protecting the privacy of the soul', *Ethics and Information Technology*, **1**(4), 257-263.

- Newman, A. (2005) 'Database security best practices', *Security*, **42**(8), 32-34.
- Rescue Project (2006), 'Research Thrusts', <http://www.itr-rescue.org> (accessed December 26, 2006).
- Responsphere (2006), 'An IT infrastructure for responding to the unexpected', <http://www.responsphere.org> (accessed January 4, 2007).
- Smith, J.R, Fiskin, K.P., Jiang, B., and Mamishev, A. (2005) 'RFID-based techniques for human-activity detection', *Association for Computing Machinery, Communications of the ACM*, **48**(9), 39.
- Wickramasuriya, J., Alhazzazi, M., Datt, M., Mehrotra, S., and Venkatasubramanian, N. (2005) 'Privacy-protecting Video Surveillance', *SPIE International Symposium on Electronic Imaging (Real-Time Imaging IX)*.

Received: June 15th 2006

Accepted in final format: April 8th 2007 after three revisions.

About the author

Christopher B. Davison is working towards his PhD degree at Capella University. He is the Technology Manger for the Rescue Project: University of California, Irvine, USA and can be reached at cbdaviso@uci.edu.