Protecting Personal Information in Continuous Control Monitoring and Continuous Audit Environments

by

Marilyn Greenstein-Prosch, Ph.D., CIPP
Arizona State University
School of Global Management and Leadership

Working Paper
October 2006

Protecting Personal Information in Continuous Control Monitoring and Continuous Audit Environments

Marilyn Greenstein-Prosch, Ph.D.
Arizona State University
School of Global Management and Leadership

Section 1: Introduction

According to many sources, 2005 was the worst year by far in terms of the sheer number of privacy breaches made by organizations[1]. Unfortunately this negative trend has continued into 2006; "the dizzying pace of data-breach notifications in recent months shows no signs of slowing, as several more organizations have disclosed major data compromises over the past few days."[2] Privacy issues, including both security and corporate abuse of personal information, are being hotly debated in the US between consumer advocacy groups, privacy advocacy groups, legislators, regulators, industry groups and the press. State legislators, frustrated with the lack of federal legislation, have increasingly been enacting their own legislation with California typically leading the way. Internationally, the US has far less privacy protection for consumers and employees than the EU, Canada, Australia, Switzerland, and Argentina, among others.

As the cost of data collection, storage, and processing increasingly declines due to software and hardware enhancements, the ability for individuals to control data kept by business and government entities also declines. What is considered a precious asset by many businesses is the object of concern by many individuals. In the past, businesses collected data primarily about customers based on their purchasing history. These same businesses, along with ever-changing technology, now have web-based and wireless

[1] Lemos, Robert. 2005. "Data Security Moves Front and Center in 2005," *Security Focus*, December 29, 2005. http://www.securityfocus.com/news/11366

[2] Vijayan, Jaikumar, and Todd Weiss. 2006. "Flurry of New Data Breaches Disclosed," *Computerworld Online*, June 29, 2006. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001282

capabilities that allow them to monitor and record other types of behavior, such as browsing activity, frequently without the knowledge or consent of the individual. "The computer has been accused of harboring a potential for increased surveillance of the citizen by the state, and the consumer by the corporation [Clarke, 1988]

The objective of this paper is twofold. First, a discussion of the cultural lag [Ogburn, 1966] in the management of personal information (PI) that has resulted from the advances in technology accelerating faster than the capacity to control such information is presented. The second objective is to briefly introduce the AICPA/CICA's Generally Accepted Privacy Principles (GAPP) and to discuss how these principles can, and ultimately should, be used in Continuous Control Monitoring (CCM) and Continuous Audit (CA) environments containing personal information. The benefits of using the criteria in GAPP and incorporating them into CCM and CA environments are also discussed.

Section 2: Technology, Privacy and Cultural Lag

The value of privacy protection of personal information is hotly debated. As we consider this issue, one important question posed by businesses as they are confronted by various groups to invest in data protection and privacy enhancing technologies and processes is this – *what is in it for me*? Cavoukian and Hamilton (2002) espouse the benefits of the privacy payoff to businesses, asserting that "being exposed as a privacy misfit can damage your company's reputation, lead to costly litigation and send your customers running to the competition." That book was written by two Canadians, one of whom was the Privacy Commissioner of Ontario at about the same time that wide-sweeping federal legislation was being phased in for all organizations operating in

Canada. The Canadian legislation, Personal Information Protection and Electronic Documents Act (PIPEDA), was largely based on the European Commission's 1995 Data Protection Directive. Increasingly, Canadian companies are finding themselves with a competitive advantage simply because they keep their customers' data in Canada and specifically not sending it to the U.S. because it is better protected in Canada [McQuay, 2006] As the value of privacy protection is discussed, differences between the U.S. and other prominent economic communities must be noted as well.

A fundamental difference between the European Commission's widely recognized and pioneering E.U. Data Protection Directive and the U.S. privacy regime regarding employees is succinctly stated as employer data collection requirements (U.S.) vs. employee privacy rights (E.U.). Anti-discrimination laws and worker safety laws in the US require that employees collect all types of personal information, whereas the collection of such data in the E.U. is generally strictly prohibited. Consider that while Canada and its provinces and the E.U. and its member countries all have some form of Privacy Commissioner's office, the U.S. has no equivalent position at the federal level, and very few at the state level. Regarding customers, the EU provides data protection for all consumers that requires that personal data on the Internet be:

- processed fairly and lawfully;
- collected and processed for specified, explicit legitimate purpose;
- accurate and current; and
- kept no longer than deemed necessary to fulfill the stated purpose.

Further, users have the following rights:

- access;

- correction, erasure, or blocking of information;
- object to usage;
- oppose automated individual decisions; and
- judicial remedy and compensation.

Since consumers in the U.S. do not have the same sort of data protection mandated in the E.U. and Canada, among other countries, the question to businesses is whether this privacy is valued. Millions of data transfers occur every day between the U.S. and E.U., and the E.U. directive gives its member countries essentially "a global reach" with an attached liability for non-compliance. Basically, non-European companies have to meet the E.U.'s directive if they want to conduct electronic commerce in Europe or risk legal action. In response to the E.U.'s Directive, the U.S. Department of Commerce and the European Commission developed a "safe harbor" framework in July 2000 that allows U.S. organizations to satisfy the requirements and ensure that personal data flows to the United States are not interrupted. The safe harbor framework "bridges the differences between the EU and U.S. approaches to privacy protection and ensures adequate protection for EU citizen's personal information." Many U.S. privacy advocates are upset that the implementation of safe harbor provisions by U.S. firms will result in greater privacy rights for foreign citizens than for the U.S.'s own citizens.

The cultural differences in these countries have had a profound impact on the evolution of privacy protection requirements. Cultural differences can shape expectations, and expectations can, to some extent, shape legislation and regulatory requirements [Shapiro and Baker, 2001]. Technology as an enabler of the silent erosion of a reasonable expectation of privacy is arguably occurring in the U.S. [Shapiro and

Baker, 2001] and to a lesser extent, in the E.U. and Canada. The difference is likely due to the cultural expectations of the two populations and the approaches by government and regulatory agencies to either protect the consumer (E.U.) or to protect business (U.S.). The resulting fundamental differences in privacy environments and privacy practices between these different cultures is reminiscent of a sentiment made by Tinker [1988] that no reason exists "why the social environment should be treated as inevitable and immutable; it has to be created, together with the institutions that populate it." Society's expectations about privacy can actually be eroded [Shapiro and Baker, 2001].

At this juncture in the U.S., the trajectory that privacy issues will take, both now and in the future, is uncertain. What is certain is that if technological solutions are not offered in a cost-effective manner to businesses in a largely self-regulated environment then the solutions offered will not then be embraced by the businesses. Marshall [1999] notes that the rapid rise of the Internet and electronic commerce has not allowed the ethical support theory and implementation to develop at a fast enough rate to maintain a proper balance between technology and individual rights. This phenomenon is known as Ogburn's cultural lag theory where rapid technological progress occurs with inadequate development of ethical support for new technology [Ogburn, 1966] Rapid technological advances that easily allow privacy infringements are widely in use, yet little has been done to implement privacy through technology [Karat et al., 2006]. Data security and flagrant breaches of privacy have recently reached an epidemic stage, and consumers are beginning to question whether they want to accept the erosion of their privacy by the business community.

Ethicists and groups, such as the Center for Democracy and Technology, have been championing privacy efforts since technology that easily and cheaply allows e-

surveillance first became available; however, "until a technology has achieved a critical level of social diffusion sufficient to engender popular controversy, broad social attention is seldom given" [Marshall, 1999]. The relationship between technology, social culture and privacy controls is illustrated using an adaptation of Ogburn's cultural lag diagram in Figure 1.

Insert Figure 1 Here

Typically, Ogburn's cultural lag theory is categorized as one of four types of cultural lags: material culture accelerates faster than nonmaterial culture, material culture accelerates faster than other types of material culture, social culture accelerates faster than material culture, or nonmaterial culture accelerates other types of nonmaterial culture [Brinkman and Brinkman, 20005]. In trying to understand privacy, technology and consumer's expectations, three elements are present: 1) material culture – technologies, such as the internet and wireless devices, such as RFID technologies, 2) social culture – consumer's expectations of privacy, and 3) material culture – privacy enhancing technologies and controls.

The relationship among these three elements is illustrated in Figure 1. Up until time a, technology, privacy expectations and privacy controls are all fairly congruent. New technologies (such as the ability to track clickstream data, use global positioning systems and wireless devices) begin to get introduced at time a, at which point in time social expectations and controls over the new technologies became lagging behind the new technologies. Then as members of society begin to realize that the data is being collected, shared, even generated as in the case of profiles that are shared, and sold among companies, and that the data is not all that well protected against theft or loss, cries for greater protection begin to be made at time b. During the period between points

b and c, the awareness of privacy issues is raised and the increased privacy expectations cause the community to seek enhanced material culture in the form of privacy enhancing technologies and controls.

At this point in time, our society is somewhere between time periods b and c in Figure 1. In 2005, 81% of firms surveyed experienced the loss of one or more laptops containing sensitive information during the past 12 months [Ponemon Institute and Vontu, 2006], 4% of all Americans were affected by identity fraud in 2005 [Weiss, 2006], and over 200 privacy breaches have been reported thus far in 2006 affecting millions of people. A study conducted by Javelin and the Better Business Bureau found that for a 12 month period ending in early 2006, 8.9 million individuals in the US were victims of identity fraud. Further, the average amount per fraud victim was $6,383 and the average fraud resolution time spent by each victim was 40 hours! Thus, technology has accelerated faster than controls and monitoring devices have been developed and implemented to control the associated technologies that were previously developed and implemented, and a period a maladjustment has resulted. This is a time period where much focus needs to be placed on creating and implementing the privacy enhancing technologies and controls so that the environment can return to a more adjusted state. The next sections discuss current privacy technologies and the need for privacy enhancing technologies and controls that are designed to be effective, continuous, measurable and auditable, so that members of society can be assured that their privacy needs are being met.

Section 3: Data Touchpoints and Associated Technologies

Data concerns arise surrounding certain critical data touchpoints. Events where data are collected, processed, stored or used are considered to be touchpoints. Figure 2 illustrates such touchpoints. It also illustrates the many times and ways in which data may be replicated. Data may be collected in digital format directly from the individual when he/she is on the Internet. The data collected may be entered directly by the individual or it may be data recorded about what the individual is doing on the organization's website, such as which items or pages are examined and/or for how long. Logs of chats may be kept as well. Data need not be entered digitally, however, for it to end up in an organization's database. Data, such as medical histories, may be collected on paper-based forms and entered into the computer. Also, transactions need not occur on the Internet to be recorded in the corporate database; for example, data about purchases made at retail stores or phone orders may also be transferred to the database. Data collection does not stop with the individual, however, notes/observations made by employees of the organization may also be collected, linked to the individual, and entered into the system.

Insert Figure 2 here

Once data is collected by the original organization with which the individual is conducting business or visiting, the data may be shared with other subsidiaries or the parent company, called the Organizational Family System in Figure 2. The data may be shared with both the operational databases and the data warehouses. Organizations may also forward the data on to affiliate organizations for a variety of reasons:

- it may need the data to help process the transaction (e.g. credit card company)

- it may need the data to help fill the order (e.g. a transportation company or a supplier that is drop-shipping to the customer)
- data-sharing arrangements may have been negotiated.

Individuals and organizations should be informed about any such onward transfers of data for any of the above reasons and how the data will be kept and used by such affiliates. Further any of the data touchpoints referred to in Figure 2 may be collected, used, or stored by a third party processor on behalf of the organization.

Data at rest and data in transit are both at risk; the number of laptop thefts/losses as mentioned earlier is at an unacceptably high level - 81% of firms surveyed experienced such losses in 2005. Further, given the increased uses of wireless devices, the security of data being transmitted must be treated as if it is going over an unsecured channel and thus be encrypted as well as the data at rest.

Technologies and declining cost of storage devices make data replication and data sharing very ease at a low cost. Data replication and data sharing presents challenges for the adequate correction of data inaccuracies and fulfilling data purging requests by individuals. Data is often cleansed and/or transformed before it goes into a data warehouse or is transferred/shared with another company. Such processes may make it even more difficult to process update or deletion requests throughout the system. Also, a firm may no longer have an affiliation with an organization with which it did previously. In fact, over time, an organization may have many different affiliation agreements. Keeping track of which data was transferred at any given point in time would require that very detailed logs be kept on all such transfers. To further exasperate

the problem, data that has been forwarded to an affiliate may have been sold as a result of the sale or merger of the affiliate with another company.

Data backup and recovery procedures can also add to the difficulty of fulfilling correction and deletion requests. Data in master or reference files that have been either corrected or deleted since the last backup, may have the errors reintroduced if backup restorations are made and the updates are lost. Also, periodic replication procedures to update two files will reintroduce a purged record if has not been successfully purged from the multiple databases that are being cross-referenced and replicated as illustrate in Figure 3. John Doe notifies a company to purge them from their database. Except for necessary transactional data, such as purchase information, the business unit purges John's request from its data warehouse. If the same purge notification is not sent to the organizational family database, then during periodic cross-referencing update/replication of data, John Doe's data may be reintroduced to the business unit's system from the corporate-wide system.

Insert Figure 3 Here

Wireless devices, by definition, are unsecured from interception, so personal information sent over these devices, like all other confidential information, needs to be secured with some form of encryption. Wireless devices are increasingly coming equipped with global positioning system (GPS) devices. Technology has been developed to allow the location of cell phone users to be identified. The Federal Communications Commission mandated that the capability be in place by the end of 2001 to allow fire and police rescue workers to be able to pinpoint 911 callers. Many privacy advocates are concerned about what businesses will do with wireless devices that enable the recording of the device's location and time. The term automatic location identification (ALI) data

has been coined to represent this type of data. One example of how this data has been used against a consumer is a Connecticut man who was very surprised when he got an extra $400 plus bill charged to his debit card by a car rental agency, Acme Rent-A-Car. Upon inquiry, he found out that the system tracked his location and speed and billed the man each time he exceeded the speed limit in excess a certain period of time. This incident outraged privacy groups that a corporation would track the whereabouts of its customers. Car rental industry advocates claim that they are just tracking and protecting their assets.

A concern by many individuals is having their whereabouts tracked and linked to their personally identifiable information. Should private agencies become law enforcers? In most cases, they are not turning the records over to the law enforcement agencies yet, but could that be next? What about the sharing of data with an automobile insurer where a ticket was not issued, but driving habits in violation of the law were still recorded? Somewhat naively, many individuals have their whereabouts tracked on the Internet, but now when their off-line, physical whereabouts may be tracked from either GPS systems in their cars (or a rented car) or phones have many individuals worried about "Big Brother" excesses. Also, the sharing of such data with affiliate firms is also a concern of many individuals.

In terms of marketing data, many marketing firms would enjoy being able to market specific wireless advertisement to individuals profiled with a certain traffic pattern. For example, if a marketing firm "learns" that an individual travels a certain route everyday beginning around 5:15 PM, around 5:00 they may start sending advertisements or coupon codes for gas stations, restaurants, and bars that are on the route. Depending on whom you ask, this could be construed as intelligent marketing or

annoying invasions of privacy. In terms of good privacy practices, such advertisements should only be sent if the individual has agreed to have their locations tracked and if they want to receive such advertisements.

Another big issue being debated by privacy experts is the use of RFID tags. RFID tags contain microchips and very small radio antennas than can be attached to products. They transmit a unique identifying number to an electronic reader, which in turn links to a computer database where information about the item is stored. Many privacy advocates are concerned about these devices being placed in items which can be read very easily from a distance and personal items being used to track both the whereabouts of individuals and personal use patterns of such devices.

Section 3: Privacy Enhancing Technologies

Given the developments in technology that allows organizations to collect a multitude of types of PI, some software consortiums and vendors have already begun to develop privacy enhancing technologies. This section will briefly review one consortium and two software vendors that are developing privacy enhancing technologies. Developed by the World Wide Web Consortium (W3C), the Platform for Privacy Preferences (P3P) is a mechanism designed to make it easier for consumers to understand whether a particular website's privacy policy is in congruence with their own privacy policies. P3P is designed so that consumers can, through an online interview process, indicate their privacy preferences. When the consumer visits a website, a P3P-enabled browser can then compare that consumer's preferences with a P3P-enabled organization's privacy policies. Any discrepancies found between the consumer's privacy preferences

and the websites privacy practices will be displayed to the consumer. Thus, the consumer does not need to read the privacy policy of each site visited.

P3P does not, however, monitor the sites to determine whether they actually follow their own privacy policies. Also, P3P does not P3P does not include mechanisms for transferring data or for securing personal data in transit, such as Secure Sockets Layer (SSL), or data at rest. Thus, the purpose of P3P is to provide a standardized format for defining privacy preferences of consumers and privacy practices of websites and identifying discrepancies.

An example of a company providing commercial solutions that are focused on assisting companies secure and protect confidential information is Vontu. The products that Vontu offers are add-on programs that companies may use – their various products scan files looking for unprotected, confidential information, monitor servers examining all files being passed through servers, and actively block email and web communications that contain confidential data, including email, web and secure web (HTTP over SSL), and file transfers (FTP).

Systems are best controlled when they are designed and integrated into the system. P3P is a good, sound concept, but it only addresses the privacy policies of the business as they are self-reported by the company. No actual audit or monitoring of the company to determine if it actually follows its policies is present. Vontu provides some nice tools that organizations may wish to use as they develop or enhance their privacy programs, but it does not provide a holistic, built-in approach to privacy assurance. IBM has developed a comprehensive approach with its Enterprise Privacy Authorization Language (EPAL). Enterprise Privacy Authorization Language (EPAL) is a mechanism by which an organization can extend specific privacy rules across internal business

systems and then automate compliance to those rules. While P3P communicates privacy policies from business applications to consumer applications, EPAL goes one step further, providing an XML language that enables organizations to enforce P3P policies behind the Web, among applications and databases [IBM, 2003]. The next section of this paper discusses the accounting profession and privacy, followed by a section discussing accountants, privacy enhancement, and continuous control monitoring.

Section 4: GAPP and Accountants as Providers of Assurance Services

In 2001, the AICPA formed a Privacy Task Force to develop a Privacy Framework and Criteria which resulted in the formulation of Generally Accepted Privacy Principles (GAPP) that could be used by accounting firms all sizes to provide privacy services and *assurances* to their clients. As mentioned previously, various U.S. and international legislative acts have been passed. This myriad of legislation can make privacy assessment and compliance an overwhelming task. One objective of the AICPA's task forces is to provide a consistent framework for developing sound, auditable privacy practices that when implemented will likely comply with any applicable legislation. Accountants are uniquely qualified to provide and implement comprehensive privacy services. Greenstein and Hunton (2002) give the following reasons why accountants are uniquely qualified to provide these services. Accountants have the ability to:

- comprehensively understand both current and future statutory regulations that may be applicable to a firm
- assess the risk faced by a firm for inadequate privacy policy and practices

- align systems and infrastructure with developed policies and close any privacy gaps
- design both high-level plan and detailed working documents in order to achieve privacy compliance
- identify the various privacy components, as well as build and implement any necessary changes to them to close any privacy gaps
- assess the adequacy of privacy policies and practices of relevant business partners and service providers
- monitor the implemented system's compliance with its stated policies and practices

Each of these core skill sets are based on activities that accountants have been performing for decades in their attest, assurance and tax advisory services. A major problem with P3P and stated privacy policies is that a consumer has no real way of knowing whether a firm abides by it. For example, if a consumer requests that a firm erase personal information from their database, such as, items browsed on a web site over the past 5 years, they have no way of knowing whether this data was in fact purged on both its operational database and its archived databases. Accountants are uniquely positioned to provide an attest function over compliance with stated privacy practices.

The FTC has recently been investigating organizations that have not been adequately protecting personal information, and have required that some of them, such as Petco, Tower Records, Microsoft, and ChoicePoint, obtain a third party privacy audit every two years for a period of 10- 20 years. While the FTC does not specify by whom or what standards these audits should be performed, GAPP provides a sound set of

auditable privacy criteria. GAPP is composed of 10 Privacy Principles and 66 auditable criteria with examples. These 10 principles are listed and defined in Table 1. GAPP actually goes beyond what is required by the FTC in its orders to these companies that have experienced security breaches.

Insert Table 1 Here

GAPP is presented in three-column format. The first column contains the criteria[3]. The second column, which contains illustrations and explanations, is designed to enhance the understanding of the criteria. The illustrations are not intended to be comprehensive, nor are any of the illustrations required for an entity to have met the privacy criteria. The third column contains additional considerations, including supplemental information such as good privacy practices and selected requirements of specific laws and regulations that pertain to a certain industry or country. With each principle, the criteria are organized as either policies and communications or procedures and controls. The following table illustrates a breakdown of each component by the number and type of criteria for each, and the following section details the 10 principles and the 66 criteria.

Criteria	Principles										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
Policies & Communications	3	2	3	3	2	2	3	2	2	2	24
Procedures & Controls	7	3	4	3	2	7	4	6	2	4	42
Total	**10**	**5**	**7**	**6**	**4**	**9**	**7**	**8**	**4**	**6**	**66**

[3] These criteria meet the definition of "criteria established by a recognized body" described in the third general standard for attestation engagements in the United States in Chapter 1 of Statement on Standards for Attestation Engagements No. 10, *Attestation Engagements: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101.24), as amended, and in the standards for assurance engagements in Canada (CICA Handbook, paragraph 5025.41).

Greenstein and Hunton (2002) also distinguish between the AICPA's WebTrust Online Privacy offering, however, that product offering is restricted to data collected from web-based ecommerce forms and is generally related to providing consumer confidence. Some specific differences between WebTrust and GAPP are:

- GAPP encompasses the protection of data, in any format, as it being collected, processed, used, and maintained. Thus, it provides guidance in the protection of all forms of electronically and paper-based data collection, storage and use.
- GAPP includes the protection of employee data in addition to customer data.
- GAPP includes the protection and appropriate use of data after it is collected and provides guidance on data retention and data destruction policies.

WebTrust Online Privacy Services now fall under GAPP as assurance services can potentially be scoped such that they only include online operations, but only if that data is not co-mingled with other enterprise-wide data.

Section 5: Continuous Control Monitoring Environments and GAPP

As mentioned earlier, the ability to track PI has accelerated faster that the ability to control and monitor such PI. Privacy enhancing technologies and methodologies are in their infancy. Developing privacy technologies and methodologies with a continuous monitoring/assurance perspective makes good business sense given the many recent privacy breaches. With traditional financial audits, "the major obstacle to adopting a continuous process remains the lack of commitment by organizations to invest in the

technology required to develop and implement a continuous auditing process" [Alles et al, 2006]. The same arguments are being heard on the privacy assurance front as well. However, great opportunity exists for companies developing/enhancing privacy regimes to design continuous monitoring and reporting components into the system since we are still in the early development stages. As of the end of 2006, no company has as of yet received an assurance opinion based on GAPP. Practitioners are currently using GAPP as a consulting framework with the goal of helping organizations to adopt a best practices mindset, and hopefully leading the organizations down a path that will ultimately allow them to meet all of the criteria in the future.

GAPP does not specifically have continuous audit requirements, but it does have many process-related criteria that lend themselves well to continuous monitoring and reporting processes. Thus, while the formal assurance opinions that can currently be rendered are for a historical period, the "process" requirements contain many salient ingredients for a continuous control monitoring environment (CCM). CCM is a management methodology aimed at facilitating corporate operations, supervision and meta-supervision through the constant measurement of corporate activity, its comparison against standards and the reporting of discrepancies leading to corrective management action [Alles et al., 2006]. Further continuous audit (CA) techniques may also be used to monitor personal information and evaluate it more frequently than the "historical" perspective. Table 2 categorizes the 66 criteria into whether they are more process oriented (CCM) or data oriented (CA). A few of the criteria fall into both categories.

Insert Table 2 Here

Placing each of the criteria into one of these two "buckets" provides guidance for developing specific metrics and guidance for extending GAPP to a continuous environment. Assurance can be performed at three different levels [Alles et. al, 2006]: opinion level, process level, and data level. This categorization is very useful for providing guidance for privacy assurance engagements. GAPP can currently be used for a historical opinion level assurance, such as the one illustrated in Figure 4. These opinions would necessitate an evaluation of all of the relevant 66 criteria including both the process-oriented items and a historical evaluation of data. A more frequent process level assurance (PLA) can be useful for continuous monitoring of the effectiveness of the process-related criteria. Table 3 illustrates, through a few examples, how the GAPP criteria might be enhanced to facilitate PLA. Further, many of the criteria can be implemented and evaluated in a "data-driven" fashion if the system is designed to collect the data for such evaluations. Table 4 illustrates, through a few examples, how the GAPP criteria related to data (CA) might be enhanced to facilitate data level assurance (DLA).

Insert Tables 3 and 4 Here

Section 6: Discussion

The accounting profession has recognized that protection of personal information is an important aspect of controlling an organization's systems and business environment. Undoubtedly, material and social lags have occurred between privacy-invasive technologies, consumers' awareness and expectations of privacy issues, and privacy enhancing technologies. Accountants are already guiding top management to implement sound ethical and reliable systems, and corporate accountability for controls has increased due to Sarbanes-Oxley. Many of the tasks involved in protecting personal

information build upon characteristics and skills that members of the accounting profession already have [Greenstein and Hunton, 2003]. The AICPA/CICA has responded to the cultural lag by developing a comprehensive set of auditable privacy criteria. In this paper, the merits of enhancing GAPP to both CCM and CA environments were discussed. A presentation of how this might be obtained by categorizing the 66 GAPP criteria into each of these environments was given. Further, specific criteria were analyzed and extended to include CCM and CA activities and sample metrics were given to illustrate how privacy protection activities can be monitored and audited using continuous methodologies. Future researchers can perform case studies on organizations to determine the feasibility of these criteria and control techniques from a cost-benefit perspective. They can also be used to present a privacy-compliance "dashboard" to management.

Endnotes

AICPA/CICA. 2006. *Generally Accepted Privacy Principles*. AICPA/CICA.

Alles Michael, Alexander Kogan, Miklos A. Vasarhelyi, and J. Donald Warren, Jr. *Continuous Auditing: A Portfolio Assembled for the Bureau of National Affairs*. Rutgers University, 2006.

Brinkman, Richard L. and June E Brinkman. 2005. "Cultural Lag: A Framework for Social Justice," *International Journal of Social Economics*. Vol.32, Iss. 3; pp. 228-249.

Cavoukian, Ann and Tyler Hamilton. 2002. *Privacy Payoff*. McGraw-Hill.

Clarke, Roger A. 1988. "Information Technology and Dataveillance" *Communications of the ACM*, Vo. 31, No. 5, May.

Greenstein, Marilyn and James Hunton. 2003. "Extending the Accounting Brand to Privacy Services, *Journal of Information Systems*. Vol. 17, No. 2, Fall.

IBM. 2003. IBM Introduces New Language to Automate Privacy Compliance, Press Release, July 2, 2003.

Karat, Clare-Maried, and Carolyn Brodie, and John Karat. 2006. "Usable Privacy and Security for Personal Information Management," *Communications of the ACM*, Vol. 49, No. 1.

McQuay, Terry. 2006. "Privacy is changing Outsourcing in Canada," *Globeandmail.com*, July 27.

Ogburn, W.F. 1966. *Social Change*. Dell Publishing, New York, NY.

_____. 1957. "Cultural lag as theory", *Sociology and Social Research*, Vol. 41, pp. 167-74.

Poneman Institute and Vontu, Inc. 2006. 2006 Cost of Data Breach Study.

Shapiro, Brian, and C. Richard Baker. 2001. "Information Technology and the Social Construction of Information Privacy," *Journal of Accounting and Public Policy*, 20, pp. 295-322.

Tinker, Tony. 1988. "Panglossian Accounting Theories: The Science of Apologizing in Style," *Accounting, Organisations and Society*, vol. 13, No. 2, pp.-165-189.

Weiss, Todd. 2006. "Customers don't want data handled by outside vendors: They'll likely go elsewhere if a data breach occurs," *Computerworld Online*, October 24, 2006.

Figure 1
Ogburn's Sequential Time-Paradigm of Cultural Lag
Technology, Social Culture, and Privacy Controls

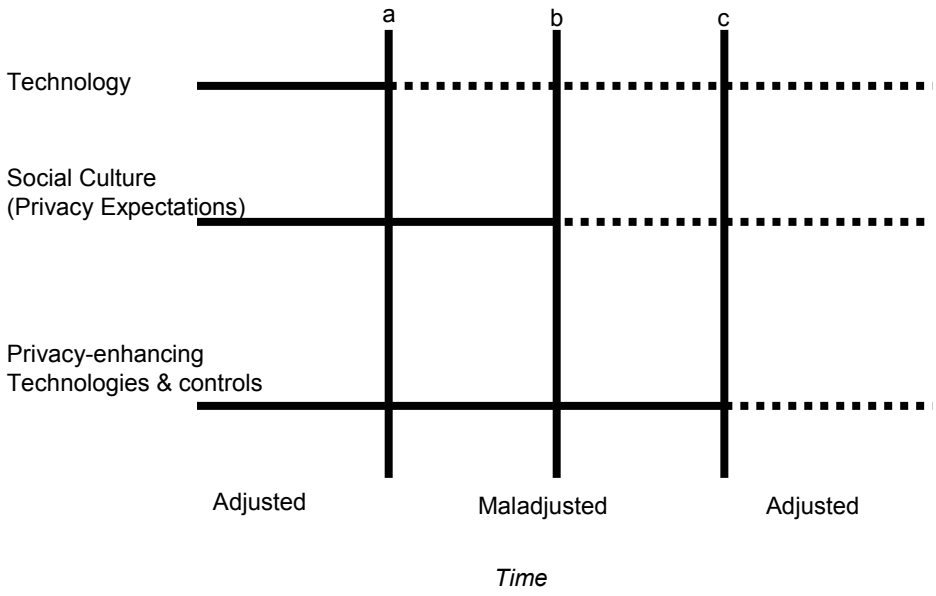

Figure 2
Data Touchpoints

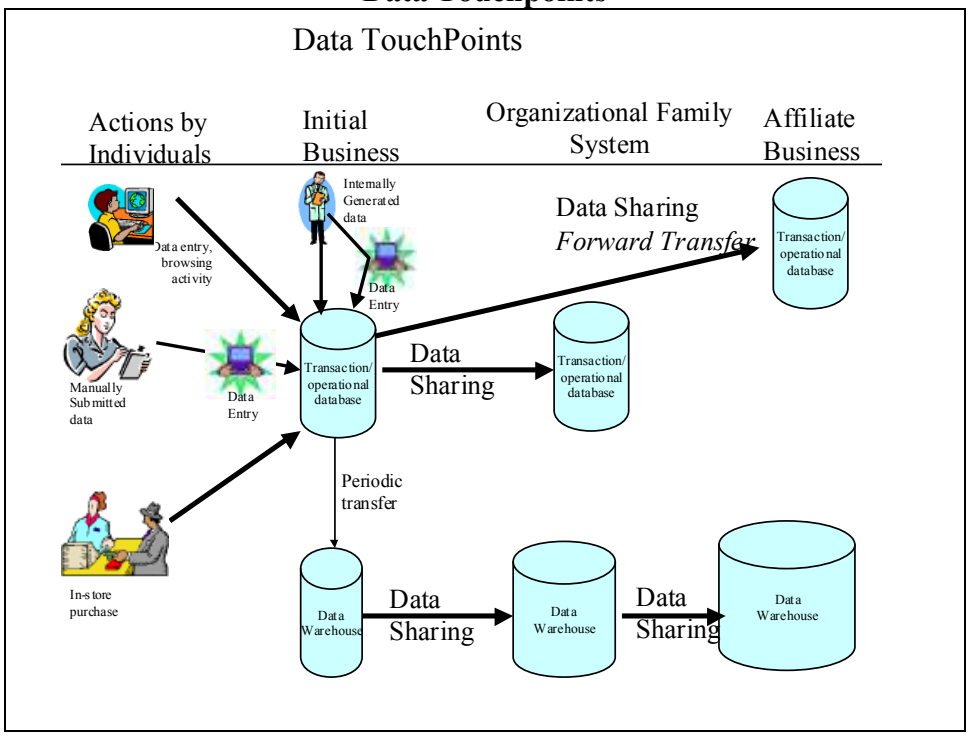

Figure 3
Data Correction/Update

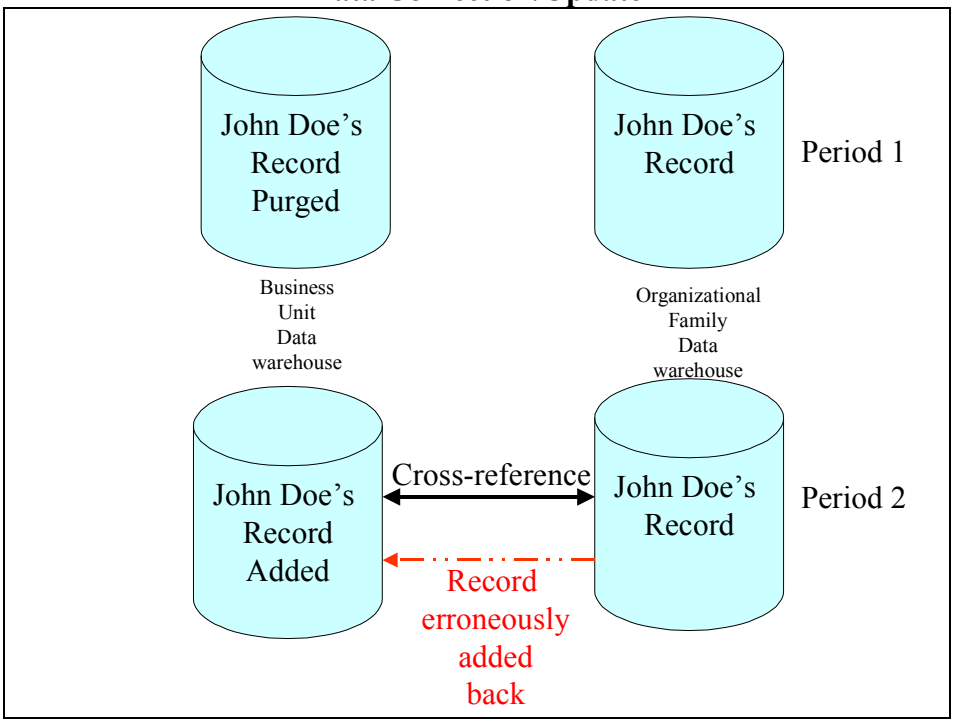

Figure 4
Reporting Directly on the Subject Matter Under AICPA Attestation Standard
Independent Practitioner's Privacy Report – GAPP Example

To the Management of ABC Company, Inc.:

We have examined (1) the effectiveness of ABC Company, Inc.'s (ABC Company) controls over the personal information collected in its _____ [*description of the entities and activities covered, for example "the mail-order catalog-sales operations"*] business (the Business) to provide reasonable assurance that the personal information was collected, used, retained, and disclosed in conformity with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants, and (2) ABC Company's compliance with its commitments in its privacy notice related to the Business during the period Xxxx xx, 2006 through Yyyy yy, 2006. ABC Company's management is responsible for maintaining the effectiveness of these controls and for compliance with its commitments in its privacy notice. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of ABC Company's controls over the privacy of personal information, (2) testing and evaluating the operating effectiveness of the controls, (3) testing compliance with ABC Company's commitments in its privacy notice, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, during the period Xxxx xx, 2006 through Yyyy yy, 2006, ABC Company, in all material respects (1) maintained effective controls over privacy of personal information collected in the Business to provide reasonable assurance that the personal information was collected, used, retained, and disclosed in conformity with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles; and (2) complied with its commitments in its privacy notice.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]

[*Date]*

Table 1
AICPA Generally Accepted Privacy Principles

1. **Management**. The entity defines, documents, communicates, and assigns accountability for its privacy policies and documents
2. **Notice**. The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **Choice and consent**. The entity described the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, retention and disclosure of personal information.
4. **Collection**. The entity collects personal information only for the purposes identified in the notice.
5. **Use and retention.** The entity limits the use of personal information to the purposes identified in the notice and the information for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.
6. **Access**. The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties**. The entity discloses personal information to third parties only for the purposes identified in the notice and only with the implicit or explicit consent of the individual.
8. **Security**. The entity protects personal information against unauthorized access (both physical and logical.
9. **Quality**. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement**. The entity monitors with its privacy policies and procedures to address privacy-related inquiries and disputes.

Table 2
GAPP Criteria Categorized as CCM or CA

CCM - Process	CA – Auditable Data
1.1.1 Communication to Internal Personnel	1.1.0 Privacy Policies - Management
1.1.1 Responsibility and Accountability for Policies	2.1.0 Privacy Policies - Notice
1.2.1 Review and Approval	2.1.1 Communication to Individuals - notice
1.2.2 Consistency of Privacy Policies and Procedures With Laws and Regulations	2.2.1 Provision of Notice
1.2.3 Consistency of Commitments With Privacy Policies and Procedures	2.2.2 Entities and Activities Covered
1.2.4 Infrastructure and Systems Management	2.2.3 Clear and Conspicuous (Conspicuous)
1.2.5 Supporting Resources	3.1.0 Privacy Policies - Choice and Consent
1.2.6 Qualifications of Internal Personnel	3.1.1 Communication to Individuals – Choice and Consent
1.2.7 Changes in Business and Regulatory Environments	3.1.2 Consequences of Denying or Withdrawing Consent
2.2.3 Clear and Conspicuous (Clear)	3.2.1 Implicit or Explicit Consent
4.1.2 Types of Personal Information Collected and Methods of Collection (documented)	3.2.2 Consent for New Purposes and Uses
4.2.1 Collection Limited to Identified Purpose	3.2.3 Explicit Consent for Sensitive Information
4.2.2 Collection by Fair and Lawful Means	3.2.4 Consent for Online Data Transfers to/From an Individual's Computer
4.2.3 Collection From Third Parties	4.1.0 Privacy Policies – Collection
5.2.1 Use of Personal Information	4.1.1 Communication to Individuals - Collection
5.2.2 Retention of Personal Information	4.1.2 Types of Personal Information Collected and Methods of Collection (communicated)
6.2.1 Access by Individuals to Their Personal Information	5.1.0 Privacy Policies – Use and Retention
6.2.3 Understandable Personal Information, Time Frame, and Cost	5.1.1 Communication to Individuals – Use and Retention
6.2.7 Escalation of Complaints and Disputes	6.1.0 Privacy Policies – Access
7.2.1 Disclosure of Personal Information	6.1.1 Communication to Individuals – Access
7.2.2 Protection of Personal Information	6.2.2 Confirmation of an Individual's Identity
7.2.4 Misuse of Personal Information by a Third Party	6.2.4 Denial of Access
8.2.1 Information Security Program	6.2.5 Updating or Correcting Personal Information

Table 2 (Continued)
GAPP Criteria Categorized as CCM or CA

8.2.6 Testing Security Safeguards	7.1.0 Privacy Policies – Disclosure to Third Parties
9.2.1 Accuracy and Completeness of Personal Information	7.1.1 Communication to Individuals – Disclosure to Third Parties
9.2.2 Relevance of Personal Information	7.1.2 Communication to Third Parties
10.2.1 Complaint Process	7.2.3 New Purposes and Uses
10.2.3 Compliance Review	8.1.0 Privacy Policies – Security
	8.1.1 Communication to Individuals – Security
	8.2.2 Logical Access Controls
	8.2.3 Physical Access Controls
	8.2.5 Transmitted Personal Information
	9.1.0 Privacy Policies – Quality
	9.1.1 Communication to Individuals – Quality
	10.1.0 Privacy Policies – Monitoring and Enforcement
	10.1.1 Communication to Individuals – Monitoring and Enforcement
	10.2.2 Dispute Resolution and Recourse

Table 3
GAPP and Process Level Assurances
*(Columns 2 and 3 are **NOT** part of GAPP)*

Criteria	Controls in Place	Frequency
1.1.1 Communication to Internal Personnel Privacy policies and the consequences of noncompliance with such policies are communicated at least annually to the entity's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	1. Employees are provided with electronic versions of the privacy policy annually. 2. Employees are electronically quizzed annually over the privacy policies. 3. Employees electronically agree that a) they understand the policy and b) that they will abide by the policy. 4. All of the above items are repeated each time a *significant* change in privacy policy is made.	Upon hire and annually
1.1.2 Responsibility and Accountability for Policies Responsibility and accountability are assigned to a person or group for documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	1. The name and contact information of the person that is responsible for privacy within an organization is encoded into an XML tagged form. 2. The name of this person is included in the annual distribution of the privacy policy to employees (see 1.1.1).	Monthly examination

Table 3 (Continued)
GAPP and Process Level Assurances
*(Columns 2 and 3 are **NOT** part of GAPP)*

1.2.1 Review and Approval Privacy policies and procedures and changes thereto are reviewed and approved by management.	1. An authorization to change the privacy policy should be completed and signed by a person designated in 1.1.2 as being responsible for privacy, and legal counsel, if appropriate. 2. All authorized changes should be logged and linked to the version of the privacy policy to which it was made.	Monthly examination
1.2.2 Consistency of Privacy Policies and Procedures With Laws and Regulations Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever there are changes to such laws and regulations. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.	1. An initial formal review of applicable laws and regulations is performed and the privacy policies and procedures are designed to be in compliance with applicable laws and regulations. If laws and regulations are being phased in, then a specific implementation plan is designed. 2. A person or group is identified as being responsible for monitoring current laws and regulations and assessing the adequacy of any planned phase-ins identified in the preceding item. 3. This person or group responsible prepares a laws and regulation form indicating any new laws or regulations that have been enacted since the last report, an impact assessment, and a plan of action if applicable. This form is to be signed by the person identified in 1.1.2 and legal counsel if applicable.	Initially Monthly Monthly

Table 3 (Continued)
GAPP and Process Level Assurances
*(Columns 2 and 3 are **NOT** part of GAPP)*

1.2.3 Consistency of Commitments With Privacy Policies and Procedures Internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.	1. Contracts with third-parties that collect, use or store personal information on behalf of the companies are reviewed and inconsistencies are formally noted. 2. A resolutions plan is developed to address any inconsistencies and it is signed by the person identified by 1.1.2. If necessary, customers and/or employees are notified of the discrepancies.	Initially and Quarterly Initially and Quarterly
1.2.5 Supporting Resources Resources are provided by the entity to implement and support its privacy policies.	1. A privacy resource budget to support the privacy program is prepared and approved by the person designated in 1.1.2 as being responsible for privacy and is approved by management. 2. The resources available and used to support the privacy program are tracked and monitored.	Annually Quarterly
1.2.6 Qualifications of Internal Personnel The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.	1. Formal job descriptions are in place for personnel responsible for protecting personal information. 2. Formal job descriptions are reviewed for appropriateness. 3. Verification and documentation of employees skills/experience and job description/experience are made during the hiring process by human resources. 4. Certifications and credentials, such CIPP or CISA, are kept current and verified by human resources. 5. Changes in technology and privacy requirements are identified and a plan of action for updated training is made by the person identified in 1.1.2 as being responsible for privacy.	As created Annually As hired Quarterly Semi-annually

Table 4
GAPP and Data Level Assurances
*(Columns 2 and 3 are **NOT** part of GAPP)*

Criteria	Controls in Place	Frequency
2.1.0 Privacy Policies The entity's privacy policies *address* providing notice to individuals.	1. Management develops and reviews the notice component, verbage, and mechanisms and the person identified in 1.1.2 as being responsible for privacy completes and signs a notice policy review form.	Annually
2.1.1 Communication to Individuals Notice is provided to individuals regarding the following privacy policies: • Purpose for collecting personal information • Choice and Consent (See 3.1.1) • Collection (See 4.1.1) • Use and Retention (See 5.1.1) • Access (See 6.1.1) • Onward Transfer and Disclosure (See 7.1.1) • Security (See 8.1.1) • Quality (See 9.1.1) • Monitoring and Enforcement (See 10.1.1) If personal information is collected from sources other than the individual, such sources are described in the notice.	1. XML fields are encoded with the specifics of each of the privacy components listed to the left and developed in 2.1.0 for online operations. 2. For off-line data collection, verification is made that physical privacy policies are prominently posted in a highly visible site (short notice) and/or hard copies (long version) are easily and readily available.	1.Continuous random inspection for availability and comparison with authorized, archived notice xml tags. 2.Random inspections are made at least every quarter.

Table 4 (Continued)
GAPP and Data Level Assurances
*(Columns 2 and 3 are **NOT** part of GAPP)*

2.2.1 Provision of Notice Notice is provided to the individual about the entity's privacy policies and procedures: ▪ At or before the time personal information is collected, or as soon as practical thereafter. ▪ At or before the entity changes its privacy policies and procedures, or as soon as practical thereafter ▪ Before personal information is used for new purposes not previously identified.	1. Verification that an "I understand" field has been checked after the privacy notice has been display and before any data is collected. This field needs to be electronically "time-stamped" for online operations so that verification can be made that the notice was provided before the data was collected. 2. Verification that if a significant change is made in privacy polices and procedures, returning customers must be notified of the changes in the privacy policy and check and "I understand" field. 3. Verification that if data is still being used or shared with other parties and the data is being used for new purposes policies, a logged attempt to email the customer of the change in privacy policy must be made and they must be notified of the privacy policy.	1. Random inspections are made monthly. 2. Random inspections are made monthly. 3. Random inspections are made monthly.
1.2.2 Entities and Activities Covered An objective description of the entities and activities covered by the privacy policies and procedures is included in the entity's privacy notice.	1. XML tagged and encoded descriptions are available for predefined business entities and activities 2. Tags are periodically reviewed 3. Definitions of entities and activities are reviewed	Random inspections are made monthly.
2.2.3 Clear and Conspicuous The entity's privacy notice is conspicuous and uses clear language.	1. An linguistic expert verifies that the notice is appropriately written. This written verification is kept in a hardcopy file and reviewed. 2. Verification that the privacy policy is displayed on the home page and on any and all pages with data collection.	1. Initially and whenever a notice change is made. 2. Random inspections are made monthly.

Table 4 (Continued)
GAPP and Data Level Assurances
*(Columns 2 and 3 are **NOT** part of GAPP)*

3.1.0 Privacy Policies The entity's privacy policies address the choices available to individuals and the consent to be obtained.	1. Management develops and reviews the choice component, and mechanisms used to get obtain consent and the person identified in 1.1.2 as being responsible for privacy completes and signs a choice policy review form.	Annually
3.1.1 Communication to Individuals Individuals are informed: ▪ About the choices available to them with respect to the collection, use, and disclosure of personal information. That implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires otherwise.	1. XML fields are encoded with the specifics of choices available to them about the collection, use and disclosure of PI and developed in 3.1.0 for online operations. 2. XML fields are used to track both implicit (opt-out) and explicit consent (opt-out) for the specified choices. These choices need to be time-logged.	1.Continuous random inspection for availability and comparison with authorized, archived choice xml tags. 2.Continuous random inspection that customer choices are being updated to the customer data files.