FF&H

WHITE PAPER

Will Your Company Pass a Privacy Audit?

by Tammi K. Franke

The Issue -

Companies that collect personal information are under increasing scrutiny by both consumers and governments in the United States and internationally. According to the Privacy Journal's *Compilation of State and Federal Privacy Laws*, there are more than 700 state and federal laws on privacy and surveillance, including two major pieces of federal legislation - the Heath care Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). Forty-five states currently have laws requiring businesses to notify individuals of any data security breach of personal information. The European Union (EU) established a Data Protection Directive that requires each EU member country to enact laws prohibiting the transfer of personal information to non-EU countries that do not adequately protect privacy. With this large number of laws, it seems like a complex and overwhelming task to determine the privacy/data protection laws that apply to your business and to actually comply with them.

Most businesses would like to comply with privacy laws, but efficiency is key in business today. A cumbersome privacy compliance process that diminishes the profitability of your company won't work, but a multi-million dollar lawsuit over your privacy practices is not an option either. As a start, a verification or "audit" is a practical solution for determining the scope, quality and integrity of your company's current privacy practices.

Like your other business systems, privacy practices and policies need strategy, planning and process to be efficient. Planning for and executing an audit includes each of these steps. Ultimately, a completed third party or external audit of your privacy practices can engender trust with consumers and be a competitive differentiator for your company.

But how do you begin to implement a privacy compliance system and prepare for an audit? Reviewing the American Institute of Certified Public Accounts' (AICPA) and Canadian Institute of Chartered Accountants' (CICA) **Generally Accepted Privacy Principles** (**GAPP**) is a great first step. GAPP's privacy framework, principles and criteria assist organizations in the design and implementation of sound privacy practices and policies. GAPP was also designed to guide CPAs when auditing an organization's privacy practices.

The Principles –

GAPP's privacy principles and criteria are founded on concepts from state, national and international privacy laws as well as good business practices. They provide a framework on which businesses can begin building a privacy compliance program.

The following are AICPA/CICA's 10 generally accepted privacy principles, which can serve as an initial checklist to assess your current privacy status:

1. **Management**. The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

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 describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

4. **Collection**. The entity collects personal information only for the purposes identified in the notice.

5. **Use, retention, and disposal**. The entity limits the use of personal information to the purposes identified in the notice and 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 or as required by law or regulations and thereafter appropriately disposes of such information.

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 with the implicit or explicit consent of the individual.

8. **Security for privacy**. 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 compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

Measurable criteria are also provided for each of the 10 privacy principles to guide the development of your company's privacy program.

The Basics –

Following are some basic definitions to guide you when planning your compliance program and audit:

Communication – business' communication to individuals, internal personnel, and third parties about its privacy notice and its commitments regarding personal information and any other relevant information regarding privacy.

Confidential Information – The exchange of nonpublic business information or data that one or the other party requires be maintained on a confidential or "need to know" basis. Unlike the restrictions on the use and disclosure of personal information, which is subject to laws or regulations, restrictions on the use and disclosure of confidential business information are usually defined through contractual obligations.

External Audit - External auditors, such as CPAs, perform attestation and assurance services. An external auditor evaluates a business's privacy program and controls in accordance with GAPP and provides reports that are useful to individuals, customers, and business partners.

Internal Audit - Internal auditors provide objective assurance and consulting services designed to improve a business's operations. Internal auditors can evaluate your privacy program and controls using GAPP as a benchmark, and provide information and reporting to management.

Nonpersonal information - deidentified or anonymized information that cannot be associated with specific individuals such as statistical or summarized personal information where the identity of the individual is unknown or has been removed. Nonpersonal information ordinarily is not subject to privacy protection unless it is subject specific regulations or agreements; for example, nonpersonal information related to clinical research or market research.

Personal information or Personally Identifiable Information – information that is about, or can be related to, an identifiable individual such as customers, employees, or others with whom your company has a relationship. Some examples of personal information are:

- Name
- Home or e-mail address
- Identification number (for example, a Social Security Number)
- Physical characteristics
- Consumer purchase history

Privacy - the rights and obligations of individuals and organizations regarding the collection, use, retention, disclosure, and disposal of personal information.

Privacy policies - written statements that convey management's intent, objectives, requirements, responsibilities, and standards regarding personal information.

Procedures and controls - the actions a business takes to achieve the GAPP criteria.

Sensitive personal information – types of information defined by law as particularly sensitive and usually require an extra level of protection and care. Some examples of sensitive personal information are:

- Information on medical or health conditions
- Financial and credit information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

Preparing for the Audit –

Strategy. Prior to formulating your company's privacy strategy, conduct an inventory of the amount and types of personal information your company 1) collects, 2) processes and 3) discloses to third parties. Preparing a visual diagram with the flow of personal information, including inputs, processing, storage locations, outputs, personnel and third parties touch points and access, is extremely helpful in understanding the current status of your company's privacy obligations. Once this inventory is complete, the next step is ensuring that GAPP is tailored to your business' specific legal privacy requirements. By consulting with an attorney, you can determine the legal requirements that apply to the personal information you collect based on the locations where you operate (jurisdictional) or your specific industry (regulatory). Once you are aware of the scope of the personal information collected by your organization and the specific legal requirements related to that information, you are ready to formulate an overall privacy strategy.

Your company's privacy strategy is intended to describe the expected or intended future status of your privacy compliance program. In the strategy phase, you will determine the vision for an ideal program – is it mere compliance or competitive differentiation/market leadership? Establishing your company's program vision

will help you prioritize preferences and goals. Once you identify your goals, you will identify specific milestones for achieving those goals and proposed implementation factors, such as budgets and development costs. GAPP can assist you in clarifying your business's privacy objectives and ensure that you include the proper goals and milestones.

Planning. Once your strategy is set, the program planning process begins with a privacy-risk assessment. A risk assessment establishes a privacy risk baseline for your organization. The AICPA/CICA designed a Privacy Risk Assessment Tool to help accomplish this task. A risk assessment team uses the tool to record scores for each of the 10 principles and 73 criteria contained in GAPP.

Before assigning someone in your company to lead the privacy risk assessment, you should determine if it would be beneficial for the privacy risk assessment to be shielded from disclosure in a lawsuit via attorney-client privilege. Meet with your legal counsel to discuss the scope and objective of the privacy risk assessment. If it is completed under attorney-client privilege, legal counsel will control communication and distribution of the results of the assessment. Other risk assessment team members should be individuals who possess a good understanding of privacy laws regulations, best practices, operations and your company's current privacy practices and controls. This could be someone from the legal, IT, risk management, internal audit or privacy department, or an outside consultant.

At the end of the privacy risk assessment, the assessment team will deliver a detailed report that includes the scores for each of the GAPP principles and criteria along with recommendations for corrective actions, including any urgent ones. From this report, management can begin to move forward on the operational guidelines required to implement a sustainable compliance process.

Process. In the process phase, your company will develop, document, introduce, and institutionalize the privacy program's action plan. To assist in establishing controls over personal information, GAPP provides illustrative controls and procedures for all of the GAPP principles and criteria. These are crucial to the creation of your privacy program. For example, the first GAPP principle is: "Management - The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures." GAPP provides two management criteria for this principle: 1) Policies and Communications and 2) Responsibility and Accountability for Policies. For the "Policies and Communications" criteria, GAPP provides several illustrative controls and procedures, including:

- Privacy policies are documented in writing and made readily available to internal personnel and third parties who need them.
- The entity periodically communicates to internal personnel relevant information about the entity's privacy policies.
- Changes to its privacy policies are communicated shortly after approval.

For the "Responsibility and Accountability for Policies" criteria, examples of the GAPP illustrative controls and procedures are:

- The entity assigns responsibility for privacy policies to a designated person, such as a corporate privacy officer.
- A committee of the board of directors includes privacy periodically in its regular review of overall corporate governance.
- A process is in place to periodically identify the risks to the entity's personal information. Such risks may be external (such as loss of information by vendors) or internal (such as e-mailing unprotected sensitive information). When new or changed risks are identified, the privacy risk assessment and the response strategies are updated. The process considers factors such as experience with privacy incident management, the complaint and dispute resolution process, and monitoring activities.

With the privacy risk assessment report and scoring results, and the illustrative controls and procedures, your privacy team members will have a roadmap for implementation of your privacy strategy and plan. At the completion of the process phase, your company will have implemented the following:

- Systems, procedures, and processes to address privacy requirements
- Updated privacy compliant forms, brochures, and contracts
- Internal and external privacy awareness programs
- Change control process for any additional requirements

By designing a implementing a privacy program using the tools and guidelines provided by AICPA/CICA and GAPP, you'll be prepared for an evaluation of the program via a privacy audit.

The Audit –

Once you have implemented your privacy program and have some operating history, you are ready to evaluate the effectiveness of your organization's privacy program via an internal or external audit. An audit will help your company: 1) understand how your privacy program compares to industry best practices; 2) minimize exposure to liability; 3) improve efficiencies in your privacy program operations; and 3) ensure ongoing compliance.

Internal auditors provide objective assurance services designed to improve operations. They help you accomplish your objectives by bringing a systematic approach to evaluate and improve the effectiveness of your privacy program processes. Using GAPP as a benchmark, internal auditors can evaluate your privacy program's internal controls and provide the results to management for review and follow-up.

External auditors, such as CPAs or other consultants, can perform third-party attestation and assurance services. Generally, the third-party nature of these services build trust in your privacy program by enhancing transparency. An external auditor can evaluate your privacy program and controls in accordance with GAPP and provide reports useful to individuals, customers and business partners.

Either type of audit should use objective audit criteria based on industry standards, such as GAPP. The audit should examine the effectiveness and coverage of your privacy program and business processes – is it broad enough and does it actually work? The auditor will also examine whether the program meets the goals the company has stated for the program.

Internal Audits. An internal audit process usually includes the following steps:

1. Notification – The notice, or engagement letter, from the auditor indicates the objective of the audit, audit staff members assigned to the audit, the projected time frame of the audit and the information the auditors will need from you.

2. Planning – After reviewing the information, the auditor will draft an audit plan, and schedule an opening meeting. Written policies and procedures, internal controls, organizational charts and job descriptions allow auditors to plan the audit and to become more familiar with the company's operations.

3. Opening Meeting – The opening meeting includes senior management and any staff that will be involved in the audit. The attendees will discuss the purpose, scope and process of the audit, the time frame and any potential timing issues that could impact it.

4. Fieldwork – Fieldwork typically consists of talking with staff, reviewing procedure manuals, testing for compliance with your privacy program and laws and regulations, and assessing the adequacy of internal controls.

5. Communication – Throughout an internal audit, the auditor will discuss any proposed recommendations and prepare a finding sheet. Written responses should include: a plan of action, the person responsible for implementation and the target date for completion.

6. Draft Report - A draft report is prepared with a background section, the scope of the audit and detailed commentary describing the findings, recommendations and an overall conclusion. Once the draft report is prepared, you are provided with an opportunity to respond to the audit recommendations.

7. Closing Meeting - A closing meeting will be held so that everyone can discuss the audit report and review your management responses. This is an opportunity to discuss the audit process and any remaining issues. After the closing

meeting, the auditor will finalize and distribute the audit report to management and the board of directors.

8. Follow Up Audits - Follow-up audits are performed on all audit findings. These are usually performed within six months after the initial audit report is issued to verify that agreed-upon corrective actions have been implemented.

External Audits. If you are considering conducting an external audit of your privacy program, privacy seal programs are a cost-effective alternative. A privacy seal is an identifiable symbol of a third party to signify that you have implemented and are following effective privacy practices.

Any privacy seal program should: 1) have broad adoption; 2) address both sensitive and nonsensitive personal information; and 3) be accessible to individuals. It is also important for your chosen seal provider to have the depth to handle inquiries and complaints, and police seal recipients to maintain the integrity of the seal.

Two well-known organizations that provide a privacy seal are TRUSTe and Webtrust. The minimum requirements of these programs are that organizations: post a comprehensive online privacy notice with contact information for opt-outs; complete a privacy self-assessment and audit; and agree to ongoing monitoring and dispute resolution.

WebTrust is an AICPA/CICA seal that requires a CPA audit. A WebTrust audit is broader than a privacy audit. It incorporates principles and related criteria for security, availability, processing integrity, privacy, and confidentiality.

TRUSTe is the first organization to introduce a privacy seal specifically for mobile sites and apps. TRUSTe consulted with groups like the Mobile Marketing Association and the Internet Advertising Bureau when developing the mobile privacy seal program. The TRUSTe mobile seal program includes a mobile-optimized privacy notice, a micro seal that is visible on mobile device screens, and cross-platform monitoring.

According to TRUSTe, to be certified, mobile application and site providers must complete: 1) a review of all key user interactions that are related to information flow especially those concerning sensitive geo-location data; 2) an assessment of data management practices including the collection, storage, use and sharing of personally identifiable data; and 3) a verification of each mobile app, mobile web and/or PC web site against TRUSTe program requirements.

The cost of seal standard seal programs are normally tied to revenues so that small and mid-sized companies can take advantage of them without a large impact on the budget.

Conclusion –

The ultimate goal of any privacy compliance program should be transparency and stewardship. A program with transparency provides open communication to individuals regarding all activities surrounding the capture, collection, dissemination and use of personal information. With stewardship as a goal, your company assumes a fiduciary-like responsibility when it handles personal information.

Implementing a privacy compliance program does take time, but the pay-off with consumers is significant. Not only will your legal counsel and auditors celebrate your accomplishment, your customers will reward you with increased trust and transactions with your company.

Sources:

- AICPA - http://tinyurl.com/27t8j2v
- GAPP Executive Overview - http://tinyurl.com/3w9seuy
- The Privacy Journal, http://www.privacyjournal.net/work1.htm
- Institute of Internal Auditors (IIA) Standard effective October 2010
- Global Technology Audit Guide, Managing and Auditing Privacy Risks
- Computer World – "Web site privacy seals: Are they worth it?" http://tinyurl.com/3nbyuz7
- http://www.webtrust.org/index.aspx
- Venturebeat – "Truste Gives the Seal-of-Approval to Mobile Privacy Policies" http://tinyurl.com/3wk9juc
- http://www.truste.com/pdf/TRUSTe_Mobile_FAQs.pdf
- TRUSTe Mobile Privacy Program Requirements - http://tinyurl.com/3k3azu9

Contact Information

Tammi Franke
Partner
Fitzgerald, Franke & Hewes LLP
53 West Jackson
Suite 838
Chicago, IL 60604
312-447-2903
tfranke@fitzhewlaw.com