Agenda

Privacy Review
› Definition
› Trends

Privacy Program Considerations

Privacy Risk Assessment
› Risk Assessment Tools
  • Generally Accepted Privacy Principles
  • AICPA Privacy Tools
  • Privacy Maturity Model
› Other Resources
No Single Definition...

“the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.”
What is Privacy?

Examples of Customer Data:
› Email addresses
› Customer name
› Social Security Number
› Address
› Telephone number
› Drivers license number
› Credit card number
› Credit data
› Bank account number
Examples of Employee Data:
› Ethnic & Gender Info
› Physical Address
› Social Security Number
› Salary & Position
› Health Information
› Phone Numbers
› Name
› Date of birth
› Retirement & Other financial data (e.g. bank account numbers for employee direct deposit)
Privacy Trends

- Regulators more proactive & aggressive
- Shift from consumer responsibility to organizational accountability
- Increasing collection & use of information—more than consumers know
- Customers more willing to provide personal information, expecting that corporations will be accountable for its safekeeping
- Sharing data with third parties is increasing
- Services can be outsourced but accountability cannot
Since 1998, over 200 laws in over 150 countries

Since Jan 1, 2003, over 75 new privacy laws in the U.S.

46 State Breach Notification Laws, plus U.S. territories

Three leading states:
- security (Massachusetts)
- privacy (California)
- security (Nevada)
Federal enforcements are on the rise:
› FTC: Stop Unfair and Deceptive Practices
› HHS-OCR: Audit Review of Technical, Physical, and Administrative Safeguards
› FCC: Telephone Consumers Protection Act (TCPA)
› CFPB: Dodd-Frank Act § 1033
› SEC: Guidance - Cybersecurity Risks and Cyber Incidents
Technology leads to changes in security

› Cloud technologies
› Mobile technology
› Social networking
› Online behavioral advertising
› Privacy by design
Privacy Program Considerations
Privacy Program Considerations

Challenges to Privacy Program Success

› An ineffective governance structure
› Lack of a strong culture and attitude at all levels
› Lack of resources committed to building and sustaining a privacy program
› Lack of a single global framework to address all rules and requirements
› Incomplete or partially completed Data Inventory
10 Keys to a Successful Program

- Effective governance structure
- Strong culture and attitude at all levels
- **Effective risk assessment process**
- Complete, dynamic, current lifecycle data inventory that includes third parties
- **Controls aligned with a selected framework**
- Effective training and awareness program
- Effective team that ensures compliance with laws and regulations
10 Keys to a Successful Program

- An effective auditing and monitoring function
- Current, communicated and followed policies and procedures
- Effective, documented and tested incident response plan

Designing, implementing, maintaining and monitoring a solid privacy and information security program requires effective support, resources, skills, time and discipline
Role for Internal Audit Function

Ongoing independent monitoring of a company’s privacy program could include:

› Completing a privacy and security gap assessment
› Evaluating the company’s periodic privacy risk assessment process
› Evaluating compliance with established privacy policies and procedures
› Evaluating data protection and privacy training and awareness programs
› Ensuring data protection and privacy-related remediation is in place
› Reviewing third party/vendor privacy practices
Privacy Risk Assessment Approach

1. **Scope Objectives**
   - Identify key data privacy objectives (principles and criteria) and define the scope.

2. **Assess and Test**
   - Assess and/or test the people, process and technology against the defined business objectives. Identify areas of improvement.

3. **Develop Assessment Report**
   - Document results of the assessment and testing to be used to support company’s privacy policies.
Generally Accepted Privacy Principles (GAPP)

› Developed from a business perspective

› Referenced significant privacy regulations

› Created single privacy objective
  • Supported by 10 privacy principles
  • Created objective, measurable criteria for each principle
Overall Privacy Objective

Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity’s privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA and CICA.
GAPP Framework

Privacy Principles
› Management
› Notice
› Choice and consent
› Collection
› Use, retention, and disposal
Privacy Principles (continued)

› Access
› Disclosure to third parties
› Security for privacy
› Quality
› Monitoring and enforcement
How does GAPP map to US regulations?

<table>
<thead>
<tr>
<th>Generally Accepted Privacy Principles</th>
<th>U.S. FTC</th>
<th>U.S. Safe Harbor</th>
<th>U.S. HIPAA</th>
<th>U.S. GLBA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td>Administrative requirements</td>
<td></td>
</tr>
<tr>
<td>Notice</td>
<td>Notice</td>
<td>Notice</td>
<td>Notice</td>
<td>Privacy and Opt Out Notices, Exceptions</td>
</tr>
<tr>
<td>Choice and Consent</td>
<td>Choice</td>
<td>Choice</td>
<td>Consent, Uses and Disclosures</td>
<td>Privacy and Opt Out Notices</td>
</tr>
<tr>
<td>Collection</td>
<td></td>
<td>Data Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use, Retention, and Disposal</td>
<td></td>
<td>(Implied but not specified in the principles)</td>
<td>Uses and Disclosures</td>
<td>Limits on Disclosures</td>
</tr>
<tr>
<td>Access</td>
<td>Access</td>
<td></td>
<td>Access</td>
<td></td>
</tr>
<tr>
<td>Disclosure to Third Parties</td>
<td></td>
<td>Onward Transfer</td>
<td>Uses and Disclosures, Accounting of Disclosures</td>
<td>Limits on Disclosures</td>
</tr>
<tr>
<td>Security for Privacy</td>
<td>Security</td>
<td>Security</td>
<td>Security Rule</td>
<td>Security Guidelines mandated by section 501(b) of GLBA</td>
</tr>
<tr>
<td>Quality</td>
<td>Integrity</td>
<td>Data Integrity</td>
<td>Amendment</td>
<td></td>
</tr>
<tr>
<td>Monitoring and Enforcement</td>
<td>Enforcement</td>
<td>Enforcement</td>
<td>Compliance and Enforcement by the Department of Health and Human Services</td>
<td>Enforcement by financial services industry regulators, the FTC, and SEC</td>
</tr>
</tbody>
</table>
# How does GAPP map to international regulations?

<table>
<thead>
<tr>
<th>Generally Accepted Privacy Principles</th>
<th>Australia Privacy Act</th>
<th>Canada PIPEDA</th>
<th>E.U. Directive</th>
<th>OECD Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Accountability</td>
<td>Notification</td>
<td>Accountability</td>
<td></td>
</tr>
<tr>
<td>Notice</td>
<td>Openness</td>
<td>Identifying Purposes, Openness</td>
<td>Purpose Specification, Openness</td>
<td></td>
</tr>
<tr>
<td>Choice and Consent</td>
<td>Use and Disclosure</td>
<td>Consent</td>
<td>Criteria for Making Data Processing Legitimate, Data Subject's Right to Object</td>
<td></td>
</tr>
<tr>
<td>Collection</td>
<td>Collection, Sensitive Information, Anonymity</td>
<td>Limiting Collection</td>
<td>Principles Relating to Data Quality, Exemptions and Restrictions</td>
<td></td>
</tr>
<tr>
<td>Use, Retention, and Disposal</td>
<td>Identifiers, Use and Disclosure</td>
<td>Limiting Use, Disclosure, and Retention</td>
<td>Making Data Processing Legitimate, Special Categories of Processing, Principles Relating to Data Quality, Exemptions and Restrictions, The Data Subject's Right to Object</td>
<td></td>
</tr>
<tr>
<td>Access</td>
<td>Access and Correction</td>
<td>Individual Access</td>
<td>The Data Subject's Right of Access to Data</td>
<td></td>
</tr>
<tr>
<td>Disclosure to Third Parties</td>
<td>Use and Disclosure, Transborder Data Flows</td>
<td>Limiting Use, Disclosure, and Retention</td>
<td>Transfer of Personal Data to Third Countries</td>
<td></td>
</tr>
<tr>
<td>Security for Privacy</td>
<td>Data Security</td>
<td>Safeguards</td>
<td>Confidentiality and Security of Processing</td>
<td></td>
</tr>
<tr>
<td>Quality</td>
<td>Data Quality</td>
<td>Accuracy</td>
<td>Principles Relating to Data Quality</td>
<td></td>
</tr>
<tr>
<td>Monitoring and Enforcement</td>
<td>Enforcement by the Office of the Privacy Commissioner</td>
<td>Challenging Compliance</td>
<td>Judicial Remedies, Liability and Sanctions, Codes of Conduct, Supervisory Authority and Working Party on the Protection of Individuals with Regard to the Processing of Personal Data</td>
<td></td>
</tr>
</tbody>
</table>

@PerkinsCo
Based on GAPP

› Scores risk for 73 GAPP criteria based on
  • Likelihood of control failure
  • Business impact
  • Effort/cost to mitigate

› Not intended as a “plug-and-play” tool

› Requires understanding of
  • Entity’s privacy programs and initiatives
  • Privacy environment in which entity operates
  • Legislative, regulatory, industry, jurisdictional privacy requirements
<table>
<thead>
<tr>
<th>GAPP - 73 Criteria</th>
<th>Criteria Description</th>
<th>Likelihood of a Control Failure</th>
<th>Business Impact</th>
<th>Effort/Cost to Mitigate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 MANAGEMENT</td>
<td>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(14 criteria)</td>
<td>Privacy Policies (1.1.0) Policies are defined for: notice, choice/consent, collection, use/retention/disposal, access, disclosure, security, quality, and monitoring/enforcement.</td>
<td>2</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Communications to Internal Personnel (1.1.1) 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.</td>
<td>2</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Responsibility and Accountability for Policies (1.1.2) Responsibility and accountability are assigned to a person or group for developing, 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.</td>
<td>2</td>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>
### Sample Criteria Summary

Scoring: 2=Low Risk, 5=Medium Risk, 8=High Risk

<table>
<thead>
<tr>
<th>1.0 Management</th>
<th>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</th>
<th>Likelyhood of a Control Failure</th>
<th>Business Impact</th>
<th>Effort/Cost to Mitigate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>14 Criteria</strong></td>
<td><strong>Average Score - 14 Criteria</strong></td>
<td>4.4</td>
<td>5.1</td>
<td>3.9</td>
</tr>
<tr>
<td>Privacy Policies (1.1.0)</td>
<td>Policies are defined for: notice, choice/consent, collection, use/retention/ disposal, access, disclosure, security, quality, and monitoring/enforcement.</td>
<td>2</td>
<td>8</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Input 1</th>
<th>Input 2</th>
<th>Input 3</th>
<th>Input 4</th>
<th>Input 5</th>
<th>Input 6</th>
<th>Input 7</th>
<th>Input 8</th>
<th>Input 9</th>
<th>Input 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Average Score**

| 2.0 | 5.0 | 3.5 |
## Summary of Results

<table>
<thead>
<tr>
<th>GAPP - 10 Principles</th>
<th>Likelihood of a Control Failure</th>
<th>Business Impact</th>
<th>Size of Marker</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MANAGEMENT</strong></td>
<td>4.4</td>
<td>5.1</td>
<td>3.9</td>
</tr>
<tr>
<td>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NOTICE</strong></td>
<td>3.2</td>
<td>3.2</td>
<td>2.0</td>
</tr>
<tr>
<td>The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CHOICE / CONSENT</strong></td>
<td>6.7</td>
<td>7.1</td>
<td>5.0</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sample Heat Map

- Actively Manage Remediation Plans
- Requires Immediate Attention, Senior Mgmt Focus
- Fix at Mgmt Discretion, Bear Risk
- Plan to Remediate, Business Contingency Plans

- Choice / Consent
- Management
- Notice
Based on GAPP

› AICPA/CICA Privacy Task Force
  • Input from ISACA

› Requires understanding of GAPP and entity-specific privacy requirements

› Designed for organizations that have existing privacy program

› Useful for measuring progress against initial maturity (baseline) and desired maturity (goal)
Follows Capability Maturity Model (CMM)

- Five Maturity Levels
  1. Ad hoc
  2. Repeatable
  3. Defined
  4. Managed
  5. Optimized

- Recognizes not all privacy initiatives need to reach highest level of maturity

- Facilitates measurement of progress over time and identification of next steps for continuous improvement
Privacy Maturity Model

To be effective, PMM must consider:

› Maturity of the entity’s privacy program
› Ability to obtain complete and accurate information on the entity’s privacy initiatives
› Agreement on the Privacy Maturity assessment criteria
› Level of understanding of GAPP and the PMM
## Sample PMM Criteria Maturity

<table>
<thead>
<tr>
<th>GAPP – 73 Criteria</th>
<th>Criteria Description</th>
<th>Maturity Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ad HOC</td>
</tr>
<tr>
<td>Management</td>
<td>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.</td>
<td></td>
</tr>
<tr>
<td>Privacy Policies</td>
<td>The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.</td>
<td></td>
</tr>
<tr>
<td>(1.1.0)</td>
<td>Some aspects of privacy policies exist informally.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privacy policies exist but may not be complete and are not fully documented.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policies are defined for: notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compliance with privacy policies are monitored and the results of such monitoring are used to reinforce key privacy messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management monitors compliance with policies and procedures concerning information. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely manner.</td>
<td></td>
</tr>
</tbody>
</table>
Sample PMM Report

Maturity Reporting by Principle

<table>
<thead>
<tr>
<th>Principle</th>
<th>Maturity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>3</td>
</tr>
<tr>
<td>Notice</td>
<td>4</td>
</tr>
<tr>
<td>Choice &amp; Consent</td>
<td>2</td>
</tr>
<tr>
<td>Collection</td>
<td>3</td>
</tr>
<tr>
<td>Use, Retention &amp; Disposal</td>
<td>2</td>
</tr>
<tr>
<td>Access</td>
<td>1</td>
</tr>
<tr>
<td>Disclosure to 3rd Parties</td>
<td>4</td>
</tr>
<tr>
<td>Security for Privacy</td>
<td>5</td>
</tr>
<tr>
<td>Quality</td>
<td>4</td>
</tr>
<tr>
<td>Monitoring &amp; Enforcement</td>
<td>2</td>
</tr>
</tbody>
</table>

Entity’s Desired Maturity Level: 4
**Other Resources**

**AICPA**
http://www.aicpa.org/INTERESTAREAS/INFORMATION/TECHNOLOGY/RESOURCES/PRIVACY/Pages/default.aspx

**IAPP** https://www.privacyassociation.org/

**FTC** http://business.ftc.gov/privacy-and-security

**ISACA**
http://www.isaca.org/Groups/Professional-English/privacy-data-protection/Pages/Overview.aspx
Privacy laws and risks will continue to evolve
Privacy programs can be effective at reducing risks
A privacy risk assessment can identify risks and facilitate mitigation
Numerous resources are available to support the practitioner in performing a privacy risk assessment