The Evolution of Privacy Risks

Prepared For IIA San Diego Chapter

September 7, 2016
Introduction

Eric Dieterich
Partner, National Privacy Practice
Sunera LLC
edieterich@sunera.com
786.390.1490
Sunera – A leading provider of risk-based consulting services

- Founded in 2005 by a small group of founding members, Sunera has grown to nearly 400 full-time employees across 16 locations within the U.S. and Canada.
- We have delivered more than 3,000 projects to over 700 clients.
- The large majority of our growth has been through referrals and reoccurring projects at existing clients.
- Entrepreneurial environment promotes growth and innovation from our team members.
- Team members have diverse backgrounds and skill sets.
- Highly credentialed professionals, including CISA, CISSP, CIPP, CISM, CRISC, CBCP & PMP.
- Dedicated national teams for Privacy and Information Security.
- Provide a wide range of risk and compliance consulting services with experiences relating to HIPAA, GLBA, GAPP, Cross Boarder Data Transfers, ISO 27001/27002, NIST 800-53 v4, PCI, FedRamp, and others.
Agenda

• The Evolving Privacy Landscape
  • Privacy Risks
  • Enforcement Actions
  • Regulatory Landscape

• Internal Audit’s Role
  • Areas of Focus
  • Information Mapping of Sensitive Information
  • Privacy Risk Assessments
  • Privacy Audits

• Privacy Communication Challenges and Solutions
The Evolving Privacy Landscape
Privacy Risks

Biometric Security Poses Huge Privacy Risks

Without explicit safeguards, your personal biometric data are destined for a government database

FDA issues guidance on medical device cybersecurity and interoperable medical devices

How drones raised privacy concerns across cyberspace

How GM warns Corvette drivers new valet mode may be illegal

How Hackers Violate Privacy and Security of the Smart Home
Enforcement Actions

TECHNOLOGY

Snapchat Settles FTC Charges
Mobile Messaging App Developer Will Face Privacy Monitoring for 20 Years

According to the FTC, Snapchat promised users that messages, photos and video sent through the app would self-destruct and disappear in 10 seconds or less. In fact, the commission said, recipients and outsiders could continue to access the messages. The FTC also said Snapchat told users it didn't collect information about their location when the Android version of the app did.

FTC Brings First Privacy Enforcement Action Against a Mobile Ad Network

June 27, 2016

On June 22, 2016, the Federal Trade Commission (FTC) announced that it has settled charges that InMobi, a Singapore-based mobile advertising company, deceptively tracked the locations of hundreds of millions of consumers, including children, to deliver geo-targeted advertising, and violated both the FTC Act and the Children's Online Privacy Protection Act (COPPA). This is the FTC's first enforcement action against a mobile advertising network. The FTC alleges that, in instances when consumers had set their device settings to deny access to location information, InMobi inferred consumers' locations based on the WiFi networks near their devices and served them geo-targeted ads. As part of the settlement, InMobi has agreed to implement a comprehensive privacy program, to collect or infer location information only after obtaining consumers' affirmative express consent, and only in a manner consistent with consumers' device location settings, and to pay a civil penalty of $950,000 to resolve the alleged COPPA violations.
Enforcement Actions

The Risks of TCPA-Related Class-Action Lawsuits Are Rising

February 2015 – Capital One paid $75 million in settlement, the largest TCPA settlement to date.

January 2016 – Life Time Fitness paid $15 million for sending text messages to customers without prior express written consent.

February 2016 – Facebook Inc. faces a suit for sending users unsolicited, automated text messages to remind users of their friends’ birthdays. Facebook is seeking dismissal of the case.

May 2016 – Caribou Coffee is hit with an accusation of sending unsolicited texts.
The TCPA is designed to protect consumer privacy by regulating automated telemarketing and informational calls and text messages, including the use of autodialers, pre-recorded voice messages, and unsolicited faxes.

- It was created and is controlled by the Federal Communications Commission (FCC).
- The National Do-Not-Call List stems from this regulation.
Increasing number and size of class action lawsuits (e.g., TCPA, Security Events).

U.S. privacy landscape continues to be industry and state specific.

Major regulatory changes in Europe with the passage of GDPR.

U.S. Safe Harbor Framework disbanded, replaced with Privacy Shield.

Increased enforcement and oversight from various regulatory bodies including OCR, FTC and State Attorney Generals.
What Does This All Mean?

- Know your privacy risks, build your risk universe.
- Consider industry specific trends.
- Consider areas that are often overlooked (e.g., marketing, HR, mobile apps).
- Think beyond specific regulatory requirements.
Managing Privacy Risks – Internal Audit’s Roles
In response to growing privacy risks, Internal Audit departments have begun performing the following:

1. Establishing programs to ensure accurate information mappings of sensitive information throughout the organization.
2. Increasing the frequency and/or scope of organizational privacy risk assessments.
3. Conducting audits focused on key privacy risks.
4. Performing recurring, security and privacy specific gap assessments to benchmark operations against relevant standards.
5. Performing Privacy Impact Assessments (PIA’s).
6. Active participation in the incident management and breach response programs.
(1) Information Mapping of Sensitive Information

Defining
– Establish a framework for defining how sensitive information is collected, processed, stored, and shared throughout the organization.

Importance
– Enables the implementation of policies, procedures, and controls to help reduce the associated privacy risks.

Strategy
– Understanding of how and where information flows through business processes.
– A framework can then be established to ensure sensitive information is protected throughout the life cycle.
Goals

• Understand the information life cycle of sensitive information for key processes throughout the business.

• Evaluate strength and effectiveness of controls and safeguards, focused on privacy and security.

• Create a repository of information life cycle details including data element types, collection mechanisms, transfers, privacy and security practices, and transfers to third parties.

• Establish a risk threshold so audit activities can focus on areas with the greatest privacy and security risks.
(2) Privacy Risk Assessment

Key Privacy Risk Assessment Activities

1. Creation of a risk catalog for the key business processes.
2. An overall inherit risk profile is calculated for each key process.
3. The identification and evaluation of mitigation techniques are evaluated leveraging a catalog of illustrative controls.
4. An overall residual risk score for each key process is calculated helping to identify areas of privacy risk across the enterprise.
5. The results can drive the definition of a roadmap to mitigate the privacy risks.
Process Based Analysis

– Each area of privacy risk is analyzed by business unit, process and/or sub-process.

<table>
<thead>
<tr>
<th>Elec. PII Risk Process No.</th>
<th>Business Unit</th>
<th>Process</th>
<th>Process Description</th>
<th>PII Data Elements</th>
<th>Inquiry</th>
<th>Vendor</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Human Resources</td>
<td>New Applicant</td>
<td>Each applicant submits contact detail with work history, criminal history (voluntary) and a copy of a resume. A skills assessment, if required, is completed on the Connect Approver site, Profile XT Assessment and is only used for senior level positions. Only the name and mailing address of the applicant are sent back to the applicant. No PII is sent to the applicant prior to the interview, only informational brochures.</td>
<td>Applicant Information</td>
<td>John Smith</td>
<td>Success Factors</td>
<td>PictureSaver</td>
</tr>
</tbody>
</table>
(2) Privacy Risk Assessment – Defining the Risk Criteria

Four key “buckets” of risk criteria:

1. Electronic Privacy Risks
2. Application Privacy Risks
3. Vendor Privacy Risks
4. Paper File Privacy Risks

The risk criteria buckets can be added or changed depending on the industry or focus of the risk assessment.
# Privacy Risk Assessment – Defining the Risk Criteria

## Electronic Privacy Risks

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Factor</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-01</td>
<td>Inappropriate notice provided during collection of PII</td>
<td>A person is not informed or misinformed about the intended use or purpose of PII collected which may lead to non-compliance with stated policies or regulatory standards.</td>
</tr>
<tr>
<td>R-02</td>
<td>Over collection of PII</td>
<td>The PII collected is not required for the intended business activity which increases the exposure during a breach.</td>
</tr>
<tr>
<td>R-03</td>
<td>Inappropriate use of PII</td>
<td>The misuse of PII other than for the purpose stated during collection maybe lead to non-compliance with stated policies or regulatory standards.</td>
</tr>
<tr>
<td>R-04</td>
<td>Inaccurate PII</td>
<td>The PII collected is not accurate, complete or relevant which may lead to inappropriate business actions.</td>
</tr>
</tbody>
</table>
(2) Privacy Risk Assessment – Evaluating Inherent Risks

- For each department, process or sub-process, the inherent risks need to be evaluated.
- The risk criteria should be defined specific for your organization, ensuring the criteria address all relevant data privacy risks including both paper and electronic.
- The sample below identifies how the inherent risk could be scored for each risk and unique vendor or application specific risks.

<table>
<thead>
<tr>
<th>Type of NPI (Multiplier)</th>
<th>Pervasive (Additive)</th>
<th>Vulnerability (Additive)</th>
<th>Inherent Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
<td>5</td>
<td>R-01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R-02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R-03</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R-04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R-05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R-06</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R-07</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R-08</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R-09</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vendor Risks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Application Risks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Overall Inherent Risk Score</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R-01</th>
<th>R-02</th>
<th>R-03</th>
<th>R-04</th>
<th>R-05</th>
<th>R-06</th>
<th>R-07</th>
<th>R-08</th>
<th>R-09</th>
<th>R-10</th>
<th>Vendor Risks</th>
<th>Application Risks</th>
<th>Overall Inherent Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>5</td>
<td>-</td>
<td>9.3</td>
</tr>
</tbody>
</table>
(2) Privacy Risk Assessment – Evaluate Risk Mitigation Techniques

- A risk mitigation score can be assigned including the ability to assign different scores based on the level of certainty that the risk mitigation technique is operating effectively.
- The sample below shows how a risk mitigation technique may be used to lower the inherent risk for each privacy risk factor.
(2) Privacy Risk Assessment – Evaluate Residual Risk

- Taking into account the inherent risk ranking and risk mitigation techniques, an overall residual risk score can be calculated.
- The sample below identifies how the overall privacy risk score can be calculated.
- The overall residual risk score is a key factor in defining a roadmap that can help lower the privacy risks identified throughout the enterprise.

<table>
<thead>
<tr>
<th></th>
<th>Residual Risk</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th>Vendor Risks</th>
<th>Application Risks</th>
<th>Average Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-01</td>
<td>-</td>
<td>R-02</td>
<td>2</td>
<td>R-03</td>
<td>2</td>
<td>R-04</td>
<td>2</td>
<td>R-05</td>
<td>2</td>
<td>R-06</td>
<td>-</td>
<td>R-07</td>
</tr>
</tbody>
</table>

- 2 2 2 - - - - 2 - - 5.0
(3) Privacy Audits

Objective
• To review and assess the privacy risks associated with key processes that collect, process, store and transfer sensitive information.
• Many possible areas of focus for a privacy audit.

Key Areas of Focus
• Identification and evaluation of privacy risks associated with the processes for which sensitive information is collected (e.g., inbound);
• Evaluation of security for privacy controls (e.g., logical access, authentication mechanisms, remote access, audit logging) for processes involving sensitive information; and
• Identification and evaluation of privacy risks associated with processes for which sensitive information is transferred out of the organization (e.g., outbound).
(3) Privacy Audits

Common Test Procedures

• Privacy audit activities often include an evaluation of the key operations and supporting technology for which sensitive information is involved.

• Some test procedures may include:
  1. Evaluation of the governance structure for the privacy program.
  2. Identification of key privacy risk indicators;
  3. Review of privacy policies and procedures;
  4. Evaluation on the level of Integration between privacy practices and the information security program;
  5. Review of the privacy training program and content delivered to employees; and
  6. Review the privacy components of the vendor management process.
Privacy Challenges & Solutions
Common Challenges Relating to Privacy

• Often a shared responsibilities for privacy and security across the enterprise, no single point.
• Balancing the level of detail that is communicated.
• Limited technical and subject matter expertise.
• Limited time allocated for communicating privacy and security risks to c-suite, audit committees, boards, etc.
Overcoming These Challenges

• Obtain consensus on what is most important to protect within the organization (e.g., employee info, trade secrets, customer data, financials).

• Design a process to classify or score privacy and security risks for strategic projects and planned initiatives prior to execution.

• Communicate the effectiveness of privacy and security programs on a periodic basis (e.g., quarterly).

• Increase awareness to help drive a culture that is directed by the “tone-at-the-top”.

• Allocate as much time as possible to discuss current privacy and security risk mitigation strategy with leadership:
  • Risk factors applicable to our business
  • Risk mitigation/controls
  • Industry and enforcement trends
Questions?

Eric Dieterich
Partner, National Data Privacy Practice
edieterich@sunera.com
786.390.1490