Privacy, Security, and Compliance: Strange Bedfellows or a Marriage Made in Heaven?

Jane Rosenthal (KU) and Michael Corn (UIUC)
Outline
• Privacy & Compliance Function
• Privacy & Security in Conflict
• Privacy within Organizational Ecosystem

Ben Rosenthal & Louis Pitluck, circa 1940
Privacy and Compliance

- Federal Legislation
  - HIPAA/HITECH
  - FERPA
  - GLBA
  - COPPA
  - FACTA (Red flags)
  - FCRA
  - Privacy Act (etc....)
Privacy and Compliance

• Most states & territories now have (what passes as) privacy legislation
  – Illinois:
    • Illinois Identity Protection Act (IIPA)
    • Personal Information Protection Act (PIPA)
    • Employer access to social media passwords
  – Kansas:
    • Protection of Consumer Information
      – Name + SSN /DL # + financial information
  – Exceptions:
    • SD, KY, NM, AL
Where privacy offices are placed

- Legal
- Compliance
- Information Security
- It is its own function reporting directly to the top executive
- Risk Management
- Information Technology

2011
2012
How is the privacy office function shaped by where it is placed?
<table>
<thead>
<tr>
<th>Areas</th>
<th>Privacy (Why)</th>
<th>Security (How)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability</td>
<td>Track PII disclosure trail; data controller <strong>responsible for complying with measures</strong> give effect to the other principles</td>
<td>Track individual’s actions &amp; handling of information</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Dictates derivation of new PII not allowed <strong>IF new information is not authorized by law nor necessary for stated purpose</strong></td>
<td>Determine the sensitivity of device &amp; aggregated data in order to provide access guidance</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Ensure PII <strong>only disclosed for purpose consistent with reason it was collected</strong></td>
<td>Process &amp; mechanism focus (e.g. authenticators) that prevent unauthorized access</td>
</tr>
<tr>
<td>Destruction</td>
<td>Address need for elimination of collected information, once the purpose is met</td>
<td>Ensure information cannot be recovered once deleted/wiped/destroyed</td>
</tr>
<tr>
<td>Integrity</td>
<td>Ensure inaccurate PII not used to make inappropriate decision about a person</td>
<td>Protect against data corruptions by authorized or unauthorized individuals</td>
</tr>
</tbody>
</table>
Security and Privacy in Conflict?

Three Use Cases

– Web & IP tracking
– MDM technologies
– Security/Video Camera
# Web, IP tracking, and Privacy

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.17.25.231</td>
<td>72.32.147.161</td>
<td>128.174.45.5 (128.174.45.5) : NETFLOW MAPPED: 128</td>
<td>128.174.45.5 TCF</td>
<td></td>
</tr>
<tr>
<td>192.17.25.231</td>
<td>72.32.147.161</td>
<td>128.174.45.5 (128.174.45.5) : NETFLOW MAPPED: 128</td>
<td>128.174.45.5 TCF</td>
<td></td>
</tr>
<tr>
<td>192.17.25.231</td>
<td>69.174.80.128</td>
<td>128.174.45.5 (128.174.45.5) : NETFLOW MAPPED: 128</td>
<td>128.174.45.5 TCF</td>
<td></td>
</tr>
<tr>
<td>192.17.25.231</td>
<td>69.174.80.128</td>
<td>128.174.45.5 (128.174.45.5) : NETFLOW MAPPED: 128</td>
<td>128.174.45.5 TCF</td>
<td></td>
</tr>
<tr>
<td>192.17.25.231</td>
<td>69.46.228.167</td>
<td>128.174.45.5 (128.174.45.5) : NETFLOW MAPPED: 128</td>
<td>128.174.45.5 TCF</td>
<td></td>
</tr>
<tr>
<td>192.17.25.231</td>
<td>69.46.228.167</td>
<td>128.174.45.5 (128.174.45.5) : NETFLOW MAPPED: 128</td>
<td>128.174.45.5 TCF</td>
<td></td>
</tr>
<tr>
<td>192.17.25.231</td>
<td>69.46.228.167</td>
<td>128.174.45.5 (128.174.45.5) : NETFLOW MAPPED: 128</td>
<td>128.174.45.5 TCF</td>
<td></td>
</tr>
<tr>
<td>192.17.25.231</td>
<td>69.46.228.167</td>
<td>128.174.45.5 (128.174.45.5) : NETFLOW MAPPED: 128</td>
<td>128.174.45.5 TCF</td>
<td></td>
</tr>
<tr>
<td>192.17.25.231</td>
<td>207.123.152.36</td>
<td>128.174.45.5 (128.174.45.5) : NETFLOW MAPPED: 128</td>
<td>128.174.45.5 TCF</td>
<td></td>
</tr>
<tr>
<td>192.17.25.231</td>
<td>207.123.152.36</td>
<td>128.174.45.5 (128.174.45.5) : NETFLOW MAPPED: 128</td>
<td>128.174.45.5 TCF</td>
<td></td>
</tr>
</tbody>
</table>
Mobile Device Management
MDM / EPM /App Development

• Excerpt from proposed mobile application terms of services/privacy statement

*We do not use or collect your precise geographic location.*

**OR**

*To provide location-based services, we may collect, use, and share precise location data, including the real-time geographic location of your computer or device. You will be asked for your permission before your first use of a location-based service.*

• E911 Services (need location information)

• Misc. features of MDM
  – Apps installed
  – Website browsed
  – Basic activity: logged in, checking email, calendar notifications
  – Location: during working hours, vacation/sick leave, class time

Protocol + Transparency = Trust
Security Cameras/Surveillance Tech

TRESPASSING

THIS PROPERTY IS PROTECTED BY VIDEO CAMERAS AND ATTACK DOGS

TRESPASSERS WILL BE PROSECUTED
Protocol + Transparency = Respect

- All locations with security cameras will have signs displayed that provide reasonable notification of the presence of security cameras.
- Security cameras may not be used in private areas, which include residence hall rooms, bathrooms, shower areas, locker and changing rooms, areas where a reasonable person might change clothes, and private offices. Additionally rooms for medical, physical, or mental therapy or treatment are private. Where security cameras are permitted in private areas, they will to the maximum extent possible be used narrowly to protect money, real or personal property, documents, supplies, equipment, or pharmaceuticals from theft, destruction, or tampering.
- Security camera recordings may not be used in the course of personnel investigations such as those related to (but not limited to) workplace attendance or work quality.
Privacy in your Ecosystem

• Does it make sense for endless varieties of compliance challenges to be housed together?
• How does the U avoid silos if they’re not housed or reporting together?
• Can institutions afford not to separate & mature compliance, security, & privacy functions?
• Will each area have access to senior decision makers about risk?
Illinois & Kansas

• Kansas
  – Privacy in compliance office environment
  – Answers through Academic Vice Provost
  – Security through CIO

• Illinois
  – Security & Privacy together in IT
  – Access to upper tiers as needed
Privacy != Compliance

• Privacy = expression of RESPECT for our communities
• We express this respect by adhering to basic principles of fair information handling (Fair Information Practice Principles)
Basic Principles of FIPP

- Collection Limitation
- Notice
- Choice/Opt-Out
- Security
- Accountability
T176: Apply principles of privacy when handling personal information

Requirements

T179: Allow access for users to remove their data from the system
T178: Ask for consent from user prior to collecting personal information
T177: Allow users to review and update their personal data

Testing

T240: Test that users can remove their data from the system
T239: Test that users must provide consent prior to collection of personal information
T238: Test that users can review and update their personal data
Comments or Questions

– Jane Rosenthal jer@ku.edu
– Michael Corn mcorn@illinois.edu