ENGINEERING ETHICS INTO THE NIST PRIVACY FRAMEWORK

R. Jason Cronk
PEPR' 20
R. Jason Cronk
Privacy Engineer
Enterprivacy Consulting Group

Author, *Strategic Privacy by Design*
Licensed Attorney in Florida,
PbD Ambassador,
IAPP FIP, CIPP/US, CIPT, CIPM
NIST introduces Privacy Framework V1.0
Feb 2014

NIST introduces Cybersecurity Framework V1.0
V1.1 Apr 2018

Profiles

Tiers

Core

NIST PRIVACY FRAMEWORK

Identify

Asset Management

Business Environment

ID.BE-3 Priorities for organizational mission, objectives, and activities are established and communicated.
“Priorities for organizational mission, objectives, and activities are established and communicated.”

“Physical access to assets is managed and protected.”

“Physical access to data and devices is managed.”

“Privacy values, policies, and training are reviewed and any updates are communicated.”

“Privacy values, policies, and training are reviewed and any updates are communicated.”
PR.AC-P2 Physical access to data and devices is managed.

- Security guards at building entrances
- Exterior doors are locked and alarmed
- USB ports disabled
- All servers in locked cages
PR.AC - Physical access to data and devices is managed.

Security guards at building entrances
Exterior doors are locked and alarmed
USB ports disabled
All servers in locked cages

PROFILES

WHY?

“Profiles enable the prioritization of the outcomes and activities that best meet organizational privacy values, mission or business needs, and risks.”
Malum in se – evil/wrong in itself (i.e. murder)

Malum prohibitum – wrong because a statute/law/regulation says so (i.e. prohibition on exceeding 55mph)

PRIVACY AS SOCIAL NORMS
MODELS OF PRIVACY NORMS

**Hartzog's Privacy Pillars**
- Obscurity
- Autonomy
- Trust

**WESTIN's States of Privacy**
- Anonymity
- Intimacy
- Seclusion
- Solitude

**Prosser's Privacy Torts**
- False Light
- Intrusion Upon Seclusion
- Public Disclosure
- Appropriation

**Calo's Harms**
- Objective
- Subjective
MODELS OF PRIVACY NORMS

INFORMATION PROCESSING
- Aggregation
- Identification
- Secondary Use
- Exclusion
- Insecurity

INFORMATION DISSEMINATION
- Breach of Confidentiality
- Disclosure
- Exposure
- Increased Accessibility
- Blackmail
- Appropriation
- Distortion

INVASION
- Intrusion
- Decisional Interference

COLLECTION
- Surveillance
- Interrogation

PROF. DAN SOLOVE
USING NORMS IN NIST PRIVACY FRAMEWORK
<table>
<thead>
<tr>
<th>Hartzog</th>
<th>Westin</th>
<th>Prosser</th>
<th>Calo</th>
<th>Solove</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pillars of Privacy</td>
<td>States of Privacy</td>
<td>Common Law Privacy Torts</td>
<td>Subjective and Objective Harms</td>
<td>Taxonomy of Privacy</td>
</tr>
<tr>
<td><strong>Trust</strong>-willingness to become vulnerable to the actions of another</td>
<td><strong>Intimacy</strong> is a &quot;close, relaxed, and frank relationship between two or more individuals&quot; that results from the seclusion of a pair or small group of individuals.</td>
<td><strong>Objective</strong> Unanticipated or coerced use of information</td>
<td><strong>INFORMATION DISSEMINATION Breach of Confidentiality</strong> breaking a promise to keep a person's information confidential</td>
<td></td>
</tr>
<tr>
<td><strong>INFORMATION PROCESSING Secondary Use</strong> information collected for one purpose is used for another purpose</td>
<td><strong>INFORMATION PROCESSING Insecurity</strong> carelessness in protecting information from leaks or improper access</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## ORGANIZATION SPECIFIC VALUES

<table>
<thead>
<tr>
<th>Hartzog</th>
<th>Westin</th>
<th>Calo</th>
<th>Solove</th>
<th>Text-a-Cleric privacy value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obscurity, Trust, Autonomy</td>
<td>Solitude, Intimacy, Anonymity, Reserve</td>
<td>Subjective and Objective Harms</td>
<td>Information Dissemination, Information Processing, Collection, Invasion</td>
<td>Seal of Confession—Text-a-cleric will protect and not use or reveal any information divulged.</td>
</tr>
<tr>
<td>Trust—willingness to become vulnerable to the actions of another</td>
<td>Intimacy is a &quot;close, relaxed, and frank relationship between two or more individuals&quot; that results from the seclusion of a pair or small group of individuals.</td>
<td>Objective Unanticipated or coerced use of information</td>
<td>INFORMATION DISSEMINATION Breach of Confidentiality breaking a promise to keep a person's information confidential</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>INFORMATION PROCESSING Secondary Use information collected for one purpose is used for another purpose</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>INFORMATION PROCESSING Insecurity carelessness in protecting information from leaks or improper access</td>
<td></td>
</tr>
</tbody>
</table>
**USING NORMS IN NIST PRIVACY FRAMEWORK**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ID.IM-P4:</strong> Data actions of the systems/products/services are inventoried.</td>
<td>All touch-points for confessional message data are kept in a system architecture diagram.</td>
<td></td>
</tr>
<tr>
<td><strong>GV.PP-P3:</strong> Roles and responsibilities for the workforce are established with respect to privacy.</td>
<td>Organization has both a CISO and CPO with job responsibilities for security and privacy, respectively.</td>
<td></td>
</tr>
<tr>
<td><strong>CT.DM-P8:</strong> Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.</td>
<td>Access to confessional message data is controlled and access is logged and reviewed monthly for anomalies.</td>
<td></td>
</tr>
<tr>
<td><strong>CM.AW-P1:</strong> Mechanisms for communicating data processing purposes .... are established and in place.</td>
<td>Clerics are notified when entering chat that they may not use or divulge information obtained.</td>
<td></td>
</tr>
<tr>
<td><strong>PR.DS-P2:</strong> Data-in-transit are protected.</td>
<td>Data between the parishioner’s App and our systems are encrypted.</td>
<td></td>
</tr>
</tbody>
</table>
RESOURCES

- NIST Privacy Framework v1.0
- Models of Privacy Norms Infographic
- Deriving and Using Synthetic Consequences For Privacy
  - For a more formal, rigorous methodology of combining privacy norms

rjc@enterprivacy.com
@privacymaverick on Twitter