# Recommended Practice for Privacy Considerations for IEEE 802 Technologies

Date: 2016-01-18

***Authors:***

| *Name* | *Affiliation* | *Phone* | *Email* |
|---|---|---|---|
| Jerome Henry | Cisco Systems | +1 919 392 2503 | jerhenry@cisco.com |
| | | | |
| | | | |

***Notice:***
This document does not represent the agreed view of the IEEE 802.1 TG. It represents only the views of the participants listed in the 'Authors:' field above. It is offered as a basis for discussion. It is not binding on the contributor, who reserve the right to add, amend or withdraw material contained herein.

***Patent policy:***
The contributor is familiar with the IEEE-SA Patent Policy and Procedures:
<http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>.

## Abstract

The slide set provides some very initial thoughts about how privacy aspects may be approached in the 802E specification.

# References

- The Privacy Engineer’s Manifesto - Getting from Policy to Code to QA to Value (Michelle Finneran Dennedy Jonathan Fox Thomas R. Finneran; ApressOpen)
  - http://www.apress.com/9781430263555

- Privacy Engineering Framework (MITRE Privacy Community of Practice (CoP) July 18, 2014)
  - http://www.mitre.org/publications/technical-papers/privacy-engineering-framework

- Engineering Privacy (Sarah Spiekermann, Lorrie Faith Cranor; IEEE Transactions on Software Engineering, Vol. 35, No. 1, Jan/Feb 2009)
  - http://ssrn.com/abstract=1085333
- OmniRAN Privacy Engineered Access network presentation, Max Riegel (Nokia)
  - https://mentor.ieee.org/omniran/dcn/15/omniran-15-0015-00-CF00-privacy-engineered-access-network.pptx

# Privacy
# Some common definitions:

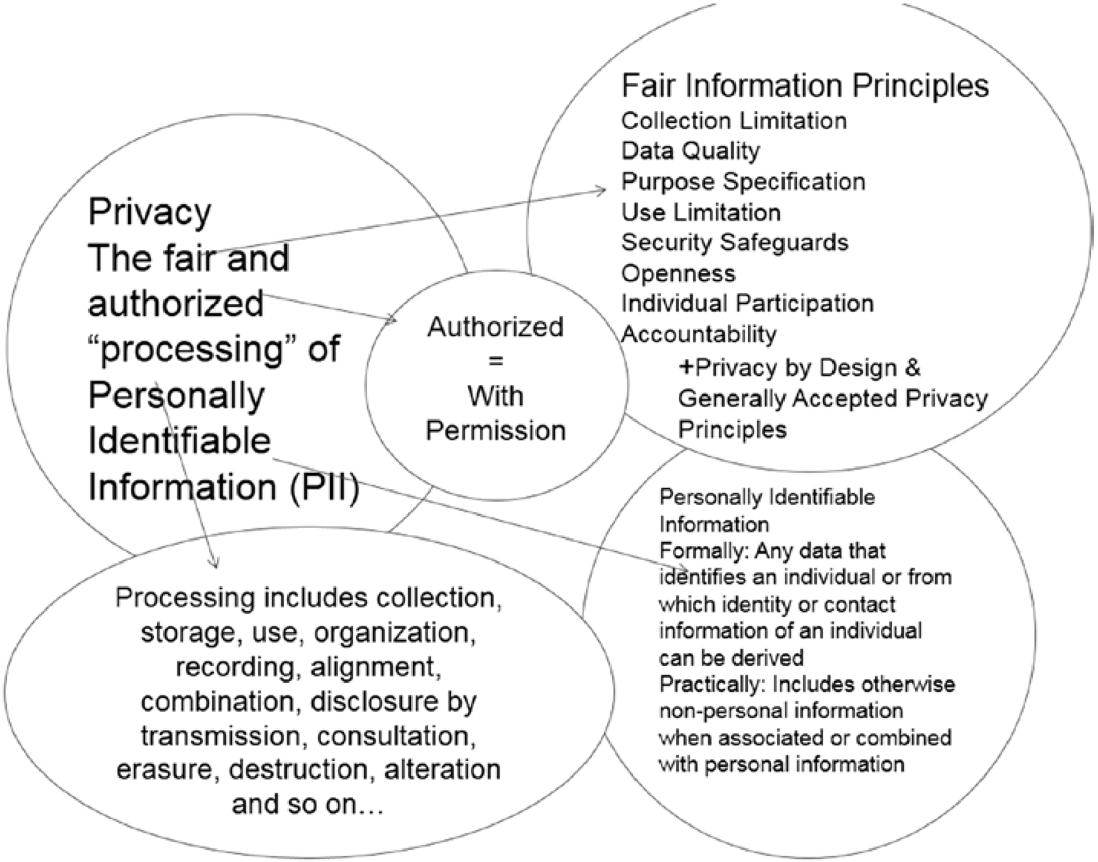
- Merriam-Webster’s Dictionary:
  - 1a: the quality or state of being apart from company or observation: seclusion
    1b: freedom from unauthorized intrusion one’s right to privacy
  - 2. archaic: a place of seclusion
  - 3a: secrecy
    3b: a private matter: secret

- According to Yael Onn et al., Privacy in the Digital Environment. Haifa Center of Law & Technology, 2005:

  *“The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets, and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner, and timing of the use of those parts we choose to disclose.”*

# Privacy

## *a targeted definition*



Privacy
The fair and authorized "processing" of Personally Identifiable Information (PII)

Authorized
=
With Permission

Fair Information Principles
Collection Limitation
Data Quality
Purpose Specification
Use Limitation
Security Safeguards
Openness
Individual Participation
Accountability
+Privacy by Design & Generally Accepted Privacy Principles

Processing includes collection, storage, use, organization, recording, alignment, combination, disclosure by transmission, consultation, erasure, destruction, alteration and so on…

Personally Identifiable Information
Formally: Any data that identifies an individual or from which identity or contact information of an individual can be derived
Practically: Includes otherwise non-personal information when associated or combined with personal information

**Taken from:** The Privacy Engineer's Manifesto - Getting from Policy to Code to QA to Value (Michelle Finneran Dennedy Jonathan Fox Thomas R. Finneran; ApressOpen)

# PII
# Personally Identifiable Information

- Privacy:

  “The fair and authorized “processing” of Personally Identifiable Information (PII)

- Personally Identifiable Information

  Formally: Any data that identifies an individual or from which identity or contact information of an individual can be derived

  Practically: Includes otherwise non-personal information when associated or combined with personal information

# Privacy by Design (PbD)

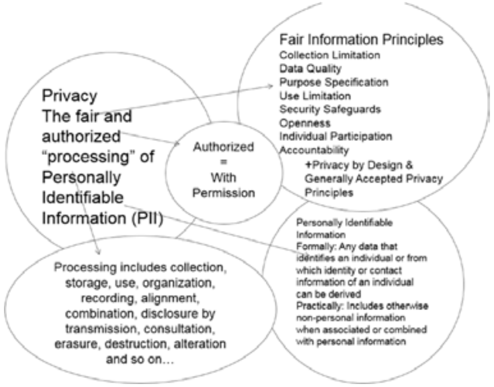
- Based on the assumption that privacy cannot be assured only by compliance with regulatory frameworks
  - Although compliance and regulatory frameworks play a crucial role
- Privacy assurance must be included into the organization and mode of operation of a system
- Adequate privacy requires thoughtful integration with every layer of an organization, including:
  - Organization policies and governance;
  - Business processes;
  - Standard operating procedures;
  - System and network architectures;
  - IT system design and development practices;
  - Management of data sources.

# PbD Foundational Principles

1. Proactive not Reactive; Preventative not Remedial
   - Anticipate issues; prevent problems before they arise
2. Privacy as the Default Setting
   - Personal data protected from inception; individuals need not act to protect data
3. Privacy Embedded into Design
   - Privacy protections are core, organic functions; not bolted on after the fact
4. Full functionality—Positive-sum, not Zero-sum
   - Privacy should enhance, not degrade, security and functionality
5. End-to-End Security—Full Lifecycle Protection
   - Security applied to each data lifecycle stage, from creation to archiving or deletion
6. Visibility and Transparency—Keep it Open
   - Individuals understand data use; privacy practices audited
7. Respect for User Privacy—Keep it User-Centric
   - Organizational imperative = privacy is about personal control and free choice
8. Privacy is not a substitute for security
   - Privacy complements other security parameters

# What does this mean for 802?

- Three dimensions:
  - Fair information principles
  - Information processing
  - Personal Identifiable Information



Privacy
The fair and authorized "processing" of Personally Identifiable Information (PII)

Authorized
=
With Permission

Fair Information Principles
Collection Limitation
Data Quality
Purpose Specification
Use Limitation
Security Safeguards
Openness
Individual Participation
Accountability
+Privacy by Design & Generally Accepted Privacy Principles

Processing includes collection, storage, use, organization, recording, alignment, combination, disclosure by transmission, consultation, erasure, destruction, alteration and so on…

Personally Identifiable Information
Formally: Any data that identifies an individual or from which identity or contact information of an individual can be derived
Practically: Includes otherwise non-personal information when associated or combined with personal information

- IEEE 802 privacy deals with:
  - PII in our standards, PII that is directly derived from our standards (e.g. IP derived from MAC), and PII in other standards that we use

# Now that we know what we protect,
# A bit more on the threats

# Threats Considerations

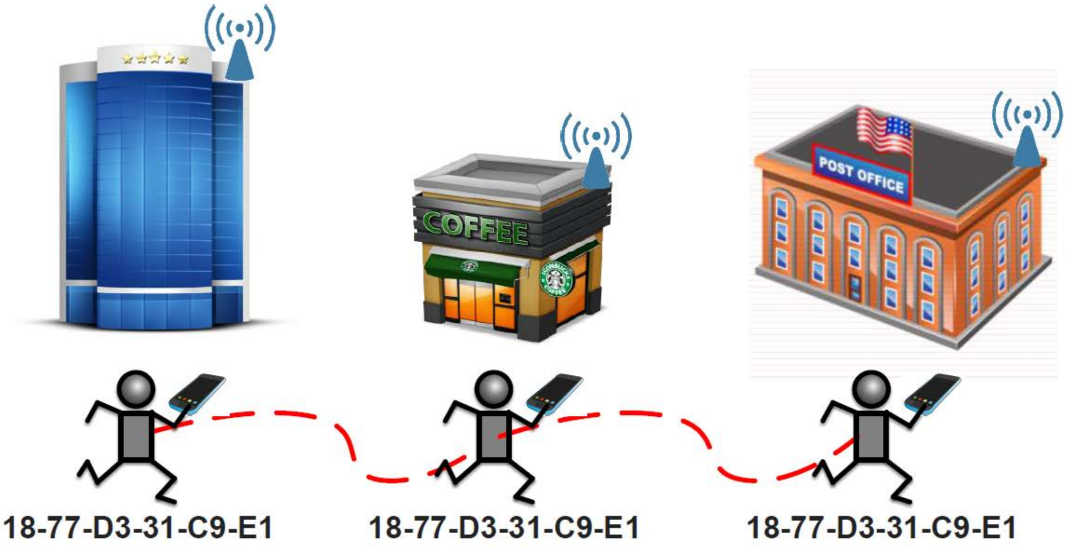
- Attack possible categorization:
  - Where
    - Is the attacker local to your L2 network (direct visibility)?
  - Who
    - Is the attacker occasional/opportunist or systematic/traceable?
  - When
    - Has the attacker ephemeral access or long term access to your network?
  - "Why" and "How" may also be of importance, in relation to the other 3 Ws… and of course "What" (next slides)

# 802E Threat Model

- Some relevant attack classes:
  - – Passive observation (Directly capture data in transit)
  - – Passive inference (Infer from reduced/encrypted)
  - – Active (Manipulate / inject data in transit)

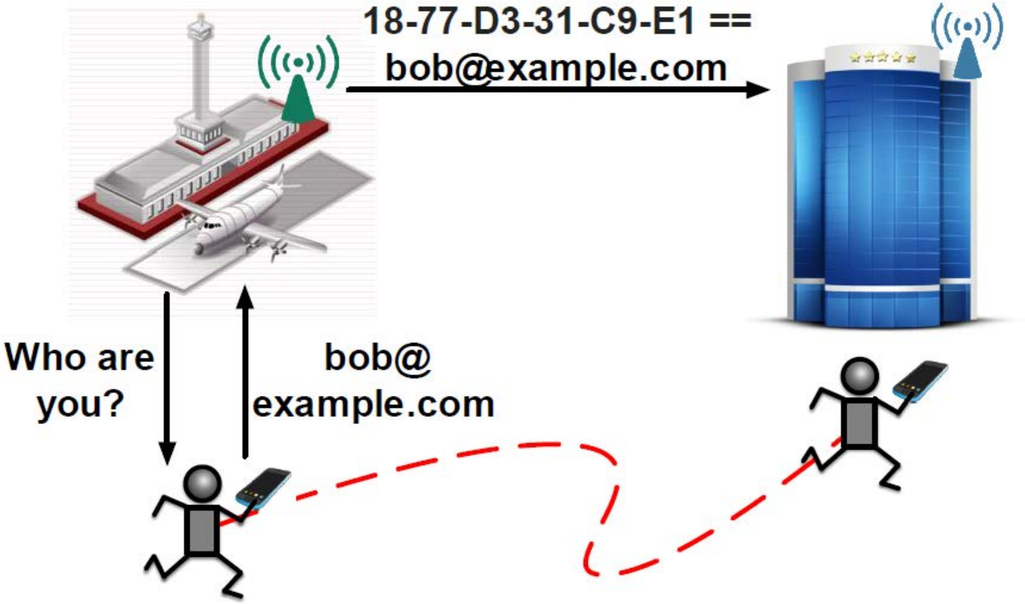
# Passive Inference / Correlation

- The combination of various pieces of information related to an individual or that obtain that characteristic when combined



# Passive Inference / Identification

- The linking of information to a particular individual to infer an individual's identity or to allow the inference of an individual's identity.



# Passive Observation

- Possible mechanisms to limit the effect of passive observation:
  - Mitigation: Hide information on the wire
  - Minimization: Don’t send the information
  - Encryption: Make the information unintelligible
  - Anonymization: Disassociate the senders and the information

# Active Attacks

- Attacker can observe and modify communications
  - Both-side identification is crucial
- Pervasive attacker may have access to multiple Layers, and multiple locations

# Summary

- 802E purpose is to promote a consistent approach by IEEE 802 protocol developers to mitigate privacy threats identified in the specified privacy threat model and provide a privacy guideline.
- First step is to identify threat models for Personal Identifiable Information (PII)
  - Identify PIIs
  - Decide which PII elements require protection
  - Identify the potential threats
  - Understand the possible effects of protecting target PII
  - Provide privacy guidelines
- An initial draft will be built to host contributions