# Privacy Harm Analysis: A Case Study on Smart Grids

Sourya Joyee De & Daniel Le Métayer
INRIA, Université de Lyon, France

26 May 2016

# PIA/ PRA is relevant today

> PIA: *"a process whereby the potential impacts and implications of proposals that involve potential privacy-invasiveness are surfaced and examined"* (Clarke'98)

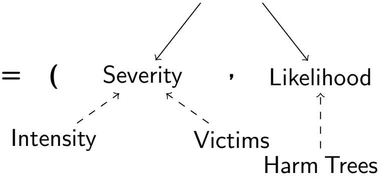
- Privacy Impact Assessments (PIA) tend to focus more on organizational aspects than technical details
  - PIA = Privacy Risk Analysis + organizational aspects . . .
- DPIA for smart grids by SGTF lacks in clarity in assessing impacts on data subjects, examples

Article 33 of the EU Regulation mandates data controllers to carry out PIA.

# A true Privacy Risk Analysis (PRA) considers harms

**Privacy Risk Analysis (PRA)** $\neq$ Traditional Security Analysis

**Privacy Harms**



**Risk Level** = ( Severity , Likelihood )

Intensity

Victims

Harm Trees

# It also considers technical ingredients

- Privacy weaknesses
- Risk Sources
- Feared Events

# But . . .

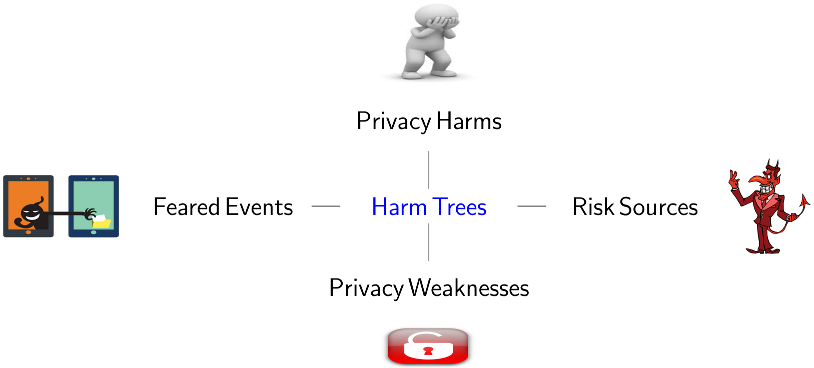
Computer scientists hardly talk about privacy harms.

Legal scholars hardly talk about feared events, risk sources or privacy weaknesses.

# So, what did we do?

We talk about all the ingredients and describe the relationship among them.

# Harm trees are central to a PRA



Privacy Harms

Feared Events — Harm Trees — Risk Sources

Privacy Weaknesses

# Why smart grids?

| Harms | Information revealed by smart meters | Pattern | Granularity |
|---|---|---|---|
| Burglary, profile based discrimination | When are you usually away from home? | High/ low power usage during the day | Hour/ minute |
| Burglary | Have you been away from home for some time? | High/ low power usage during the day | Day/ hour |
| Burglary, kidnapping, stalking, profile based discrimination | Is your home protected by an electronic alarm system? | Appliance activity matching alarm system signature | Minute/ second |
| Profile based discrimination | Do you stay at home all day watching TV or in front of the computer? | Appliance activity matching signature of TV, computer | Hour/ minute |
| Profile based discrimination, targeted advertising | Do you cook often or prefer to eat outside? | High/ low power events around meal times for microwave, cook tops etc. | Hour/ minute |

Table: Information Revealed by Smart Meters and Resulting Privacy Harms

# What are privacy harms?

Negative impacts on a data subject, or a group of data subjects, or the society.

- Effects on physical, mental, financial well-being or reputation, dignity etc.
- Useful inputs to establish a list of harms are:
  - previous privacy breaches, case law, recommendations, stakeholder consultation

| Code | Harm | Severity |
|---|---|---|
| H.1 | Profile-based discrimination | Maximum |
| H.2 | Burglary | Limited |
| H.3 | Restriction of energy usage | Maximum |
| H.4 | Kidnapping of a child | Significant |

Table: Examples of harms and their severity values in a smart grid system

Profile-based discrimination includes increase/decrease in insurance premium, less favourable commercial conditions, reflection on job or loan applications etc.

# What are privacy weaknesses?

A weakness in the data protection mechanisms of a system or lack thereof.

- Can be found out from a description of existing legal, organizational and technical controls
- Privacy weaknesses due to choices of functionalities, design, implementation of the system

| Code | Privacy weaknesses |
|---|---|
| V.1 | Security vulnerabilities in Meter Data Management System |
| V.2 | Unencrypted energy consumption data processing |
| V.3 | Unencrypted transmission of energy consumption data from home appliances to smart meter |
| V.4 | Non-enforcement of data minimization |
| V.5 | No opt-outs for consumers for high volume/precision data collection |
| V.6 | Insufficient system audit |

Table: Some relevant privacy weaknesses in a smart grid system

# What are risk sources?

An entity whose actions lead to privacy harms.

- Often referred to as *adversary* or *attacker* in the literature.
- Examples: system administrators, the utility provider, consumers, service technicians, operators or other employees, hackers.

# What are feared events?

Occurs as a result of the exploitation of one or more privacy weaknesses.

- Technical event between privacy weaknesses and harms

| Code | Feared events |
|---|---|
| FE.1 | Excessive collection of energy consumption data |
| FE.2 | Use of energy consumption data for unauthorized purpose(s) |
| FE.3 | Unauthorized access to energy consumption data |

Table: Some relevant feared events in a smart grid system

# Harm trees link them all

Harm trees depict the relationship among risk sources, privacy weaknesses, feared events and harms.

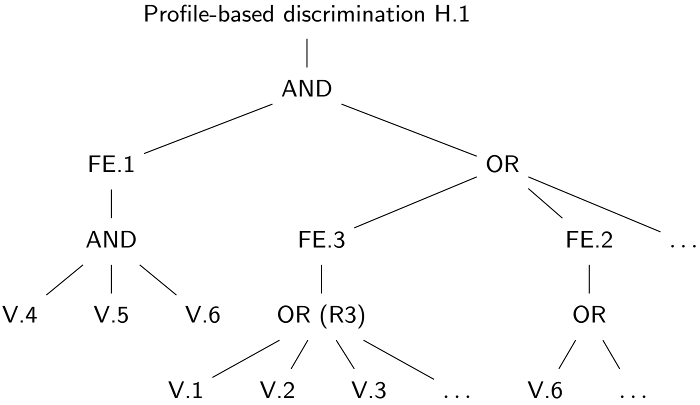
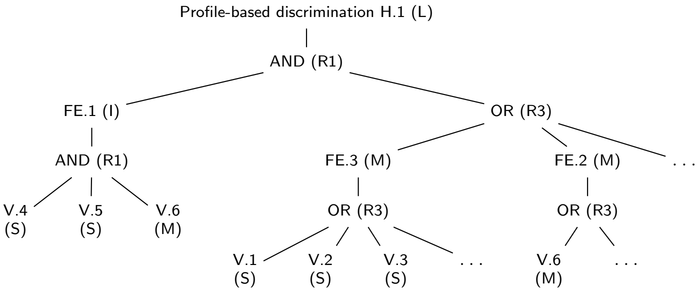


Figure: Harm tree for profile-based discrimination (H.1)

# Risk likelihood is computed using harm trees


Profile-based discrimination H.1 (L)

AND (R1)

FE.1 (I)

OR (R3)

AND (R1)

FE.3 (M)

FE.2 (M)

. . .

V.4 (S)

V.5 (S)

V.6 (M)

OR (R3)

OR (R3)

V.1 (S)

V.2 (S)

V.3 (S)

. . .

V.6 (M)

. . .

Figure: Example computation of likelihood of profile-based discrimination (H.4) using harm trees

Input and output likelihood (probability) values ($p$):
*Negligible (N)*: $p \leq 0.01\%$
*Limited (L)*: $0.01\% < p \leq 0.1\%$
*Intermediate (I)*: $0.1\% < p \leq 1\%$
*Significant (S)*: $1\% < p \leq 10\%$
*Maximum (M)*: $p > 10\%$

$P_i$ is the likelihood of $i$th child node:
R1: AND with independent children: $\prod_i P_i$.
R2: AND with dependent children: $Min_i(P_i)$.
R3: OR with independent children: $1 - \prod_i (1 - P_i)$.
R4: OR with children excluding one another: $\sum_i P_i$.

# Which harms are the riskiest?

Risk level for profile-based discrimination = *(Maximum, Limited)*
Risk level for burglary = *(Limited, Negligible)*

Based on the risk levels, risk due to profile-based discrimination should be primary target for mitigation.

This conclusion depends on initial assumptions.

# What else can be said?

Comparison of harm trees indicate which privacy weaknesses should be mitigated first.

Harm trees indicate the effect of a set of counter-measures on the risk likelihood.

The process ensures accountability by keeping track of all assumptions and choices made.

Thank you!

Contact: sourya-joyee.de@inria.fr, daniel.le-metayer@inria.fr