



The PACT Decision Support Tool for privacy, ethics and social impact assessment of surveillance technology investments

PACT, PRISMS, SURPRISE joint International Conference, 13th-14th November 2014, Vienna

Dimitris M. Kyriazanos, Olga E. Segou, Anastassios Bravakis and Stelios C. A. Thomopoulos, National Centre for Scientific Research "Demokritos", Athens, Greece.

20.11.14

PACT
Public perception of security and privacy:
Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

1



The PACT Decision Support System (DSS)

- The PACT DSS aims to support decision process for *security technologies investments* and assessment of impact in terms of *privacy, ethics, social acceptance and public perception*, assisting the decision process of experts through efficient visualisation and user-DSS interaction based on PACT's *theoretical and empirical findings*
- The PACT DSS is a decision support software tool implementing the Privacy Reference Framework for Security Technology (PRFST) 6-step methodology as described in PACT D5.2 "PACT PRFST"
- Required context data is retrieved from the system database, fed into the decision support and decision-tree process and presented accordingly to the user through multiple visualisation modes as rational arguments towards supporting the user's decision process

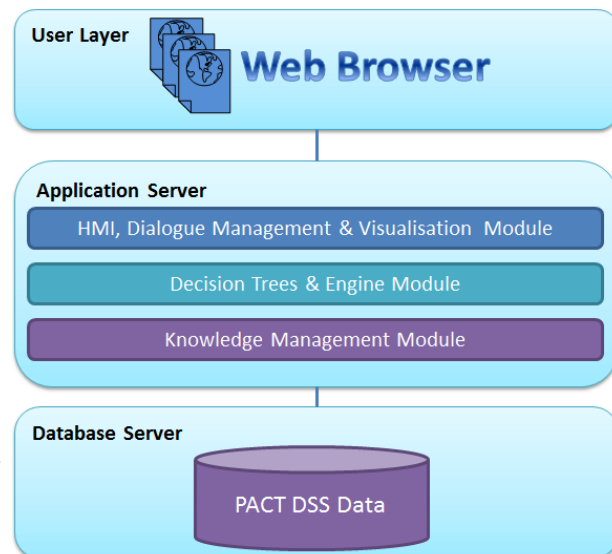
20.11.14

PACT
Public perception of security and privacy:
Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

2

A more technical view

- An Online Software Tool
- Application Logic offering personalised decision support and assistance through multiple modes
- An extensible data model, encapsulating empirical and theoretical data



PACT

Public perception of security and privacy:

Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

20.11.14

3

Context-specific, Personalised and Extensible

- Selects specific technologies, specifying also the Context according to the particular User's needs and role
- The PACT DSS is context-specific and the data model of the PACT data base builds upon the context as specified in the PACT survey, namely the Travel, Health and Internet
- A modular and extensible design, having the ability to integrate future empirical studies in other context, or enrich the existing scenarios without overhead or need for extended offline time for the PACT DSS system
- This is achieved through optimised database design, an extensible data model and a modular architecture, which allow quick inclusion of additional datasets and knowledge input

PACT

Public perception of security and privacy:

Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

20.11.14

4



Defining and Analysing the Context

- Select and analyse relevant use case context elements and retrieve relevant theoretical knowledge : e.g. stakeholders involved, standards and legislation, trustworthiness, Fundamental rights and ethical values
 - User can select specific elements and personalise according to the case and decision context
 - Expandable items offering greater customization of the current scenario and connection to survey inferences, including locality info, specifying target group (age, gender, education, work and income).
- Select the context according to empirical findings available and customization parameters provided by the user
- Select technologies to assess, linking to particular surveillance technology families and related privacy risks according to PACT Taxonomy (D1.3)

20.11.14

PACT
Public perception of security and privacy:
Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

5



Privacy, Ethics and Social Impact Assessment (i)

- PACT DSS guides the user through assessing the privacy, ethics and social impact of selected technologies within the specific context.
- Select and assess privacy risks through a provided selection according to Privacy Type: Privacy of Personal Information, Privacy of the Person, Privacy of Personal Behaviour, Privacy of Personal Communications (*UK's Information Commissioner Officer PIA Handbook*)
- Assess contribution to Privacy Targets according to *European Data Protection Directive*
- Assess Privacy risks connected with Privacy Targets
 - Create the consolidated Privacy Threat Index (PTI)

20.11.14

PACT
Public perception of security and privacy:
Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

6



Privacy, Ethics and Social Impact Assessment (ii)

- Assess relevant empirical results and inferences related to the societal perception and acceptance
 - As per the combined Context and personalised/customizable parameters
- Combine the consolidated Privacy Threat Index Metrics with empirical metrics and explore extracted decision paths in corresponding Decision Trees – **feature under development**
- Assess how the case conforms to the 8 basic privacy services identified by the OASIS Privacy Management Reference Model (PMRM), by (i) marking controls as *Mandatory*, (ii) providing ratings: *Sufficient Controls*, *Partially Sufficient Controls*, *Missing/Insufficient Controls*, and (iii) assessment comments including a prioritisation flag for each control.

20.11.14

PACT
Public perception of security and privacy:
Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

7



A Tangible and Personalised Output

- Selected Context and use case elements
- Selected technologies under investigation
- Consolidated selected privacy risks and corresponding threat metrics
 - Prioritization and assessment of applicable privacy controls
 - Comparison of decision paths and quantitative metrics
- Selection of relevant empirical inferences and societal impact references



The PACT Impact Assessment Report

20.11.14

PACT
Public perception of security and privacy:
Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

8



PACT DSS Look and Feel

User Management	PACT PRFST																					
Analysis of the scenario/use case	Visual Surveillance																					
Assets to protect	<table border="1"> <thead> <tr> <th>Privacy risk</th> <th>Likelihood</th> <th>Impact</th> </tr> </thead> <tbody> <tr> <td>Privacy of Personal Information</td> <td>High</td> <td>Medium</td> </tr> <tr> <td>Privacy of the Person</td> <td>Medium</td> <td>Medium</td> </tr> <tr> <td>Privacy of Personal Behaviour</td> <td>Low</td> <td>Low</td> </tr> <tr> <td>Privacy of Personal Communications</td> <td>Low</td> <td>Low</td> </tr> <tr> <td>Data is secretly recorded</td> <td>Medium</td> <td>High</td> </tr> <tr> <td>Data is retained longer</td> <td>Low</td> <td>Low</td> </tr> </tbody> </table>	Privacy risk	Likelihood	Impact	Privacy of Personal Information	High	Medium	Privacy of the Person	Medium	Medium	Privacy of Personal Behaviour	Low	Low	Privacy of Personal Communications	Low	Low	Data is secretly recorded	Medium	High	Data is retained longer	Low	Low
Privacy risk	Likelihood	Impact																				
Privacy of Personal Information	High	Medium																				
Privacy of the Person	Medium	Medium																				
Privacy of Personal Behaviour	Low	Low																				
Privacy of Personal Communications	Low	Low																				
Data is secretly recorded	Medium	High																				
Data is retained longer	Low	Low																				
Assessment of technological solutions	Dataveillance																					
Privacy Threat Index processing	<table border="1"> <thead> <tr> <th>Privacy risk</th> <th>Likelihood</th> <th>Impact</th> </tr> </thead> <tbody> <tr> <td>Privacy of Personal Information</td> <td>High</td> <td>Low</td> </tr> <tr> <td>Privacy of the Person</td> <td>Low</td> <td>Low</td> </tr> <tr> <td>Privacy of Personal Behaviour</td> <td>Low</td> <td>High</td> </tr> <tr> <td>Privacy of Personal Communications</td> <td>Medium</td> <td>High</td> </tr> <tr> <td>Data is secretly recorded</td> <td>Low</td> <td>Low</td> </tr> <tr> <td>Data is retained longer</td> <td>High</td> <td>High</td> </tr> </tbody> </table>	Privacy risk	Likelihood	Impact	Privacy of Personal Information	High	Low	Privacy of the Person	Low	Low	Privacy of Personal Behaviour	Low	High	Privacy of Personal Communications	Medium	High	Data is secretly recorded	Low	Low	Data is retained longer	High	High
Privacy risk	Likelihood	Impact																				
Privacy of Personal Information	High	Low																				
Privacy of the Person	Low	Low																				
Privacy of Personal Behaviour	Low	High																				
Privacy of Personal Communications	Medium	High																				
Data is secretly recorded	Low	Low																				
Data is retained longer	High	High																				
Identification of the controls to apply	Calculate																					
Reporting, guidelines and recommendations																						
tree																						

20.11.14

PACT
Public perception of security and privacy:
Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

9



DSS Success criteria, Evaluation and Validation

- PACT DSS aims at the following user-perspective success criteria:
 - Reduction on average decision process time (including collaboration with other users)
 - Improving decision specific context visibility & access to necessary knowledge for related security technologies decision making
 - Reduction on average time for compiling a privacy impact assessment report
 - Convenience and acceptance of the produced PACT impact assessment report
 - Usability & User friendliness
 - Cost effectiveness (value for money)



Validation tests and “hands-on” user evaluation feedback through the PACT cluster of end-user participants and volunteers from external experts groups. This is planned to be conducted during the combined key event consisting of the PACT consortium meeting, SAG and PAP annual meeting and HLPP final event, 18-19 December 2014 in Brussels, Belgium

20.11.14

PACT
Public perception of security and privacy:
Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

10



Decision Support, Not Decision Management



- Designed to support and not displace legitimate, democratic decision-making and validation processes
- Decisions are to be taken by the users themselves
- Supporting the process through multiple modalities and presenting quantitative and qualitative information regarding the impact of each decision path

20.11.14

PACT
Public perception of security and privacy:
Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

11



DSS developments so far and the road ahead

- A challenging inter-disciplinary work, involving all PACT partners and with the technical effort provided by ATOS and NCSR Demokritos
- The legal, technical and ethical scope of the PRFST and the DSS have been considered by consortium partners and PACT's external actors for a prolonged period of time, beginning by the Joint PRFST-DSS Workshop
- **1st Prototype Version available**
- In the process of collecting feedback and calibrate a 2nd development iteration towards the final version: **PACT-SURPRISE-PRISMS synergy**



20.11.14

12



Interested for more?



1. Visit the PACT Website:

- D1.3 "Surveillance Technologies Taxonomy"
- D4.2 "Survey Report"
- D5.1 "Report on the Definition and Design of the PRFST"
- D5.2 "PACT PRFST"
- D6.1 "DSS Architecture, Requirements and Validation Criteria"
- More to be published by Jan 2015
- <http://www.projectpact.eu/deliverables/>

2. Attend Jaime's presentation on PRFST methodology (session 4)

3. Visit our Prototype Demo Desk in the Aula (Ground Floor) and provide us with your valuable feedback [until 15:30]

20.11.14

PACT
Public perception of security and privacy:
Assessing knowledge, Collecting evidence, Translating research into action
GA 285635

13



THANK YOU FOR YOUR ATTENTION



Dimitris M. Kyriazanos, PhD
Integrated Systems Laboratory
Institute of Informatics and Telecommunications
National Center for Scientific Research "Demokritos"

E-mail: dkyri@iit.demokritos.gr

PACT Partners



PACT Project is co-funded by the European Commission - DG Enterprise Grant agreement n° 285635