



A Privacy Impact Assessment Tool For Cloud Computing

cloudcom 2010

David Tancock – University of Bristol / HP Labs Bristol - David.Tancock@hp.com

Siani Pearson – HP Labs Bristol – Siani.Pearson@hp.com

Andrew Charlesworth – University of Bristol – a.j.charlesworth@bris.ac.uk



Introduction

The presentation will outline and discuss the following aspects:

- Privacy Impact Assessments (PIAs)
- Privacy and security issues in cloud computing
- Tool development
- Alternative approaches
- Next steps
- Conclusion



Privacy Impact Assessments (PIAs)

Definition:

“A systematic process for identifying and addressing privacy issues in an information system that considers the future consequences for privacy of a current or proposed action”

(Bennett, Bayley, Charlesworth, Clarke. 2007)

- Predictive / Proactive exercise
- Consists of a series of steps
- Perceived primarily as a management tool
- Why organisations should conduct a PIA?
- No agreed international standard
- Types of PIAs



Privacy and Security Issues

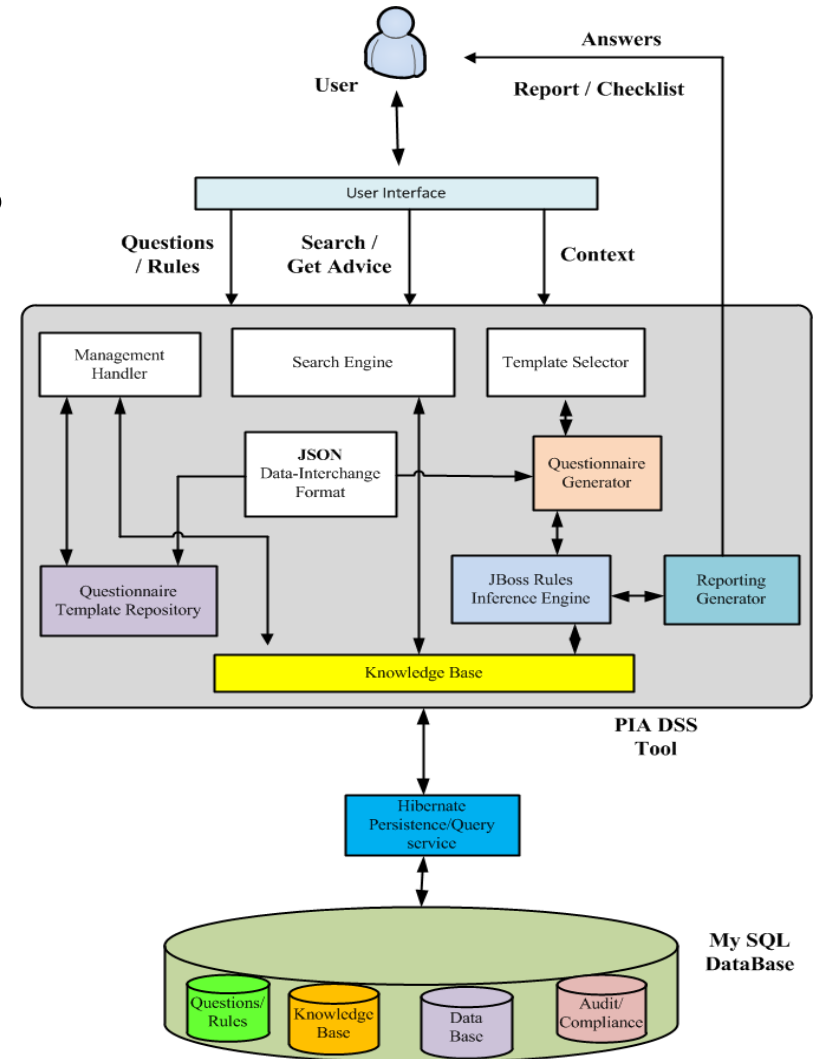
There are many concerns involving privacy and security within cloud computing including:

- Personal Identifiable Information (PII)
- Theft
- Misuse or unauthorised resale of personal data
- Loss of organisational trust by consumers
- Decrease of privacy rights, obligations and status
- Conflicting privacy laws from different jurisdictions




Tool Development

- What the PIA tool addresses?
- Tool architecture
- Knowledge representation



Tool Development

- User inputs



A Privacy Impact Assessment Tool

[Project Outline](#) [Stakeholder Analysis](#) [Environmental Scan](#)

NAVIGATION

- Welcome Page
- Initial Assessment**
- Screening Process
- Analysis of Screening Process
- PIA Assessment
- PIA Report

HELP

- PIA Handbook
- ▼ PIA Documents**
 - List of Previous Projects
 - Background Paper
 - Issue Register
- ▼ Legal Organisations**
 - Information Commissioners Office
 - Privacy International
- ▼ Legal Topics**
 - Human Rights Act 1998
 - Data Protection Act 1998
 - The Privacy and Electronic Communications Regulations 2003
 - Privacy by Design 2009
 - CCTV Code of Practice 2008
 - Information Sharing
 - Marketing

Project Information

- * Project Name:
- * Organisation Name:
- * Department Name:
- * Project Lead:
- * E-Mail Address:

Contact Information

- Contact Name:
- Contact Title:
- Telephone No:
- E-Mail Address:

* Project Description:

NOTE: The Project Description requires general information about the nature of your project. It should give a high level account of who is doing the project and what the project does.

NOTE: The fields marked with an * are mandatory and you need to fill them in before continuing.

[CONTINUE](#) [BACK](#) [For more information click on the "PIA Handbook" link on the left HELP menu](#) [SAVE](#) [EXIT](#)

Example of UK PIA tool - Project Outline form

Tool Development

- Questions and answers

The screenshot displays a web-based PIA tool interface. At the top left is a yellow padlock icon. The main title is "A Privacy Impact Assessment Tool". Below the title are navigation tabs: "Full-Scale PIA", "Small-Scale PIA", "Information Collection", "Information Processing", "Information Dissemination", and "Invasions".

NAVIGATION

- Welcome Page
- Initial Assessment
- Screening Process
- Analysis of Screening Process
- PIA Assessment**
- PIA Report

HELP

- PIA Handbook
- ▼ **PIA Documents**
 - List of Previous Projects
 - Background Paper
 - Issue Register
- ▼ **Legal Organisations**
 - Information Commissioners Office
 - Privacy International
- ▼ **Legal Topics**
 - Human Rights Act 1998
 - Data Protection Act 1998
 - The Privacy and Electronic Communications Regulations 2003
 - Privacy by Design 2009
 - CCTV Code of Practice 2008
 - Information Sharing
 - Marketing

Question

Does your product, service, program, or project collect personal information from outside the organisation?

Yes No Not Sure Question is unclear [Click for help](#)

Question

Does your product, service, program, or project collect Personal Identifiable Information (PII) from outside the European Union ?

Yes No Not Sure Question is unclear [Click for help](#)

Question

If PII is collected from outside the European Union, please state the country of origin?


 Other Question is unclear [Click for help](#)

[CONTINUE](#) [BACK](#) [For more information click on the "PIA Handbook" link on the left HELP menu](#) [SAVE](#) [EXIT](#)

Example of UK PIA tool - PIA Assessment Questions

Tool Development

- Tool outputs



A Privacy Impact Assessment Tool

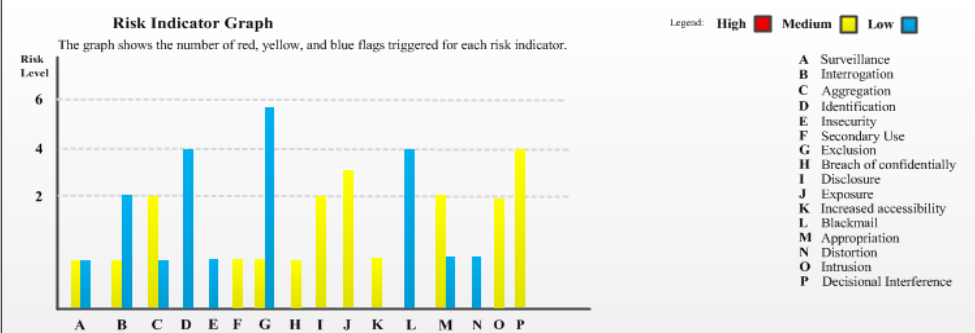
Full-Scale PIA | Small-Scale PIA | Privacy Law Compliance Check | Data Protection Compliance Check

Risk Summary

Risk Indicator Graph


The graph shows the number of red, yellow, and blue flags triggered for each risk indicator.


Legend: High (Red), Medium (Yellow), Low (Blue)



Risk Indicator	High	Medium	Low
A	1	0	1
B	0	1	2
C	0	2	1
D	0	0	4
E	0	0	1
F	0	1	0
G	0	0	6
H	0	1	0
I	0	2	0
J	0	3	0
K	0	1	0
L	0	0	4
M	1	2	0
N	0	0	1
O	0	2	0
P	0	4	0

Privacy Compliance/Non Compliance

 The reasons below provide information about Privacy related risks of your project. The results of the completed PIA Assessment has found the project to have a **Medium** level of risk, because you have 0 red flag(s) and 21 yellow flag(s) for Privacy Risk or Litigation. Changes to your project or solution may be required in order to become compliant with your applicable jurisdictional privacy laws and regulations.

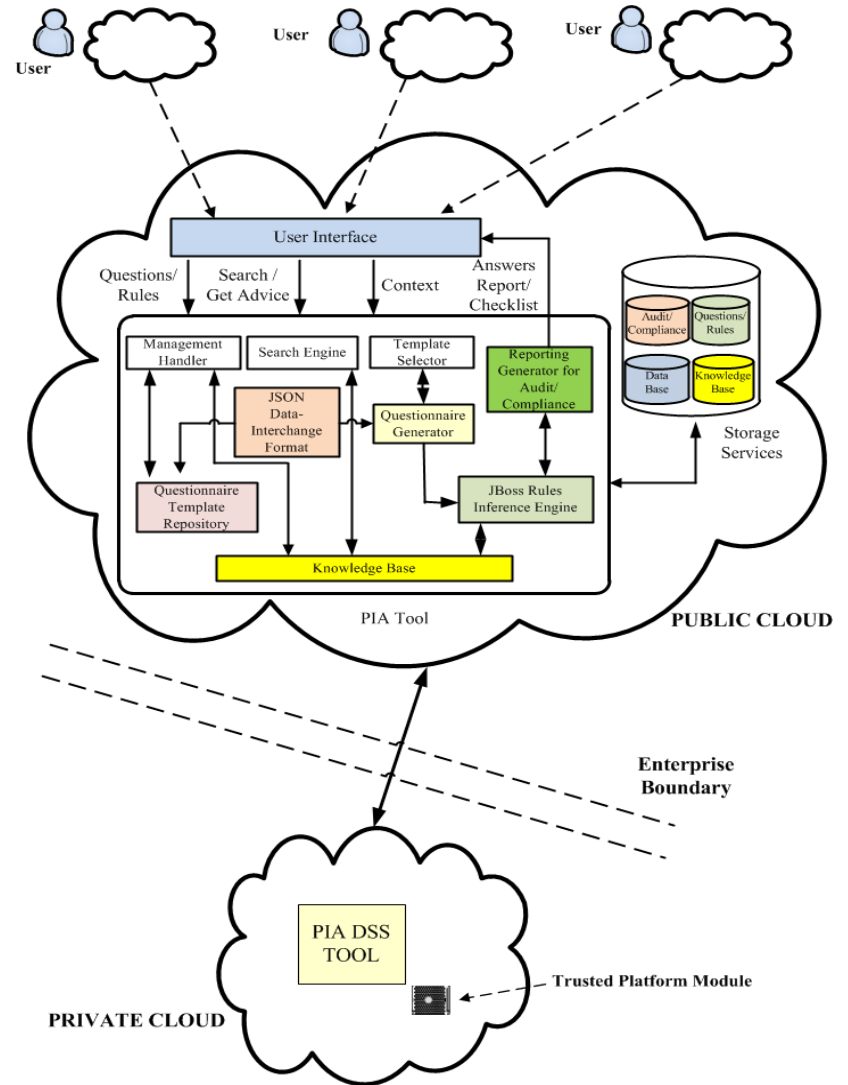
 **Reasons:** The project has not been evaluated by your organisation privacy officer to ensure that the appropriate data privacy clauses are included in any agreements or contracts [View details](#)

[For more information click on the "PIA Handbook" link on the left HELP menu](#)

Example of UK PIA tool – PIA Report page 2

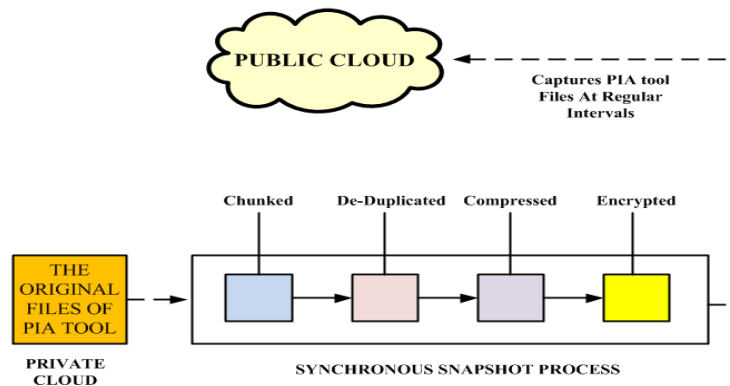
Tool Development

- Cloud deployment



Alternative Approaches

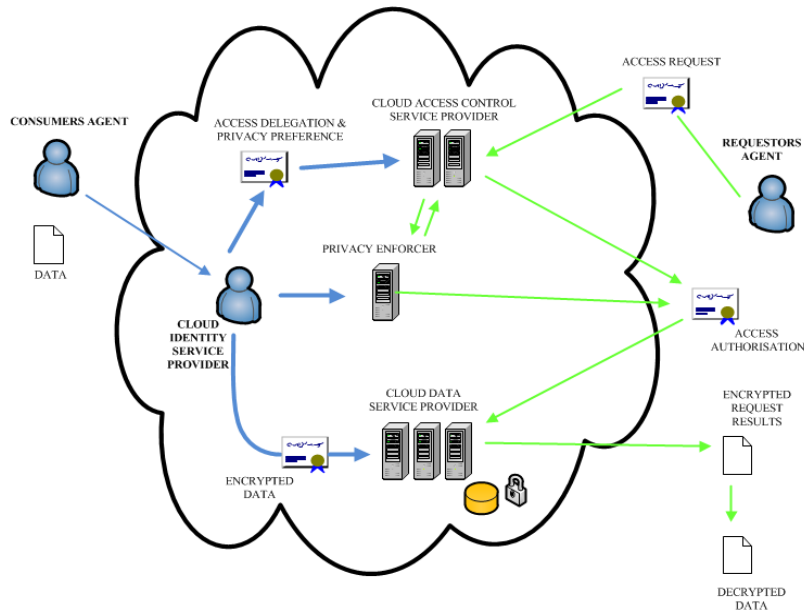
- Location register
- Cloud storage gateway
- Accountability
- Obfuscation
- Hewlett Packard Privacy Advisor (HPPA)



(Nasuni, 2010)

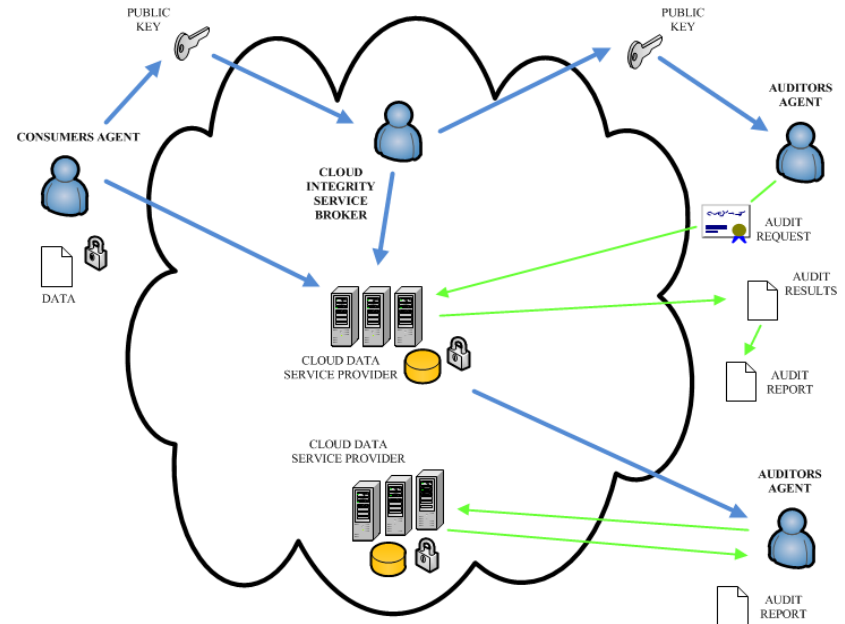
Alternative Approaches

- Privacy by Design



Cloud computing architecture for privacy-preserving and usable data outsourcing

(A. Cavoukian. 2010)



Cloud computing architecture for privacy-preserving, trustworthy, and available data outsourcing

(A. Cavoukian. 2010)

Next Steps in Development

- Analyse further how stakeholder analysis and workflow can be integrated into the tool, and whether there are any aspects of PIAs that cannot be captured by such an approach
- Conduct empirical research to obtain the initial set of rules for the KB.
- Consider different Artificial Intelligence (AI) methods for the analysis (i.e. the reports and the grading of privacy risks etc.)



Next Steps in Development

- Choose a cloud storage gateway provider for our tool. This will be measured by the services they provide and the costs that they charge for this service.
- Develop the code using Java (i.e. Java Server Pages (JSP), JavaBeans etc.) technologies. This will involve employing a modular approach from the design phase, and includes building the KB.



Conclusions

We are currently developing a PIA tool that can be used in a cloud environment to identify potential privacy risks and compliance. We believe that this generic approach will prove of increasing benefit as cloud service adoption increases.



Q/A

