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

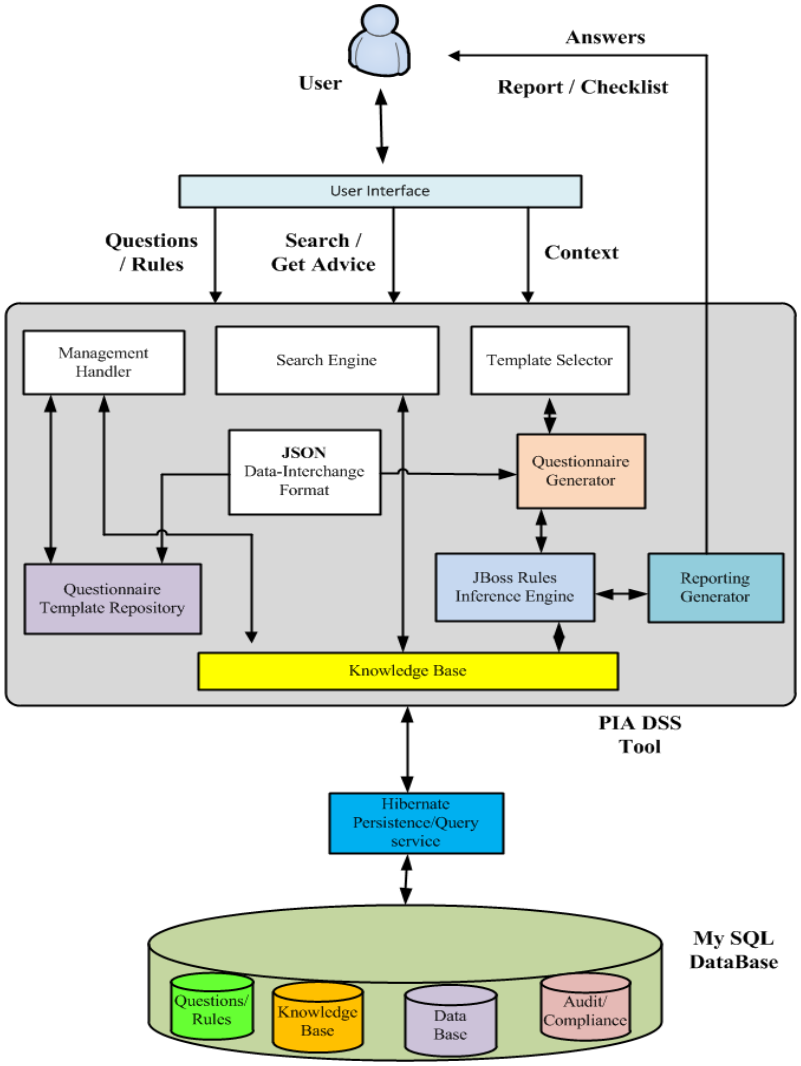
Privacy and Security Issues

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

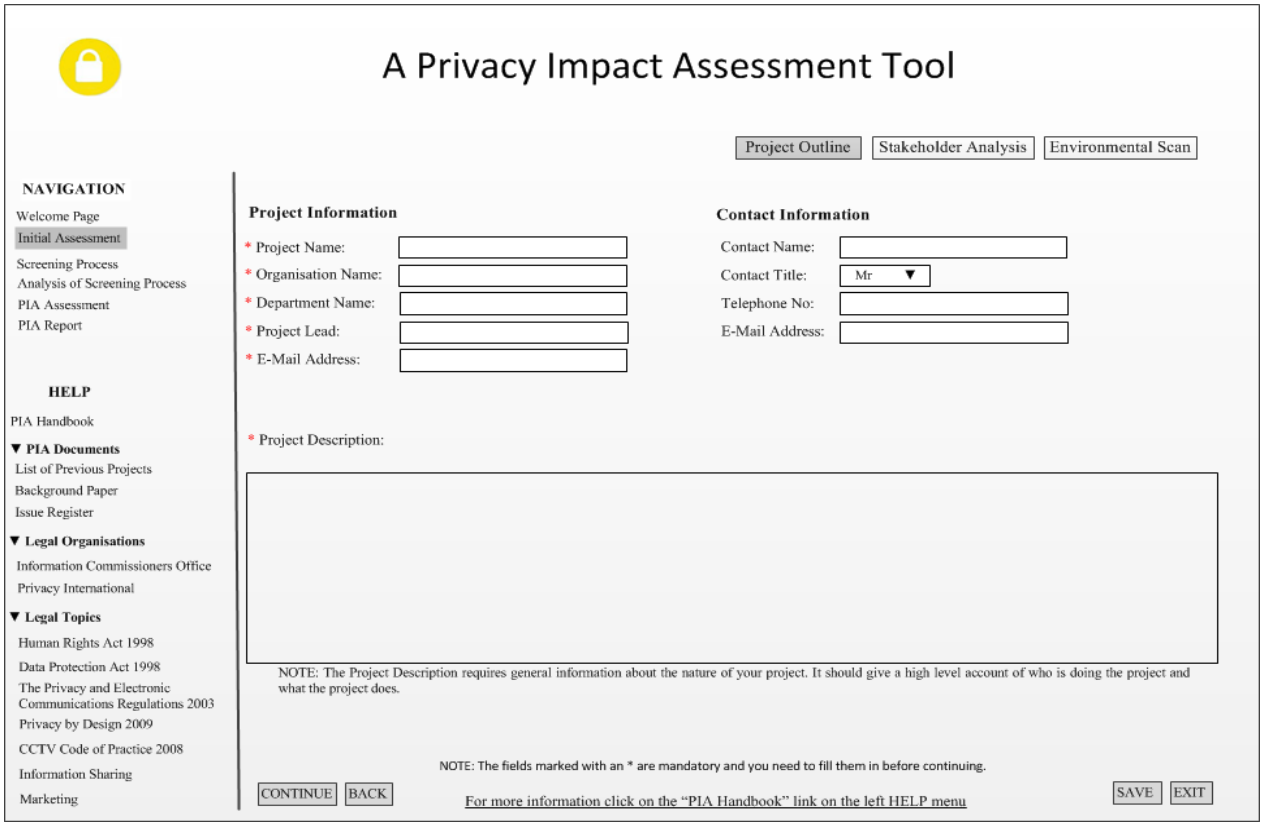
Tool Development

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



Tool Development

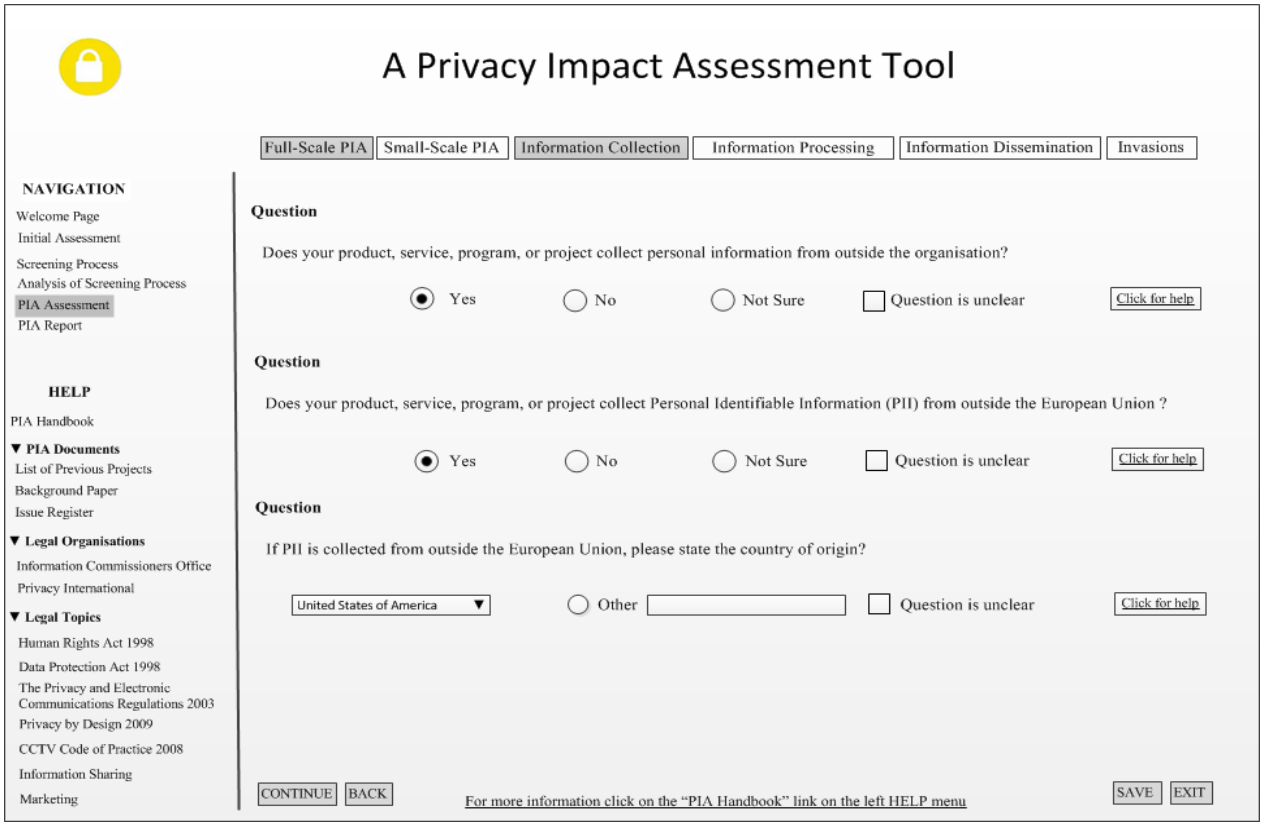
- User inputs



Example of UK PIA tool - Project Outline form

Tool Development

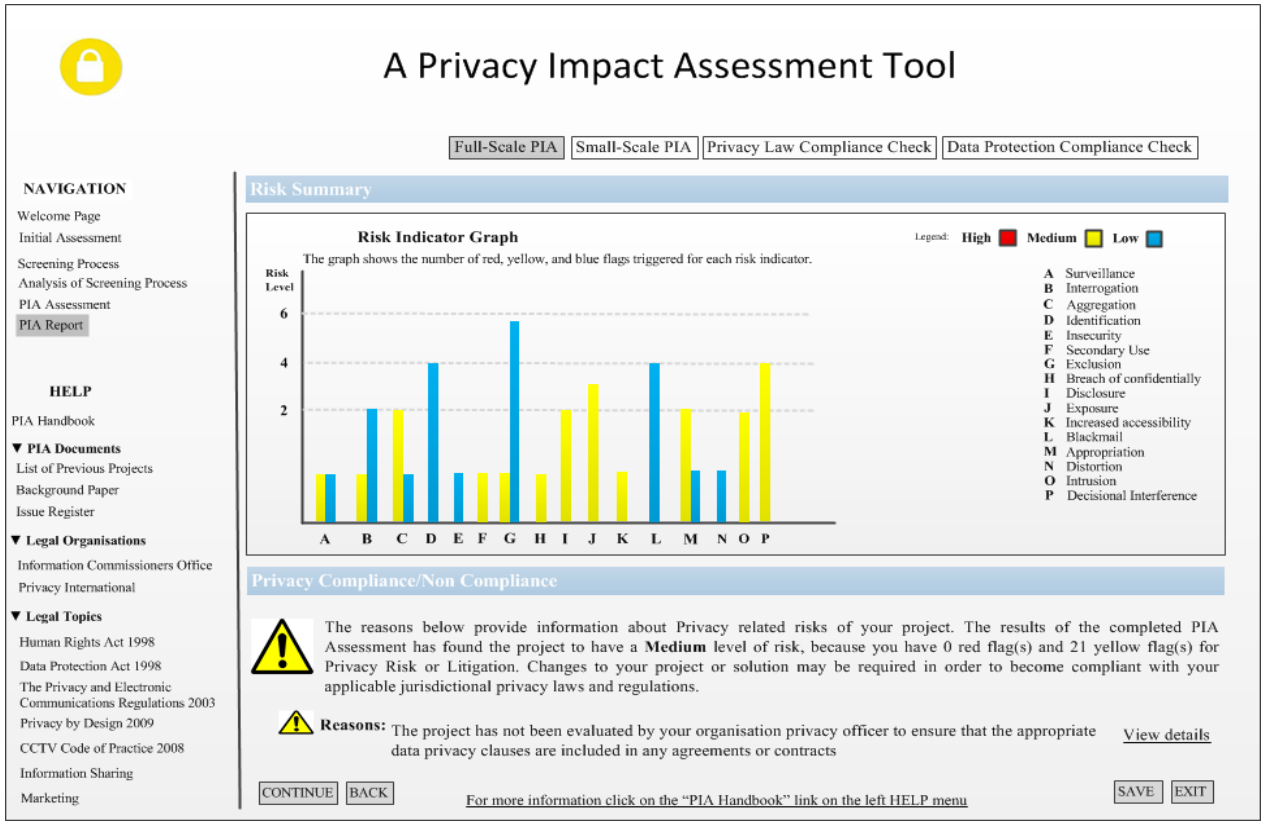
- Questions and answers



Example of UK PIA tool - PIA Assessment Questions

Tool Development

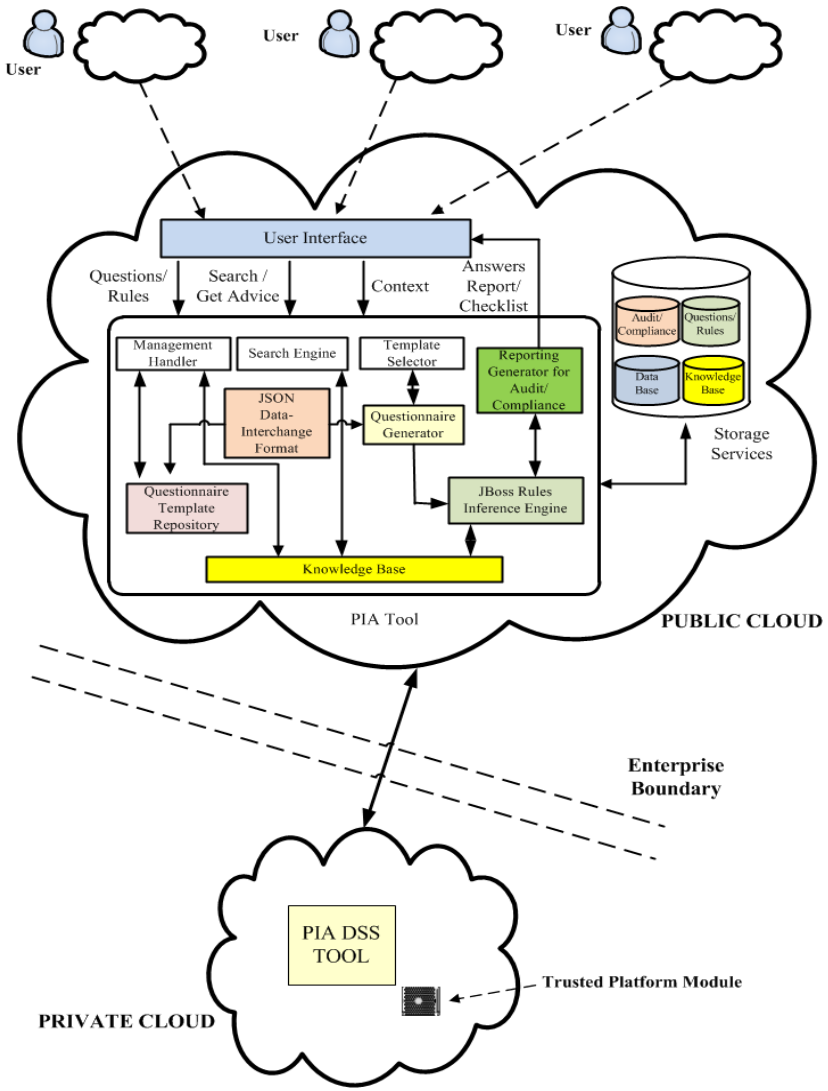
- Tool outputs



Example of UK PIA tool – PIA Report page 2

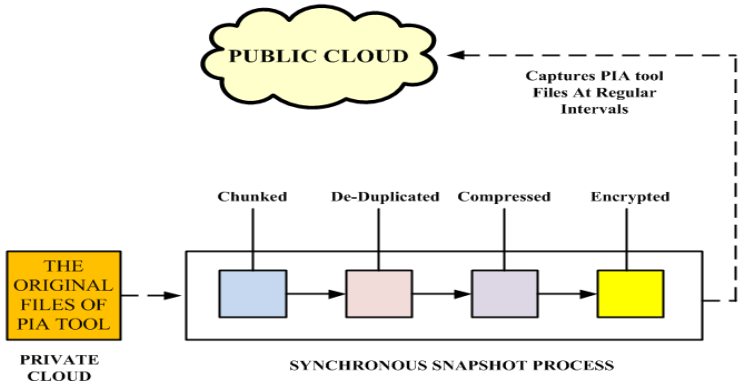
Tool Development

- Cloud deployment



Alternative Approaches

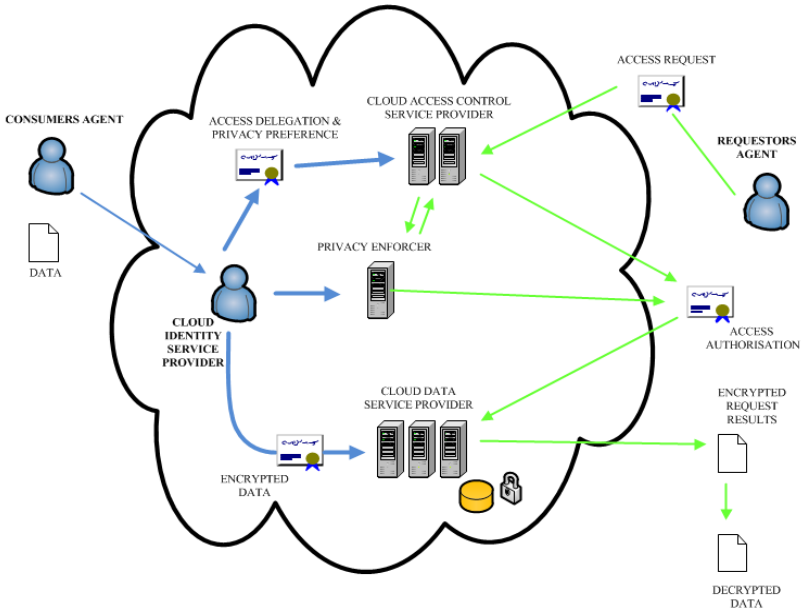
- Location register
- Cloud storage gateway
- Accountability
- Obfuscation
- Hewlett Packard Privacy Advisor (HPPA)



(Nasuni, 2010)

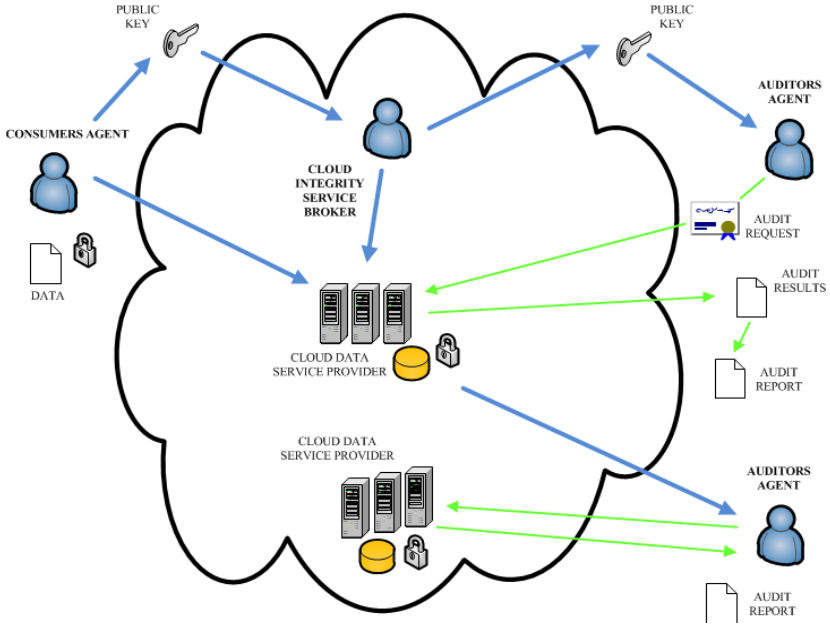
Alternative Approaches

- 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