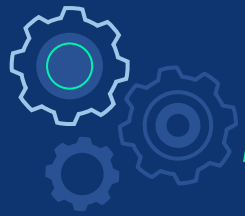
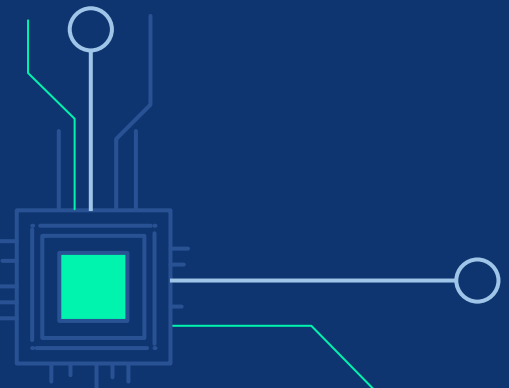


APPLYING FORMAL METHODS TO DETECT AND RESOLVE AMBIGUITIES IN PRIVACY REQUIREMENTS

Ioannis Agrafiotis, Sadie Creese, Michael Goldsmith, and Nick Papanikolaou



presented by Ioana Chelaru

TABLE OF CONTENTS

TABLE OF CONTENTS

PRIVACY

- the term has no inherent definition
- increasing number of incidents where data has been lost, mistreated, or shared without authority

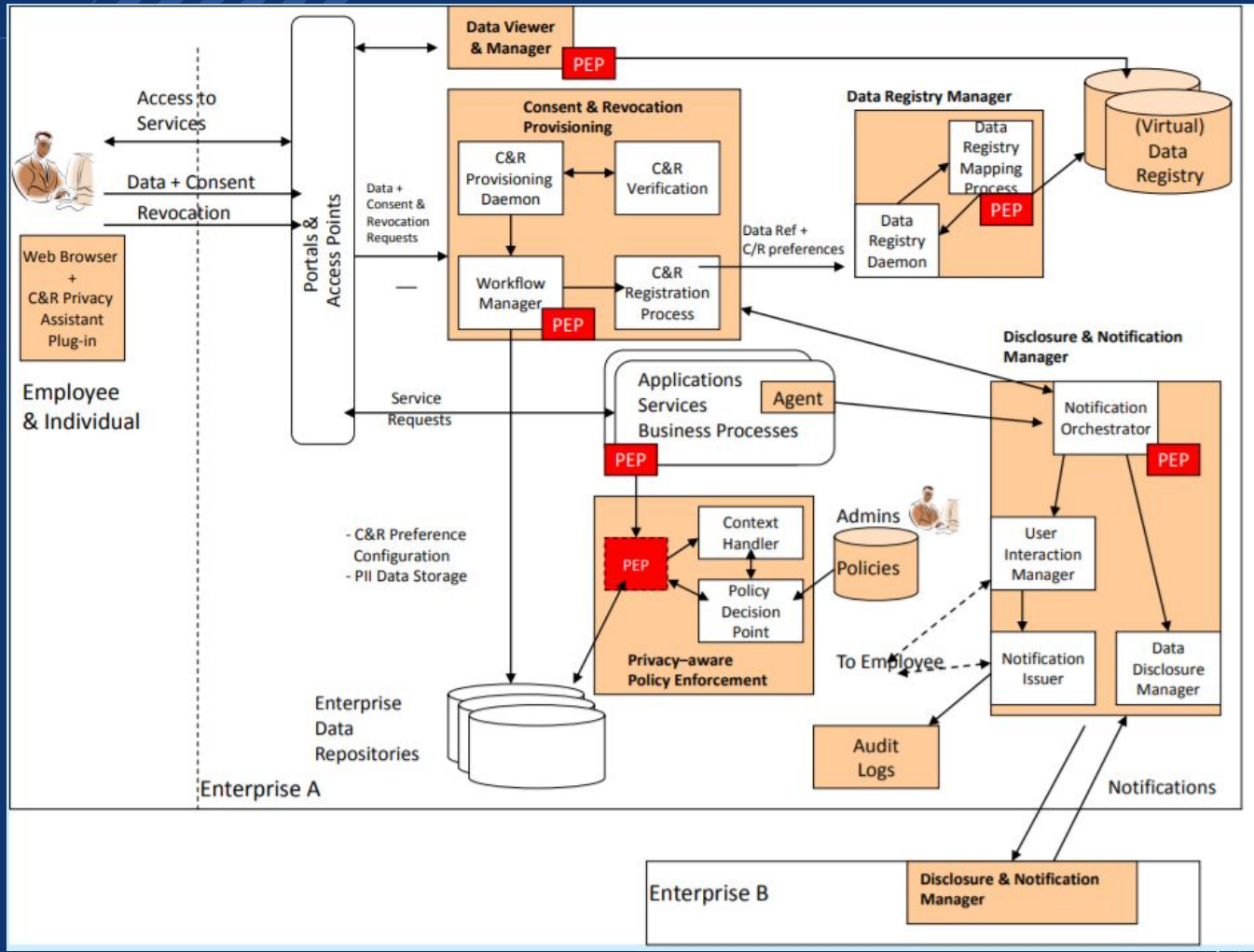
Don't let giraffes ruin your fun.

THE ENCORE PROJECT

- Ensuring Consent and Revocation
- June 2008 - November 2011
- £3.6 million

Press Briefing

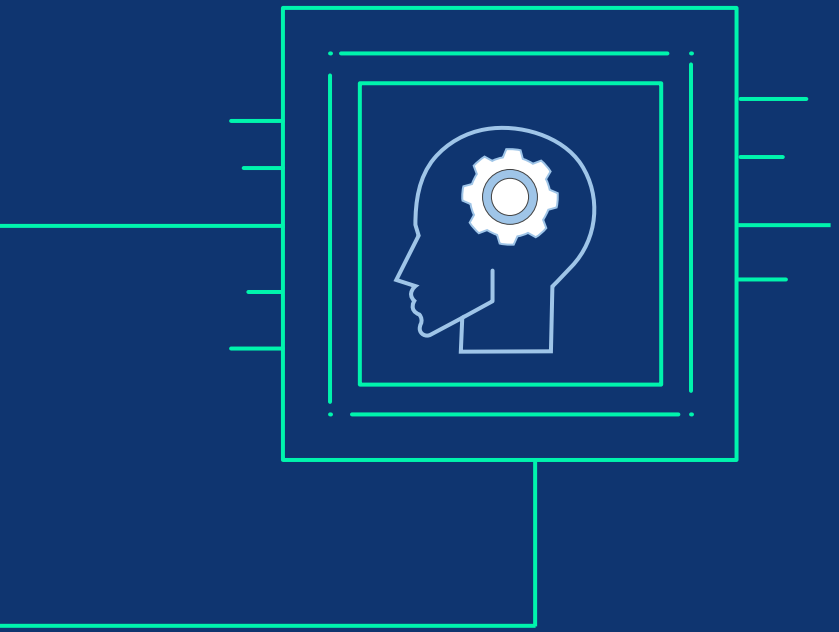
TECHNICAL ARCHITECTURE



ACCESS CONTROL MODEL

- uses labelled transition systems
- suited for expressing privacy preferences
- does not provide an intuitive language

HOARE LOGIC



- defines C&R processes with a set of rights
- it models C&R as the application of rights that allow certain permissions
- more intuitive to the way data subjects express themselves

CASE STUDY

- Enhanced Employee Data Scenario
- illustrates key points affecting the management of C&R
- the employee data scenario focuses on sensitive information

AMBIGUITIES IN REQUIREMENTS

FIRST CLASS

- details of the law
- regulations
- policy
- social factors

SECOND CLASS

- the complexity of the notion of privacy
- conflict between subjects and data controllers

CONCLUSIONS AND FUTURE WORK

THANK YOU!

Do you have any questions?