Consumer Centric Data Control, Tracking and Transparency

James Tapsell, Raja Naeem Akram, and Konstantinos Markantonakis

Information Security Group, Smart Card and IoT Security Center

The Smart Card and Internet of Things Security Centre

Objectives

The main objectives of this work can be summed up as below:

- Challenges of data ownership and control, and how it can be transferred to individual users to own/manage their data.
- A framework that brings together the three main stakeholders (users, organisations, governments) to build a Consumer Oriented Data Control & Auditability framework.
- Building blocks of CODCA: Consumer Data Control and Data Auditability.

Introduction

User data, the data that relates to a user's person, activities and services, can be considered to be a valuable commodity for not only technology oriented companies like Google, Amazon and Apple. But also its value is being recognised by traditional companies like travel/transport, banking, entertainment and marketing industry. Furthermore, these trends had led to better, targeted and personalised services for individuals – in most case at no or minimal financial cost to them. This relationship, in which user signs up to allow companies collect some data about the individual to get in return operational flexibility, personalised/targeted/context-aware services and hassle-free activities (for users) is flourishing. For both in this relationship, the data is valuable and its security, integrity and accessibility is paramount. This relationship is going to become more entrenched in the era of Internet-of-Things (IoT), autonomous vehicles and seamless travel. In this work, we exam the challenges faced by both the users and organisation in dealing with the Personal Identifiable Information (PII). We extend the discussion to the future technologies, especially the IoT and integrated transport system for better customer experience – and their ramification on the data governance and PII management.

Core Architecture

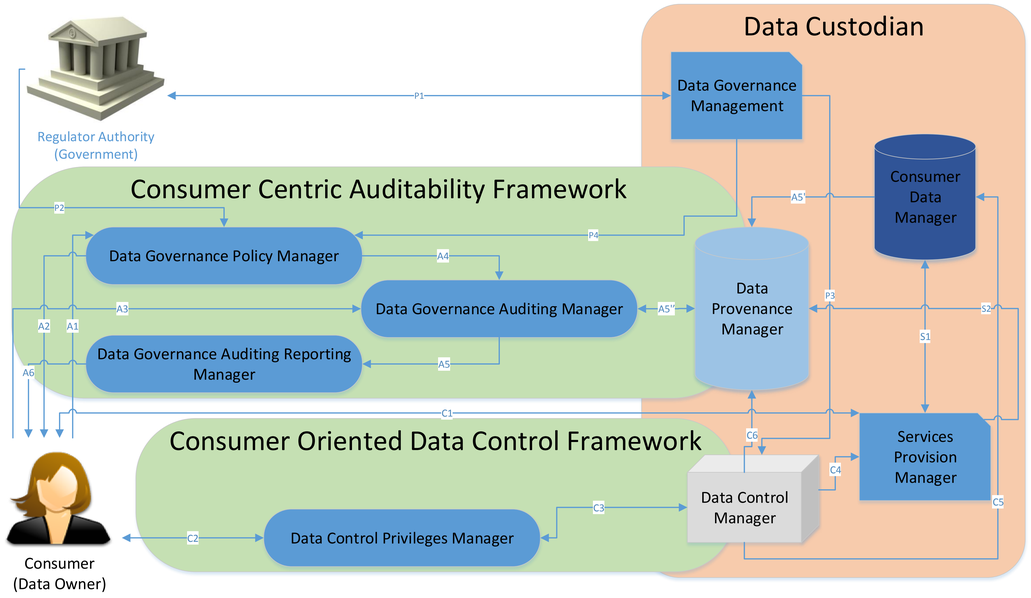

Figure 1: Overview of the CODCA Framework.

Important Result

We propose a framework that gives maintains the balance between the user's privacy (and potential desire of control) and organisations objective of delivering quality, targeted and effective services to their customers using the "user data). This framework is termed as "Consumer Oriented Data Control & Auditability" (CODCA).

Governance Policy Extraction

For a consumer to manage, track and audit her data, the crucial element is what are her privileges and rights as specified by the agreement she has accepted in relation with the data custodian. The data governance policy extractions takes a human readable agreement (signed between the consumer and data custodian) and translates into concrete data management rule sets.

Data Provenance

Data provenance, if implemented as a light-weight mechanism at system level, can provide an excellent auditing tool, which in our opinion is an important component of CODCA. Another challenge the data provenance has to overcome is how it provide privacy protection while keeping the association with the data after it is being anonymised.

Data Governance Audit

This process is dependent upon the previous two main processes discussed. The main challenge is to able to take the data policy rule set and data provenance, and detect whether the data custodian has violated the stated policy and/or regulations. On surface, this seems like a straightforward tasks; query the data provenance for violations and based on the response develop the report. However, the challenge is how to manage different levels of data provenance details - as different data custodians might collect and maintain data provenance differently.

Conclusion

The data owner, whether it is an individual user or an organisation, has complete control over how, where, and by whom their data can be accessed. In addition, the data owner should have the ability to track the data and the processes performed on it. Furthermore, the data owner have the ability to perform audit of actions performed on their data in the context of the mutual agreement that the owner has signed with the data custodian (individual/organisations).

Acknowledgements

The authors from Royal Holloway University of London acknowledge the support of the UK's EPSRC, and the contributions of the DICE project partners.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the position of the DICE project or any of organisations associated with this project. The paper is published in IEEE TrustCom 2018, New York, USA.

Contact Information

- Web: www.jrtapsell.co.uk/intern-2018.html
- Email: papers@jrtapsell.co.uk