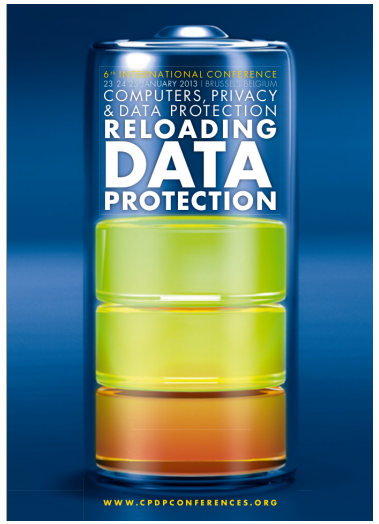
Accountability by Design — From General Principles to Effective Protection

Denis Butin, Marcos Chicote and Daniel Le Métayer

informatiques mathématiques

fi-ware



The Context — Accountability Defined

Accountability by Design in Practice

What is accountability for data protection?

- Article 29 Working Party Opinion: "showing how responsibility is exercised and making this verifiable"
- Accountability already appeared in OECD Privacy Protection Guidelines, 1981
- Accountability principle expected in EU Data Protection Regulation

Our focus: accountability of practice

- Often used vaguely — nature of the account? Identity of recipient?
- Bennett: Distinguish between accountability of policy / of procedures / of practice
- We focus on how the account looks in practice!

Motivation (1/2)

- Runtime / a posteriori verifications needed!
- DC should be accountable to DS
- Practical requirements?
- Need to provide means to check that agreements were fulfilled in terms of actual PII handling

Motivation (2/2)

- Need more precision and bridges between broadly-defined concepts and actual IT systems
- For PII handling: DS must be able to check that actual PII handling in line with agreements
- How to make those (currently legal) agreements more readable both for individuals and machines?
- How to check compliance with agreements efficiently?

Enabling accountability (1/2)

- On actual technical platforms, we deal with data handling event histories ("logs") — raw account
- Accountability does not emerge spontaneously from logs
- Feasibility of comprehensive a posteriori verification?
- Depends directly on technical architecture! Need standardised and expressive format

Enabling accountability (2/2)

- DS and DC express PII handling preferences / policies in standardised way, once and for all
- If automated matching succeeds, interaction proceeds and actual handling leaves trace (log)
- Need unforgeability guarantees
- Log checked automatically against initial policy agreement by tool

Log structure conditions accountability

- DC must provide evidence that agreements met
- Audit possible through inspection of event histories (logs) wrt data handling agreements
- Structure of logs conditions auditability, hence accountability
- Deciding what to include in logs and how to express it — no trivial tasks

Three ingredients for the account

Need to define:

- Obligations to be met
  $\longrightarrow$ in a suitable usage policy language
- Compliance checking evidence
  $\longrightarrow$ by using expressive log architecture
- Compliance checking procedure
  $\longrightarrow$ by implementing log analyzer

Summarizing (1/2)

- Classical questions when talking about accountability: of who? To whom? How?
- Focus on the *how* — the nature of the account
- In *practical* terms, close to the actual handling of PII

Summarizing (2/2)

- DC provides policy agreements compliance evidence
- Automatic audit of logs wrt agreements
- Log structure has major effect on accountability
- Log designer plays decisive role in creating the account