End-to-End Privacy Accountability

Denis Butin[1] and Daniel Le Métayer[2]

[1]TU Darmstadt

[2]Inria, Université de Lyon

TELERISE, 18 May 2015

Defining Accountability

Privacy Requirements for Accountability

End-to-End Accountability

Examples: Data Collection, Data Usage

Synthesis

Is Accountability Needed?

- Ever-increasing exchanges of personal data between systems and across countries
- Accountability as a means to provide verifiability of actual personal data handling
- Key idea: data controllers (DC) must not only comply with data protection rules but also demonstrate compliance
- Empower data subjects (DS), e.g. individuals — restore balance of power
- Importance of accountability increasingly acknowledged in legal systems, notably EU General Data Protection Regulation Draft
- Benefits also for DC, e.g. organisations, corporations

Defining Accountability — 1/2

- Principle of accountability introduced 30 years ago (OECD), increasingly mentioned
- Buzzword? Used both in technical and legal settings, widely varying situations
- Working definition: Article 29 Working Party Opinion. Accountability principle defined as *showing how responsibility is exercised and making this verifiable*
- More than mere privacy policy compliance. Includes burden of proof

Defining Accountability — 2/2

Existing literature split in two strands:

- Technical approaches: focus on specific security properties, e.g. authentication, non-repudiation, privacy property verification, log security . . .
- Policy-oriented perspectives: focus on organizational measures, legal compliance

Gap between those stances. Problematic: need integrated approach to take into account all dimensions. Combination of organisational, legal and technical measures

Categories of Accountability

Zooming in, using Colin Bennett's 3-tier terminology:

- Acc. of policy: demonstrate intent — existence of privacy policy (natural language + technical), show policy adequacy wrt norm
- Acc. of procedures: demonstrate adequacy of organisational mechanisms for implementation of privacy policies, e.g. documented processes
- Acc. of practice: a posteriori demonstration of effectiveness of acc. of procedures. Requires recording sufficient information about system operation. Formalisation useful

Excessive focus on first two layers common

Privacy Requirements for Accountability

Privacy requirements from many sources:

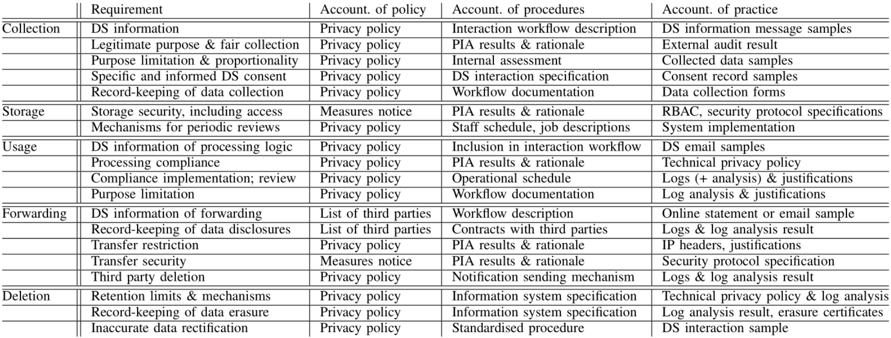
- Laws, i.e. national implementations of EU Data Protection Directive 95/46/EC or forthcoming General Data Protection Regulation
- Self-defined privacy policies by data controllers — usually declarative statements in natural language
- Technical, machine-readable privacy policies in form of data handling rules, possibly automatically negotiated with data subjects
- Many technical privacy policy languages: PPL, XACML, UCON . . . General purpose / access control / usage control. Can be used to assess log compliance

Methodology

- Look in turn at each stage of personal data life cycle wrt design and operation of accountable systems
- Data collection / storage / usage / forwarding / deletion + aspects common to all
- Illustration: requirements from General Data Protection Regulation Draft. Just an example. Key idea: general approach

Overview

TABLE I. SYNTHESIS OF EVIDENCE FOR PRIVACY REQUIREMENTS ACROSS PERSONAL DATA LIFE CYCLE STAGES



	Requirement	Account. of policy	Account. of procedures	Account. of practice
Collection	DS information	Privacy policy	Interaction workflow description	DS information message samples
	Legitimate purpose & fair collection	Privacy policy	PIA results & rationale	External audit result
	Purpose limitation & proportionality	Privacy policy	Internal assessment	Collected data samples
	Specific and informed DS consent	Privacy policy	DS interaction specification	Consent record samples
	Record-keeping of data collection	Privacy policy	Workflow documentation	Data collection forms
Storage	Storage security, including access	Measures notice	PIA results & rationale	RBAC, security protocol specifications
	Mechanisms for periodic reviews	Privacy policy	Staff schedule, job descriptions	System implementation
Usage	DS information of processing logic	Privacy policy	Inclusion in interaction workflow	DS email samples
	Processing compliance	Privacy policy	PIA results & rationale	Technical privacy policy
	Compliance implementation; review	Privacy policy	Operational schedule	Logs (+ analysis) & justifications
	Purpose limitation	Privacy policy	Workflow documentation	Log analysis & justifications
Forwarding	DS information of forwarding	List of third parties	Workflow description	Online statement or email sample
	Record-keeping of data disclosures	List of third parties	Contracts with third parties	Logs & log analysis result
	Transfer restriction	Privacy policy	PIA results & rationale	IP headers, justifications
	Transfer security	Measures notice	PIA results & rationale	Security protocol specification
	Third party deletion	Privacy policy	Notification sending mechanism	Logs & log analysis result
Deletion	Retention limits & mechanisms	Privacy policy	Information system specification	Technical privacy policy & log analysis
	Record-keeping of data erasure	Privacy policy	Information system specification	Log analysis result, erasure certificates
	Inaccurate data rectification	Privacy policy	Standardised procedure	DS interaction sample

In this talk: focus on two data cycle life stages to convey approach

Data Collection: GDPR Requirements

- DC must inform DS about many aspects of personal data collection: right to object/access/rectify/delete, purpose of processing, retention period, whether data encrypted ...
- Purposes must be specific, explicit, legitimate
- Amount of collected data must be proportional to purposes of processing
- Specific and informed consent is needed for personal data collection
- DC must keep records of data collection to enable DS to exercise right of information later (directly or via DPA)

Data Collection: Accountability Measures

- Demonstrate that right of information was respected: keep pseudonymised database listings, metadata (notably purpose). Samples of messages sent to DS. Quality assurance mechanism
- Privacy Impact Assessments to show legitimacy and proportionality of personal data processing. Performed before the design of system (PbD). PIAs are not mandatory by themselves but strongly contribute to acc.
- Demonstrate DS consent: ideally, full electronic signatures — not always feasible. Lengthy legal texts not acceptable (concision criteria)

Data Usage: GDPR Requirements

- DC must inform DS about *logic of automated processing*, profiling, data usage purposes . . .
- DC must demonstrate compliance of data processing with Regulation — extremely broad requirement
- DC must implement compliance procedures and policies that *persistently respect the autonomous choices* of DS
- DC may only use personal data in line with initially declared purpose

Data Usage: Accountability Measures (1/2)

- Acc. of practice approach to personal data processing compliance: use technical privacy policy language (PPL, SIMPLE, FLAVOR . . .)
- Combine with evidence about data handling. Evidence generated as system logs (log: trace/record of system events)
- Two aspects: existence of evidence, compliance of evidence with policies — log analysis
- Abstract away from internals: translation between low-level system events and events on categories of personal data

Data Usage: Accountability Measures (2/2)

Adequate log design not trivial. Missing details can be enough to render logs useless for compliance checking. Semantic comprehensiveness imperative. Other log considerations:

- Trustworthiness: logs must reflect actual system behaviour. Use partial formal modelling for critical components
- Storage security: monitor log access; prevent tampering (e.g. forward integrity)
- Minimisation: keep no extraneous data

Synthesis (1/2)

- Systematic analysis of acc. requirements for DC, and indirectly for system designers, across personal data life cycle
- Each requirement leads to key evidence fragments, to be gathered to present convincing narrative to auditors
- Evidence must not introduce new privacy threats — e.g. special care for system event logs

Synthesis (2/2)

- Acc. costs for DC can be minimised by including provisions in design phase
- Also added value for DC: clarify internal processes, encourage quantification, potential competitive advantage
- No promise of absolute privacy guarantees, but best bet to protect individuals by increasing pressure on DC

Thank you!

Questions & feedback welcome

TECHNISCHE
UNIVERSITÄT
DARMSTADT