Formal Accountability for Biometric Surveillance: A Case Study

Vinh Thong Ta

University of Central Lancashire, UK

vtta@uclan.ac.uk

Joint work with

Denis Butin

Technische Universität Darmstadt, Germany

Daniel Le Métayer

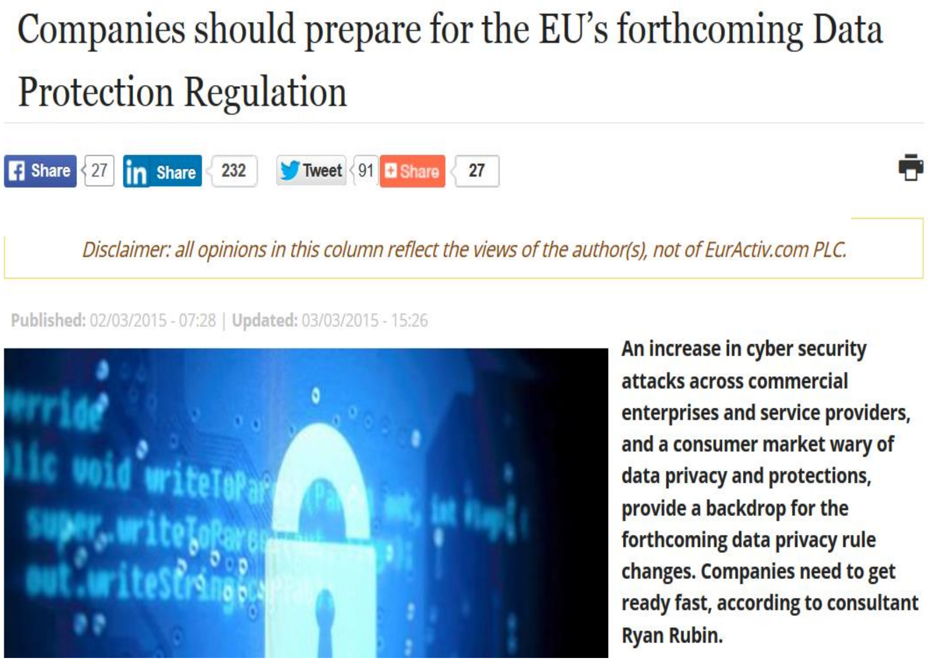
INRIA, France

APF 2015, October 7-8, Luxembourg

Motivation

Planned EU data protection reform (General Data Protection Regulation)

"Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data"

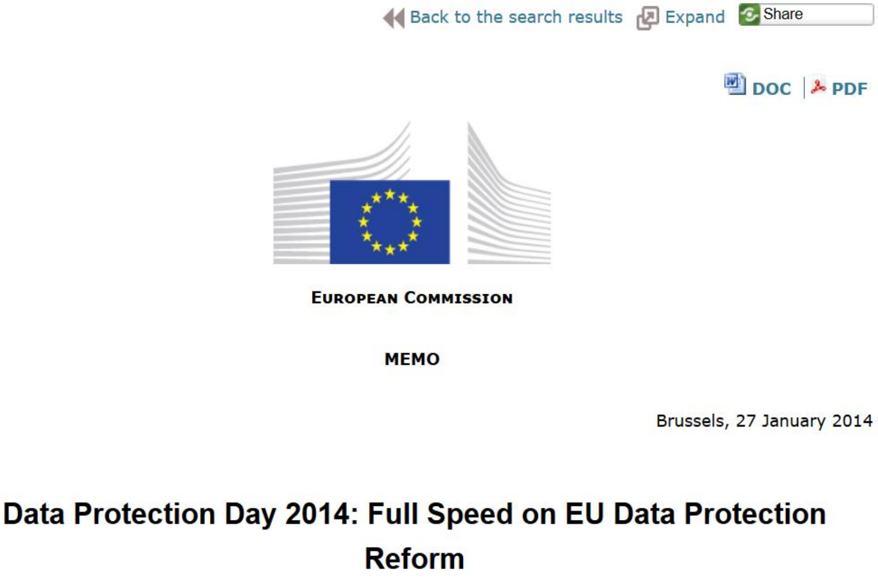


Companies should prepare for the EU's forthcoming Data Protection Regulation

Disclaimer: all opinions in this column reflect the views of the author(s), not of EurActiv.com PLC.

Published: 02/03/2015 - 07:28 | **Updated:** 03/03/2015 - 15:26

An increase in cyber security attacks across commercial enterprises and service providers, and a consumer market wary of data privacy and protections, provide a backdrop for the forthcoming data privacy rule changes. Companies need to get ready fast, according to consultant Ryan Rubin.



EUROPEAN COMMISSION

MEMO

Brussels, 27 January 2014

Data Protection Day 2014: Full Speed on EU Data Protection Reform

Motivation

Planned EU data protection reform (General Data Protection Regulation)

> *“Regulation of the European Parliament and of the Council on the protection*
> *of individual*
> *nd on the free*
> *movement o*

Privacy-by-Design

Accountability-by-Design

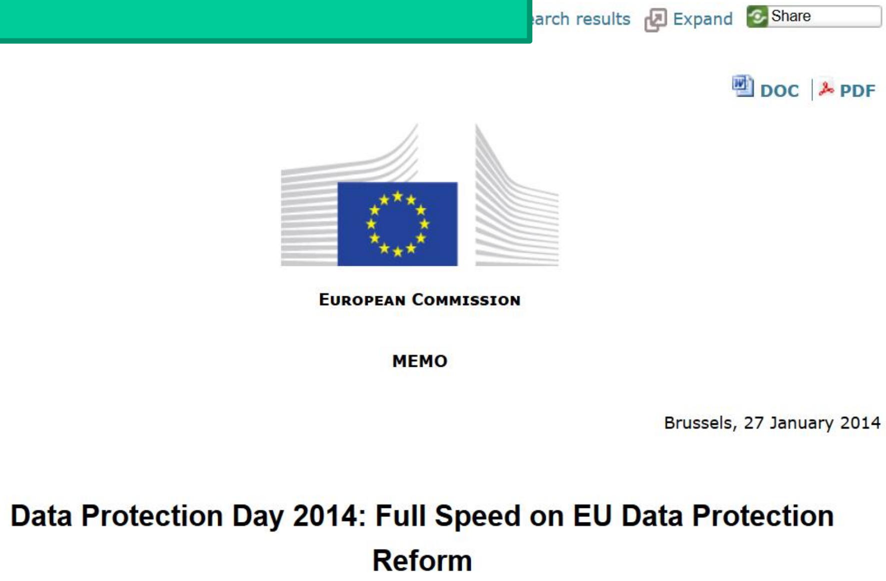
Companies should

Protection Regulati

Disclaimer: all opinions in this column reflect the views of the author(s), not of EurActiv.com PLC.

Published: 02/03/2015 - 07:28 | **Updated:** 03/03/2015 - 15:26

An increase in cyber security attacks across commercial enterprises and service providers, and a consumer market wary of data privacy and protections, provide a backdrop for the forthcoming data privacy rule changes. Companies need to get ready fast, according to consultant Ryan Rubin.



EUROPEAN COMMISSION

MEMO

Brussels, 27 January 2014

Data Protection Day 2014: Full Speed on EU Data Protection Reform

Our focus : accountability

- *Accountability* of Data Controller (DC)
  - an approach to sustain/support privacy

- The Article 29 Data Protection Working Party - Opinion 3/2010 on the principle of accountability
  - Accountability is defined as the duty
    - for DC to put in place measures guaranteeing the privacy of Data Subjects (DS),
    - and for these measures to be verifiable…
      - by independent third parties or by agents (or by the DS themselves).

… and accountability of practice

- Three types of accountability are distinguished in the literature:
  - *accountability of policy*
  - *accountability of procedures*
  - *accountability of practice*
    - Data Controllers ought to demonstrate that their actual data handling complies with their obligations.

Links among accountability, privacy policies and log compliance

Accountability of practice from the DC's point of view requires

- providing a history of system events
  - in practice, this is provided by *logs*
- a precise technical definition of what compliance means
  - this is done by using *machine-readable privacy policies*

Once these two "ingredients" are provided, they can both be used as parts of a log analyser.

Our focus : Accountability of Biometric surveillance systems

Inspired by

SEVENTH FRAMEWORK PROGRAMME

PARIS

PRIVACY PRESERVING INFRASTRUCTURE FOR SURVEILLANCE

TRIALOG (Co-ord)

VISUAL TOOLS

THALES

inria informatics mathematics

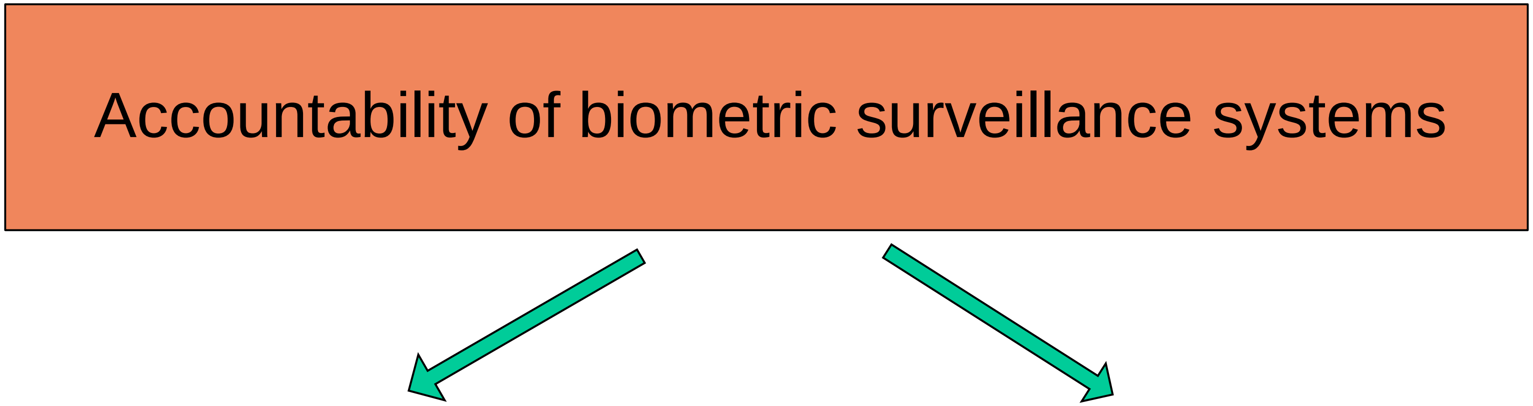
KU LEUVEN iMinds SECURITY DEPT icri

UNIVERSIDAD DE MÁLAGA

crids CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

Motivation Behind Formal Approach

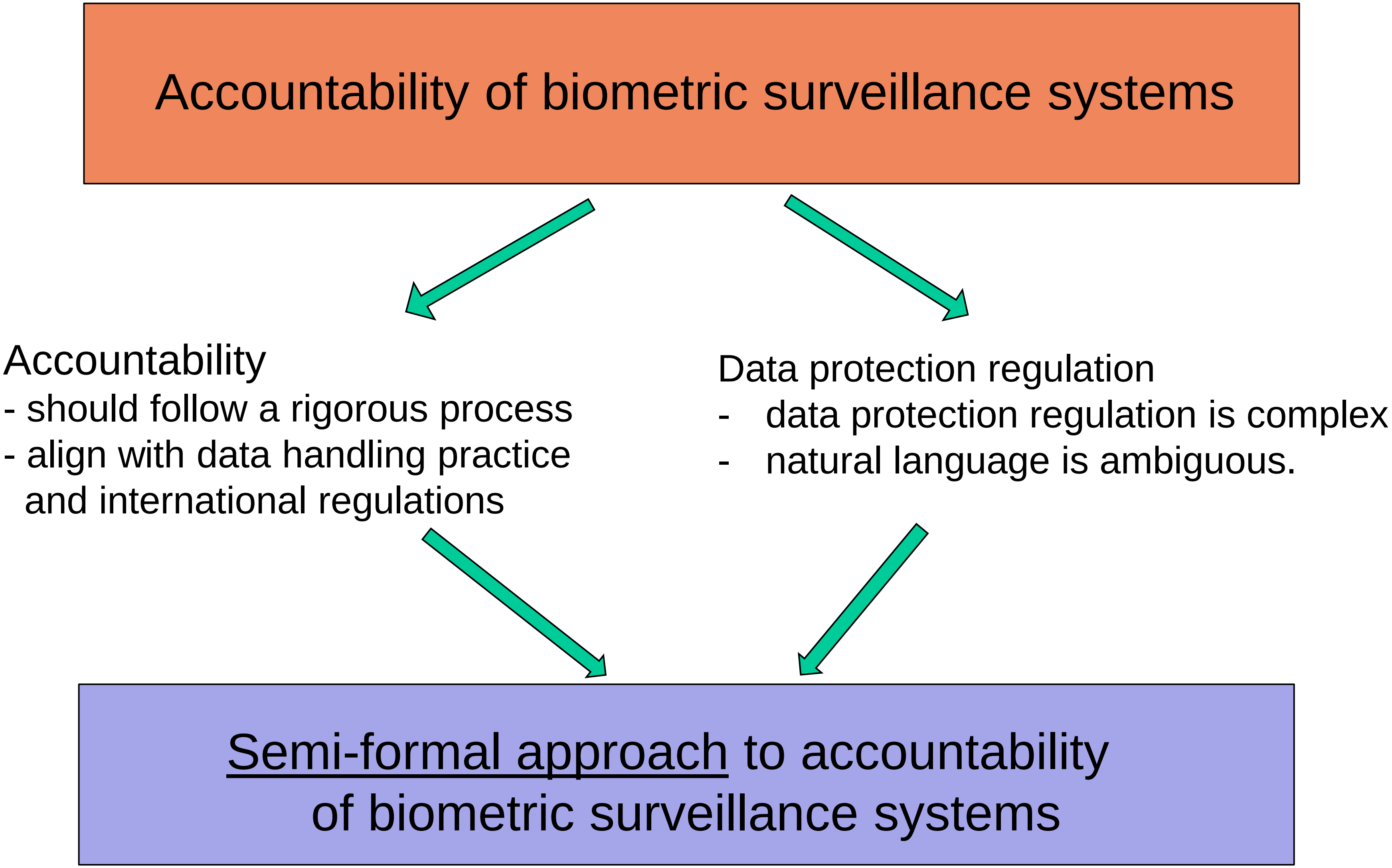


Accountability of biometric surveillance systems

Accountability
- should follow a rigorous process
- align with data handling practice and international regulations

Data protection regulation
- data protection regulation is complex
- natural language is ambiguous.

Motivation Behind Formal Approach



Accountability of biometric surveillance systems

Accountability
- should follow a rigorous process
- align with data handling practice and international regulations

Data protection regulation
- data protection regulation is complex
- natural language is ambiguous.

Semi-formal approach to accountability of biometric surveillance systems

Our Main Contributions

1. Demonstrate the practical application of a semi-formal framework for accountability to a real-world bodyprint-based surveillance system.
   - To the best of our knowledge this is the first work of such kind…

2. Our semi-formal approach is based on the work *“Butin, D., Le Métayer, D.: Log Analysis for Data Protection Accountability. 19th International Symposium on Formal Methods (FM 2014)”*

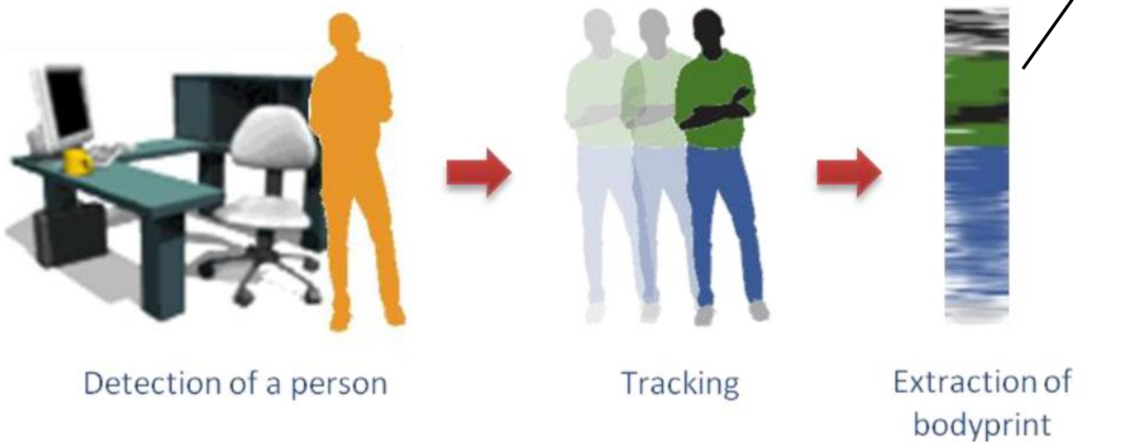
   - Proposed a generic privacy policy language, and links between high-level policy and low-level system logs.

   - We tailored this privacy language to make it suitable for our case study.

Real-world biometric surveillance system

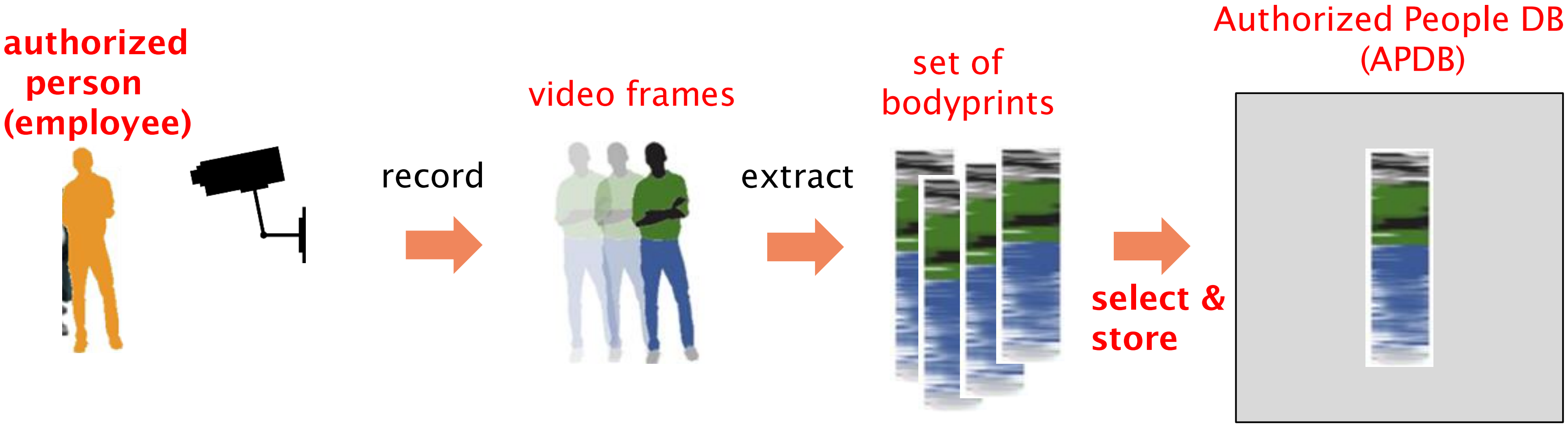
Deployed by Visual Tools Inc. (Madrid, Spain)

- detecting unauthorized people in their office during non-working hours.
- the capture and processing of the video frames, images, bodyprints, may raise major privacy concern.
- Spanish data protection law.



Bodyprint is based on
- width
- height
- clothes colour

Enrolment Phase



authorized person (employee)

record

video frames

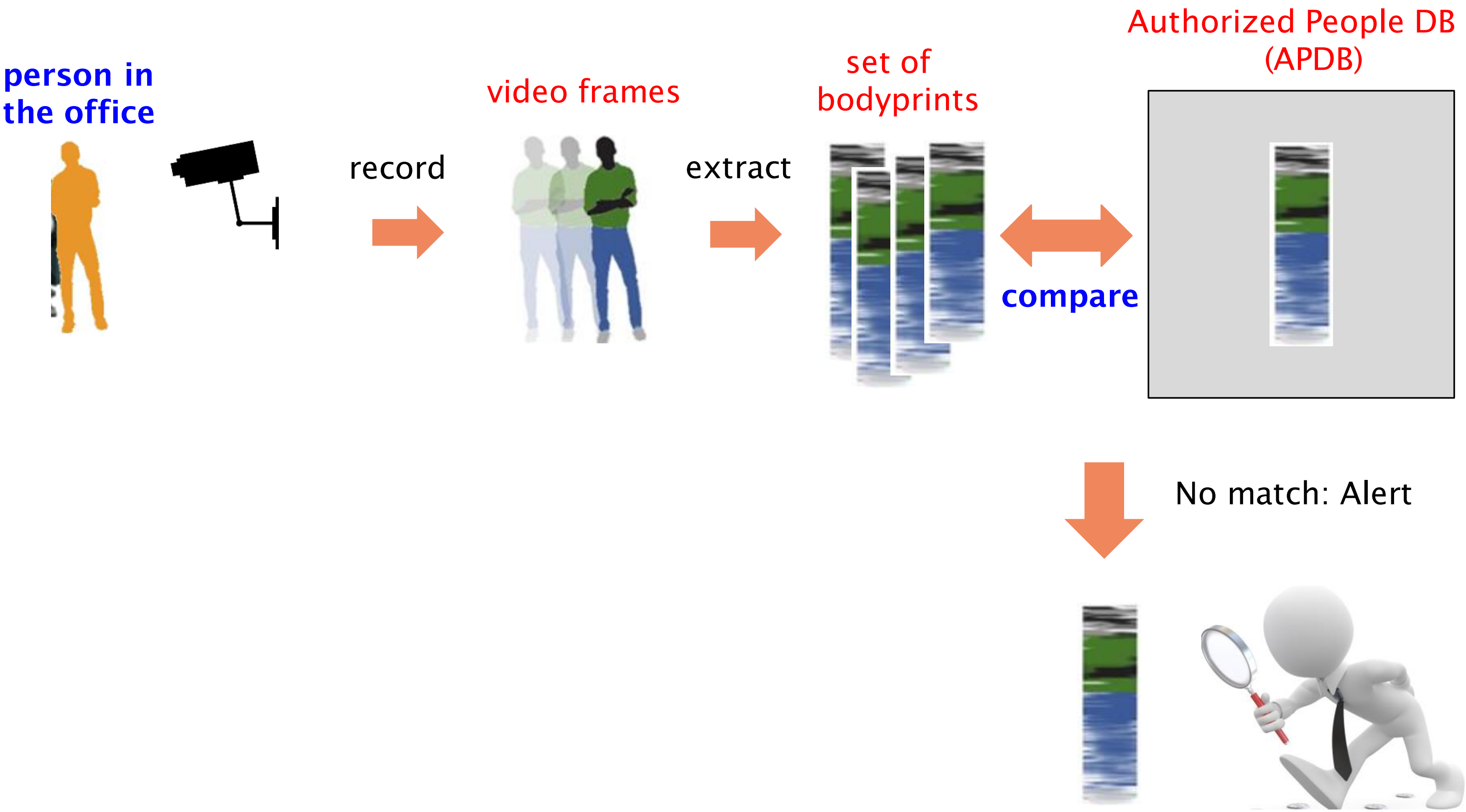
extract

set of bodyprints

select & store

Authorized People DB (APDB)

Matching Phase



person in the office

record

video frames

extract

set of bodyprints

compare

Authorized People DB (APDB)

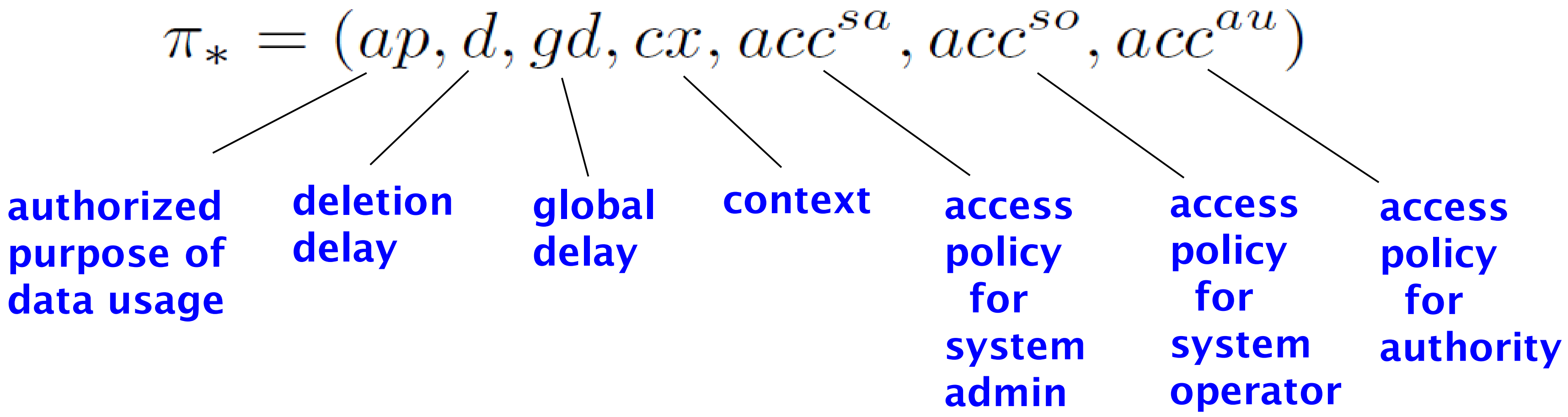
No match: Alert

System Operator (SO)
System Admin (SA)
Authority (Au)

Semi-formal approach on accountability of the bodypint-based surveillance system

Privacy Policy Language - Syntax

Policy is defined for each type of personal data in the system



$$\pi_* = (ap, d, gd, cx, acc^{sa}, acc^{so}, acc^{au})$$

authorized purpose of data usage

deletion delay

global delay

context

access policy for system admin

access policy for system operator

access policy for authority

Policies for the surveillance system (Extract)

Policy for recorded videos during enrolment phases

$$\pi_{ev} = (\{``\mathit{Enrol}", ``\mathit{Extract}"\}, \underbrace{\text{1 min, 1 month}}_{\textit{Based on Spanish data protection law}}, \{\text{DC Building}\}, \downarrow_{auth}, \uparrow, \downarrow_{auth})$$

Policy for recorded videos during matching phases

$$\pi_{mv} = (\{``\mathit{Match}", ``\mathit{Extract}"\}, \text{1 min, 1 month}, \{\text{DC Building, 21:00/07:00}\}, \uparrow, \uparrow, \uparrow)$$

Abstract Events

To reason about

- personal data handling activities
- accountability compliance properties

Capture specific actions occurring during system execution.

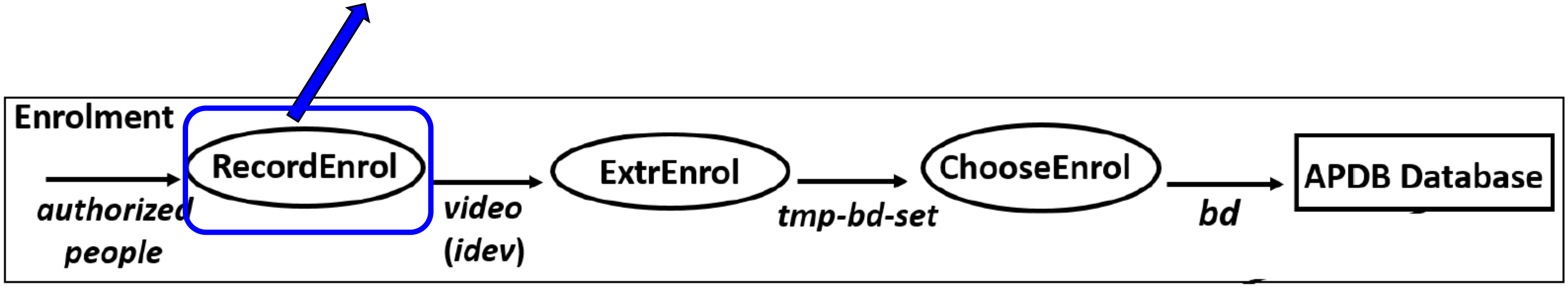
Abstract away from system internals such as writing and reading from memory addresses.

Cover all operations that can have an impact on the compliance of the system with respect to any privacy policy.

We defined 14 events

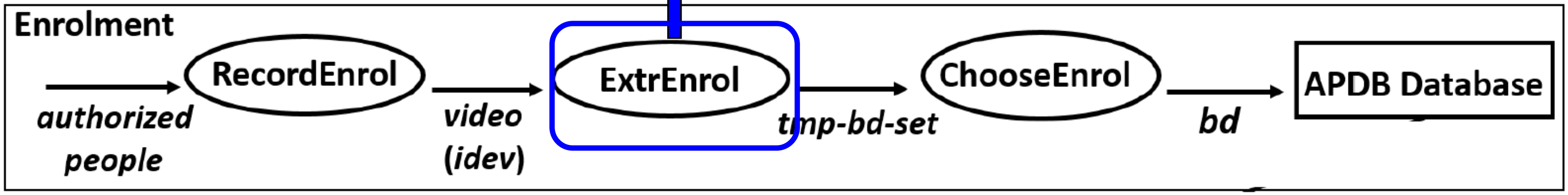
Abstract Events – Enrolment (Excerpt)

$$E_1\colon\ (\mathit{RecordEnrol},\ t,\ \mathit{cam},\ \mathit{enr\text{-}video\text{-}type},\ \mathit{video},\ \mathit{idev},\ \pi_{ev})$$



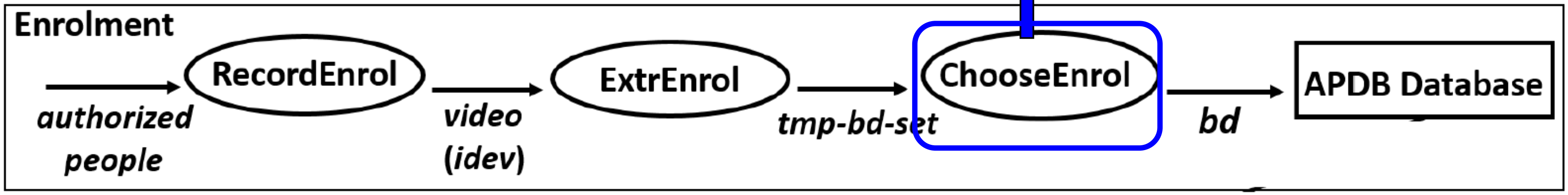
Abstract Events – Enrolment (Excerpt)

$$E_3\colon\ (\mathit{ExtrEnrol},\ t,\ \mathit{idev},\ \mathit{tmp}\text{-}\mathit{bd}\text{-}\mathit{set}\text{-}\mathit{type},\ \mathit{tmp}\text{-}\mathit{bd}\text{-}\mathit{set},\ \pi_{et})$$



Abstract Events – Enrolment (Excerpt)

$$E_5\colon\ (ChooseEnrol,\ t,\ idev,\ bd\text{-}type,\ bd,\ \pi_{ea})$$



Event Traces and Abstract state

Event Trace: *An event trace is a sequence of abstract events.*

⇒ they constitute a history of personal data handling events

Abstract state: *The abstract state of a system associated with data types and video IDs (Type, IDV) is a function*

(Type, IDV) -> Time x Cam x {Value} x Policy x P(Entity, N) x P(Entity, N) x P(Entity, N)

$$(enr\text{-}video\text{-}type, idev) \rightarrow (t, cam, \{video\}, \pi_{ev}, sa, so, aud)$$

Semantics of Events

$$\mathcal{S}_A : (Event \times \mathbb{N}) \rightarrow AbstractState \rightarrow AbstractState$$

Intuitively: State update caused by an event

Examples:

$$\mathcal{S}_A((RecordEnrol,\ t,\ cam,\ enr\text{-}video\text{-}type,\ video,\ idev,\ \pi_{ev})\ ,\ j)\sum = \sum[(enr\text{-}video\text{-}type,\ idev) \rightarrow (t,\ cam,\ \{video\},\ \pi_{ev},\ \emptyset,\ \emptyset,\ \emptyset)]$$

$$\mathcal{S}_A((Delete,\ t,\ idv,\ \theta,\ v),\ j)\sum = \sum[(\theta,\ idv) \rightarrow \bot]$$

Compliance of Event Traces

Captures the accountable operation of the biometric surveillance system

We defined 12 trace compliance properties.
Some examples:

- No data appears in an abstract state after the expiration of the global deletion delay.
- Data is used only for purposes defined in its policy.
- If the policy forbids all access to data, then there is none.
- Every access to the personal data must be preceded by the corresponding successful authentication.
- During enrolment, the deletion of a video must occur within the (specified) duration *d* after a corresponding set of (temporary) bodyprints has been extracted.

Compliant Traces Properties (Examples)

No data *idv* of type θ appears in an abstract state after the expiration of the global deletion delay.

$$A_1\colon\ State_A(\sigma, i-1)(\theta, idv) = (t, cam, \{v\}, \pi, so, sa, aud) \implies EvTime(\sigma_i) \leq t + \pi.gd$$

During enrolment, the deletion of a video must occur within the duration *d* after a corresponding set of (temporary) bodyprints has been extracted.

$$\begin{aligned} A_7\colon\ & \sigma_i = (ExtrEnrol, t', idev, tmp\text{-}bd\text{-}set\text{-}type, tmp\text{-}bd\text{-}set, \pi_{et}) \ \wedge \\ & State_A(\sigma, i - 1)(enr\text{-}video\text{-}type, idev) = (t, cam, \{video\}, \pi_{ev}, sa, so, aud) \implies \\ & \exists\ j \mid \exists\ t'' \mid \sigma_j = (Delete, t'', idev, enr\text{-}video\text{-}type, video) \ \wedge\ (t' < t'' \leq t' + \pi_{ev}.d) \end{aligned}$$

Trace Compliance Definition

Definition:
A trace is compliant if it satisfies all 12 properties $A_1, \ldots, A_{12}$.

- Can be used in practice by implementing a log analyser
  - a software tool taking as input a file containing a record of data handling events and outputting a Compliant / Non-compliant value.

- Data handling logs are files containing timestamped records of abstract events.
  - must be designed with compliance checking in mind to be usable.

Conclusion and Future Work

- We argue that a formal or semi-formal approach to accountability is important to reduce errors and ambiguity in the design of systems involving personal data.

- Provided the first case study on applying (semi) formal accountability framework to a biometric surveillance system.

- Not intended to be exhaustive, but rather to exemplify approach by addressing a number of key aspects of accountability in this context.

- This case study shows that our defined policy language, trace compliance properties and definition are suitable for compliance checking and log design in practice.

- Future works covering efficient automated compliance checking and log analyser tools based on our theoretical results.