Verifiable & Revocable Expression of Consent to Processing of Aggreg. Personal Data

Henrich C. Pöhls
Selling of Personal Data

Being able to buy personal data has made headlines ...

Source: news.bbc.co.uk/2/hi/europe/7572774.stm
Selling of Personal Data

Political reaction:

„Forbid the selling of personal data!“

... but the problem is: Missing Differenciator

Data buyers need to trust sellers to have the data subject‘s consent → no (automatic) verification

Proposal: Verifiable & revokable expression of consent

Goals: Allow identification of consented handling by all participating entities!

→ Reduce business value of illegally acquired data

→ Add transparency and allow automatic verification
Problemspace

Services store / process / forward personal data.

A Service is no single, monolithic entity:
→ Contains sub-services
→ Using several data providers
→ Cross-company relations

Service legally bound to data protection laws (EU, safe-harbour)
→ Requires „informed consent“ of the data subject
→ Retain a proof of this „informed consent“
Data Subject

Mr. Luxe
Data Subject & Data Items

- Year of birth
- Month of birth
- Day of birth
- First name
- Last name
- Gender
- Street number
- Street
- Town
- Country
- Telephone number
- Email
- IM address
- Photo
- Website URL
- Credit card details
- Political interests
- Hobbies
- Favorite music
- Nationality
Data Subject & Data Items

- Year of birth
- Month of birth
- First name
- Last name
- Gender
- Street number
- Street
- Town
- Country
- Credit card details
- Telephone number
- Email
- Day of birth
- Zip code
Data Subject & Data Items

- gender
- first name
- last name
- street
- street number
- zip code
- town
- country
- email
- telephone number
- credit card details
- day of birth
- month of birth
- year of birth

Mr. Luxe
Data Item: \( d_i = \{d_i\}_{ID} \parallel \{d_i\}_{VAL} \)

- One Data Item covers one semantic concept
- One Data Item can not be split further

Data Item is identifiable by name \( \{d_i\}_{ID} \)

- \( \{d_i\}_{ID} \) carries an agreed semantic meaning
- Data Item’s value is denoted \( \{d_i\}_{VAL} \)

Example:

last name: Luxe
Privacy Preference vs. Policy

Privacy Preference (\textit{ppref}) states restrictions under which the data subject allows data handling \rightarrow data subject‘s view

Privacy Policy (\textit{PPol}) states how service plans to handle data \rightarrow service‘s view

Assumed: Ontology for Privacy Policy and Preferences

Preference applicable to every Data Item

Example:
Data Set: All $d_i$ and $ppref_i$

gender  first name  last name

Mr. Luxe

e-mail  telephone  credit card

day of birth  month of birth  year of birth

street  number  zip code  town  country
Expression of Informed Consent

Consent to handle data according to privacy preferences is expressed by a digital signature:

- Signature applied to Data Set
- Signature protects integrity of $d_i$ and $ppref_i$

Verification: Signature verifiable with public-key

- Public-key attached $\rightarrow$ verifiable by all parties
- Public-key / ID linkage allows data subject identification (e.g. PKI)
Verification of Consent

All involved parties can verify expression of consent

Personal Data without verifiable consent is illegal to store, process, or further share

→ Unusable for legal business operations

→ No business-value (maybe even negative)

Note: No prevention of „un-consented“ operations, but

→ Adds: Detection & Transparency (think „logging“)

→ Additional: Access Controls, Encryption, DRM, ...
Allow Changes of Consent

Consent mostly not eternally given \( \rightarrow \) changes state

Possibility to vanish consent (think „revocation“):

- **time-limit:** established-until
- **online-status-checks:** consent status provider

Verifiable signature \( == \) consent established

non-verifiable signature \( == \) no consent

Expired/revoked signature \( == \) consent vanished
Allow „Changes“ within Data Set

Digital signatures allow to protect Integrity.

Holistic protection of Data Set always needed? **No.**

- Services‘ interactions require only partial Data Sets
- blank certain Data Items before transfer of data

Solution: Sign the root of a hash-tree

- Rebuild hash tree‘s root from provided hashes
- Blank any value by substitution with its hash
- Verification Rule: Ignore subst. hashes on paths with existing leaves
Data Set as a Tree: Flat

Mr. Luxe

day, month, year, gender, 1st name, last name, CC, tel, email, street, #, zip, town, country
Data Set as a Tree: Semantic
Data Set as a Tree: Binary

---

Mr. Luxe

day month year
gender 1st name last name
CC tel email
street # zip town country
Data Set’s Hash Tree

root

day  month  year  gender  1st name  last name  CC  tel  email  street  #  zip  town  country
Data Set’s Hash Tree
Data Set's Hash Tree
Blank (think „omit“) Data Items
Blank (think „omit“) Data Items

- day
- month
- year
- gender
- 1st name last name
- CC
- tel
- email
- street
- #
- zip
- town country
Blank (think „omit“) Data Items
Blank (think „omit“) Data Items

- day
- month
- year
- gender
- 1\textsuperscript{st} name
- last name
- CC
- tel
- email
- street
- #
- zip
- town country
Blank (think „omit“) Data Items
Linkage / Aggregation / Merging

s{root}
Linkage / Aggregation / Merging

s{root}

Diagram: A hierarchical structure with nodes labeled a, b, d, g, and h. The root node is highlighted.
Linkage / Aggregation / Merging

s\{root\}

+ c
Linkage / Aggregation / Merging

\[ s\{\text{root}\} \]

Diagram with nodes labeled a, b, c, d, g, h.
Linkage / Aggregation / Merging

\[ s_{\text{Luxe}}\{\text{root}\} \]

\[ + \]

\[ s_{\text{Luxe}}\{\text{root}\} \]
Linkage / Aggregation / Merging

\[ s\{\text{root}\} \]

- a
- b
- c
- d
- g
- h

✓
Linkage / Aggregation / Merging

\[ s\{\text{root}\} \]

\[ + \]

\( a \quad b \quad d \quad g \quad h \quad e \)
Linkage / Aggregation / Merging

s\{root\}

\[
\begin{array}{c}
 a \\
 b \\
 d \\
 e \\
 g \\
 h \\
\end{array}
\]
Linkage / Aggregation / Merging

\[ s_{\text{Luxe}}\{\text{root}\} \]

\[ s_{\text{Luxe}}\{\text{root}\} \]

\[ + \]

\[ s_{\text{Luxe}}\{\text{root}\} \]

\[ s_{\text{Luxe}}\{\text{root}\} \]
Linkage / Aggregation / Merging

\( s\{\text{root}\} \)
Linkage / Aggregation / Merging

s\{root\}

a b
d

+ z
g h
Linkage / Aggregation / Merging

{s\{root\}}

H. C. Pöhls 38
Linkage / Aggregation / Merging

\[ s_{\text{Luxe}} \{ \text{root} \} \]

\[ + \]

\[ s_{\text{Luxe}} \{ \text{root} \} \]

\[ \begin{array}{c}
  a \\
  b \\
  d \\
  g \\
  h \\
\end{array} \]

\[ \begin{array}{c}
  x \\
  z \\
\end{array} \]
Linkage / Aggregation / Merging

\[ s_{\text{Luxe}} \{ \text{root} \} \]

\[ \times \]

\[ s_{\text{Luxe}} \{ \text{root} \} \]

\[ \times \]

\[ \text{x} \]

\[ \text{z} \]
Linkage / Aggregation / Merging

\[ s\{\text{root}\} \]

Diagram showing a rooted tree with nodes labeled a, b, and d, and additional nodes labeled ppref, ID, and VAL.
Linkage / Aggregation / Merging

Blanking within Data Item level
Interaction during Verification

(1) Mr. Luxe

(2a) Verify

(3) Sub-Service

(4a) Online State Service (optional)

(4) Verify

(5) Service
Properties

Verifiable consent through digital signatures.

Mechanisms to update status + allow logging.

- Implementable re-using PKI mechanisms (X.509 Certificates, Validity Period, OCSP)

Allow Blanking of Data while still retaining verifiable consent.

Data Items can be blanked arbitrarily → no data subject interaction.

Merging bound by tree’s structure and service’s knowledge of substitution hashes.
Conclusion

Verification of informed consent (incl. privacy preferences) even on a partial Data Set

Verifiable informed consent on merged/linked data items from different sources originating from the same data subject

Data subjects control linkage through tree structure

Data subjects can vanish expression of consent

Data subjects get log and services get confirmation

Thanks.

Henrich C. Pöhls

henrich.poehls@uni-passau.de