LINDDUN GO

DistriNet

LINKABILITY

What?

Being able to sufficiently distinguish whether two IOI (items of interest) are linked or not, even without knowing the actual identity of the subject of the linkable IOI. [PH2010]

Tell me more!

Data items can be linked because they belong to the same data subject, with a certain probability.

Examples: web page visits by the same user, entries in two databases related to the same person, people related by a friendship link, etc.

Data items can also be linked because they share the same property.

Examples: linking people who visit the same restaurant, linking people with a similar disease, etc.

So what?

Can result in:

Inference [WP29]
Deduce information from a set of data items.

Singling out [WP29] **/ attribution**
isolate some or all records which belong to precisely one individual (without necessarily identifying).

Identifiability
Link data items to identity of data subject.

LINDDUN GO

LINKABILITY

FLOWS TO/FROM SYSTEM

INBOUND

The system can link personal data it receives to other data items

OUTBOUND

The receiving parties can link the personal data to other data items

DATA STORAGE

STORE

The system stores personal data that can be linked to data items (from the same or other databases)

RETRIEVE

The retrieved data can be linked to other data items

LINDDUN GO

IDENTIFIABILITY

What?

Being able to sufficiently identify the subject within a set of subjects (i.e. the anonymity set). [PH2010]

Tell me more!

Data items can be linked to the identity of the data subject, with a certain probability.

Examples: identifying the reader of a web page, the sender of an email, the person to whom an entry in a database relates, etc.

So what?

When personal data can be identified, they require even stricter security measures. Identified data can also result in unawareness and non-compliance issues.

IDENTIFIABILITY

FLOWS TO/FROM SYSTEM

INBOUND

The system can identify personal data it receives

OUTBOUND

The receiving parties can identify the received personal data

DATA STORAGE

STORE

The system stores personal data that can be identified

RETRIEVE

The retrieved data can be identified

LINDDUN GO

NON-REPUDIATION

What?

A data subject cannot deny they know, have done or have said something.

Tell me more!

There is evidence that can link the data subject to a certain action.

Examples: unable to deny being a customer of a certain webshop, unable to deny having filed a complaint, a user of an online voting system is unable to deny whom they voted for, etc.

Identifiability (and linkability) threats will increase the risk of non-repudiation.

Note that non-repudiation is actually a security goal. This should however not result in any conflicts, as (parts of) a system that requires non-repudiation as a security goal, should not need plausible deniability for the same data.

So what?

Non repudiation leads to data subject accountability: when a person is not able to repudiate an action or piece of information, he can be held accountable (e.g. a whistleblower can be prosecuted).

LINDDUN GO

NON-REPUDIATION

FLOWS TO/FROM SYSTEM

INBOUND

The sending party cannot deny use of the system

OUTBOUND

The receiver cannot deny receipt of a message

DATA STORAGE

STORE

The data subject cannot deny storage of their data

RETRIEVE

The retrieved data cannot be denied by the data subject

LINDDUN GO

DETECTABILITY

What?

Being able to sufficiently distinguish whether an item of interest (IOI) exists or not. [PH2010]

Tell me more!

Without having access to the data, the threat actor knows it exists. Existence of data is sufficient to infer more (sensitive) information.

Examples: By detecting that a celebrity has a health record in a rehab facility, one can infer the celebrity has an addiction, even without having access to the actual record.

So what?

Detectability can lead to the deduction of personal data. This information can be used to extend a data subject's profile (linkability) and/or identify the data subject.

DETECTABILITY

FLOWS TO/FROM SYSTEM

INBOUND

OUTBOUND

An external party can detect in- or outbound communication

DATA STORAGE

STORE

Stored data can be detected

RETRIEVE

Query responses reveal existence of data

LINDDUN GO

UNAWARENESS

What?

A data subject is unaware of, or unable to intervene in, the collection and further processing of their personal data.

Tell me more!

Unawareness relates to data subject rights and therefore focuses on transparency (or predictability) and intervenability (or manageability) threats.

Lack of transparency: a data subject is not aware of collection and/or processing of personal data related to them.

Examples: no notice is provided before collection, data subject is not informed of 3rd party sharing, etc.

Lack of intervenability: a data subject cannot access or manage their own personal data (including managing access settings).

Examples: data subject cannot access own data or cannot request rectification of data, data subject cannot (easily) update privacy settings, etc.

So what?

Unawareness leads to a violation of fundamental data subject rights.

UNAWARENESS

FLOWS TO/FROM SYSTEM

INBOUND

There is a lack of transparency and intervenability provided to the data subject at collection time

DATA STORAGE

STORE

A data subject cannot sufficiently intervene in their stored data

PROCESS

PROCESS

There is a lack of transparency and intervenability provided to the data subject w.r.t. the processing of personal data

LINDDUN GO

NON-COMPLIANCE

What?

The system does not comply with data protection principles.

Tell me more!

Data protection processing principles include:

- purpose limitation
  only collect and process data for the pre-determined purpose
- Proportionality
  Only collect and process the minimal set of data required for the purpose
- Storage limitation,
  Only store data for as long as required for the purpose
- ...

Note that this category is mainly influenced by EU's GDPR, but the general principles apply independent of a specific region or legislation.

So what?

Data protection principles are designed to protect the data subjects' privacy. They should always be implemented.
In addition, violation of these legal obligations can result in large fines and reputation damage.

NON-COMPLIANCE

FLOWS TO/FROM SYSTEM

INBOUND

Data protection principles are violated at collection time

DATA STORAGE

STORE

Storage of data is not limited to its minimum requirements (duration + amount of data)

PROCESS

PROCESS

Processing activities lack lawful ground and/or purpose, or other data protection principles

LINDDUN GO