

DPSN International Data
Protection Day work-in-
progress event on Friday
27th January 2023 online

The Data Protection Law Scholars
Network



Stream 2!



Challenges faced by controllers in post-breach risk evaluation

Lina Jasmontaite (VUB LSTS)

Challenges faced by controllers in post-breach risk evaluation(1/2)

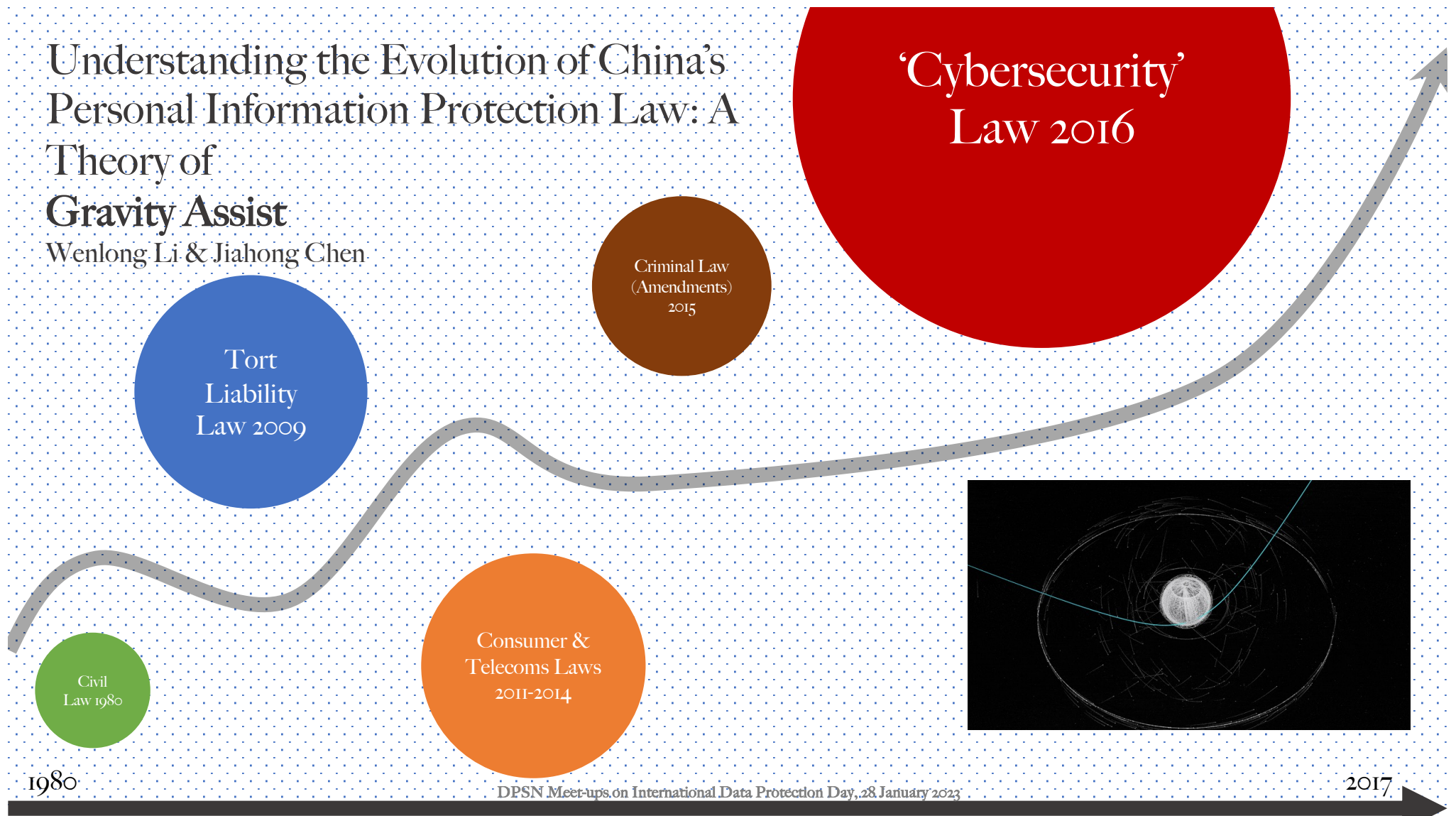
- Obligation to conduct post-breach risk evaluation
- Reasons that make post-breach risk evaluation challenging
 - 5 observations based on 42 DPA decisions

Challenges faced by controllers in post-breach risk evaluation (2/2)

- A personal data breach affects the basic categories of personal data
 - A small number of individuals are affected
- Not taking into account the state of the art of available technology that could allow misuse (and abuse) of leaked data
 - Relying exclusively on third party questionnaires and on the existing methodologies to evaluate the consequences of a personal data breach
 - No harm occurred to affected individuals

Understanding the Evolution of China's Personal Information Protection Law: A Theory of Gravity Assist

Wenlong Li & Jiahong Chen

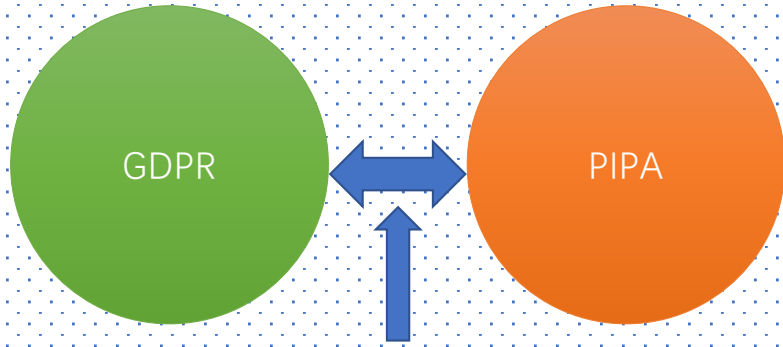


1980

DPSN Meet-ups on International Data Protection Day, 28 January 2023

2017

Brussels Effect in China?

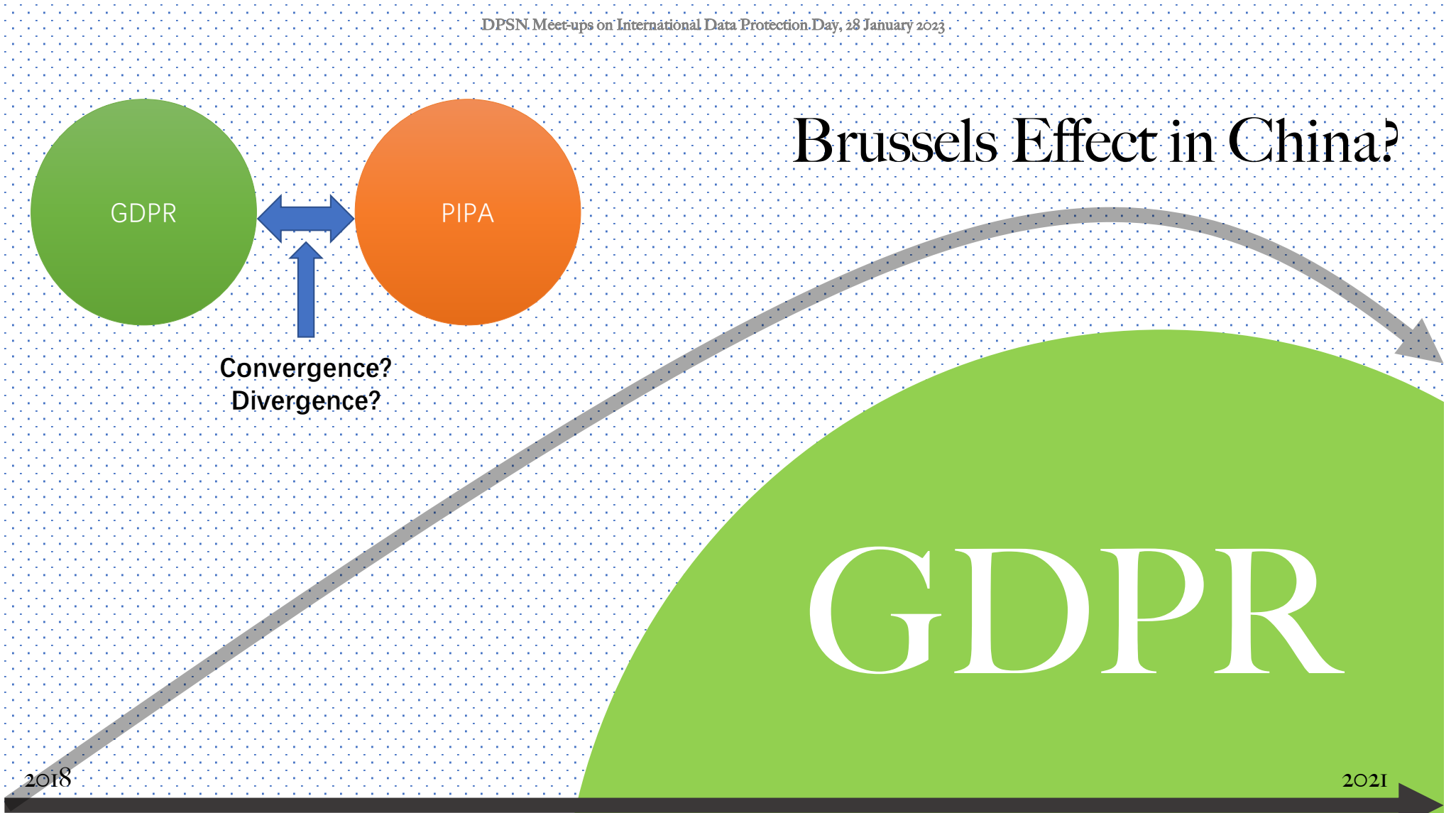


Convergence?
Divergence?

GDPR

2018

2021



'Post-GDPR' Developments and the future of China's PIPL

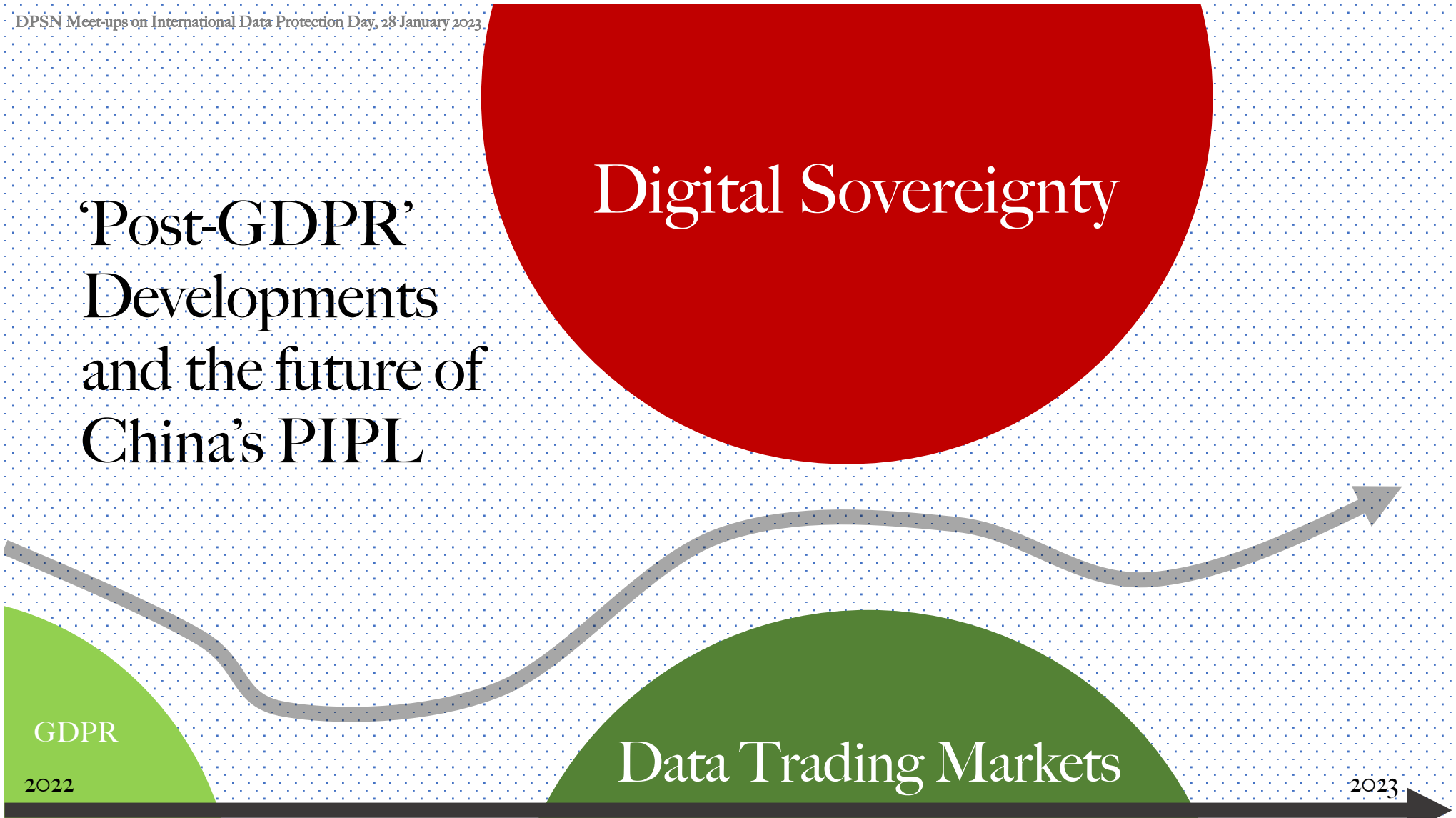
Digital Sovereignty

GDPR

2022

Data Trading Markets

2023





User empowerment at the cost of privacy – **DIGITAL IDENTITY WALLETS**

SANNA TOROPAINEN, PH.D CANDIDATE

UNIVERSITY OF HELSINKI, LEGAL TECH LAB

19.01.2023

EU Digital Identity Wallet **EUDIW**

- Does the EUDIW democratize digital identity or create new inequalities when the **responsibility of assessing privacy risks is on the user**, regardless their digital literacy or vulnerability?
- Electronic **identification and authentication** + **selective sharing**
- **REGULATION**
 - Proposal for European Digital Identity Regulation (COM/2021/281)
 - Revision of the eIDAS (910/2014)

Research

PART 1 **DOGMATIC RESEARCH**

- Mapping **legal safeguards** to protect privacy and personal data of EUDIW users
- Reflecting the theory of legal personhood (*Lindroos-Hovinheimo, Private selves*)
- Expecting tension between selective sharing and **data minimisation principle**

PART 2 **EMPIRICAL RESEARCH**

- Contribution to empirical legal research with **computational methods**
- Analysing CJEU case law with topic modelling and/or **word embedding**

The Internet of Things, Cybersecurity, and Data Protection

27-1-2023 – Data Protection Scholars Network
Mattis van 't Schip
Ph.D. Candidate – Radboud University (iHub)

The Internet of Things: Struggles in the Industry

The Internet of Things industry

- **Rapid development of new products/series**
- **Quick product-to-market action**
- **Spreading processing power across various devices**

Leading to...

- **Cybersecurity problems**
- **Data protection issues**

Unfortunately...

- **A legal gap to address these issues**

Who is responsible?

My question: “To what extent are the various actors within the supply chain of an Internet of Things device legally responsible to take cybersecurity and data protection measures appropriate to their role?” (WIP)

An Internet of Things device is created by:



- **Software developers (cloud providers, operating system developers, etc.)**
- **Hardware manufacturers (watch components, battery components, etc.)**

Meanwhile, our existing legal frameworks address (inter alia):


- **Data processing (General Data Protection Regulation)**
- **Manufacturers, importers, and distributors (Radio Equipment Directive/*Proposal Cyber Resilience Act*)**

What about...


- **The *entire* supply chain (manufacturer to seller and user)**
- **Open-source developers (Log4j)**
- **And other involved actors?**




Legal Framework and Problems of Digital Surveillance in East Asian Democracies during COVID-19



Kuan-Wei Chen
(she/her)



Doctoral Student, Faculty of Law, Ludwig-Maximilians-Universität München
JSPS Fellowship, University of Tokyo



The extensive use of digital surveillance policies to control the COVID-19 epidemic in East Asian democracies has given rise to a number of questions related to data governance. This study critically compares the relevant policies and legalisations in Japan, Korea, Taiwan and Singapore.



Features of the Data Collection Systems



Mode

South Korea
Legislative Mode
-Existed Legal Framework
(MERS 2015)

Taiwan
Rolling Amendments by
Administrative Power

Singapore
Change of Administrative
Interpretation?

Japan
Voluntary Mode

Legal
Instrument

Contagious Disease Prevention
and Control Act
v.
Personal Information
Protection Act
+
Act on the Protection and Use
of Location Information

CDC Act (SARS 2002) + COVID-
19 Act

Art 7 COVID-19 Act :
The Commander of the Central
Epidemic Command Center
may, for disease prevention and
control requirements,
implement necessary response
actions or measures.

Police used the data from
TraceTogether App for criminal
cases
(which was not allowed)

No compulsory laws

Tracing
Method

Quarantine App +
Mobile Contact Tracing
(centralized, compulsory)
(7 categories)

Digital Fence (not GPS)+
SMS Real Name System
(centralised, compulsory) +
Social Distance App
(decentralised, voluntary)

Stay-Home Notice App (GPS)+
Safe Entry QR
(centralized, compulsory)+
TraceTogether App
(partially compulsory)

**COCOA (COVID-19
Contact App)**
(decentralized)+
LINE Survey
(voluntary)



Analysis & Review



Legal Basis

SK: Yes, but reasonable?
TW: too vague
SG: Substantive rule of law?



Principles

Accountability,
transparency, and access
to remedies



Stop Mechanism

Unclear
Data retention and
follow-up?



Sensitive Data and Discrimination

Cases of gay community
(SK),
sex worker community (TW)



Other Problems

Digital divide,
Out-of-purpose use,
Data leakage/ security,
...



Public-Private Partnerships

Compulsory?
In advance?



**GDPR and decentralized models
of data governance (Solid):
responsibility is where the shoe
pinches**



**Michiel Fierens, KU Leuven & Iris Vanwyck, Ghent
University**

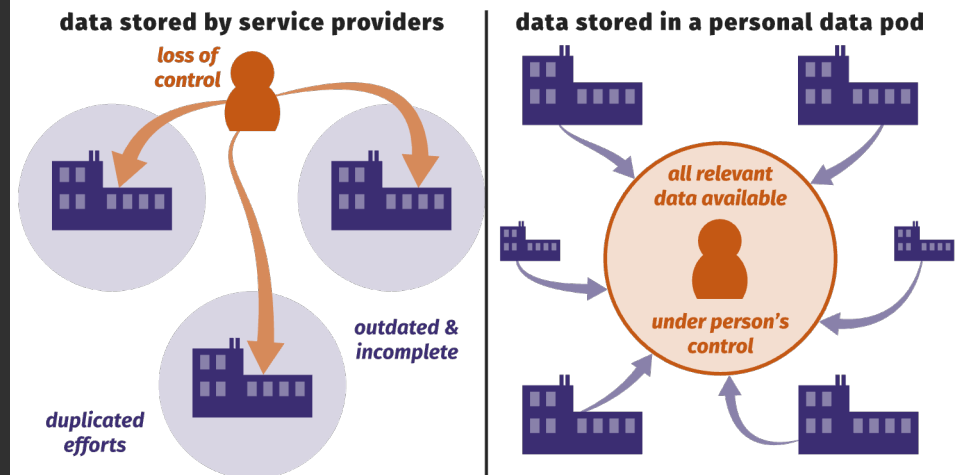
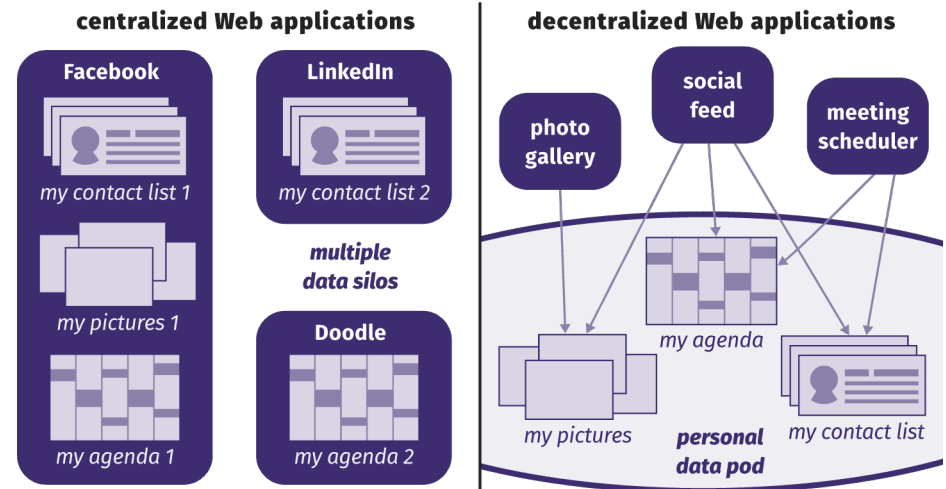
**Kimberly Garcia, University of St. Gallen
Harshvardhan J. Pandit, Dublin City University
Aurelia Tamò-Larrieux, Maastricht University**

Walled gardens of social media



Solid

- personal web server
- separating data from apps
- granular permissions
- interoperability (W3C)



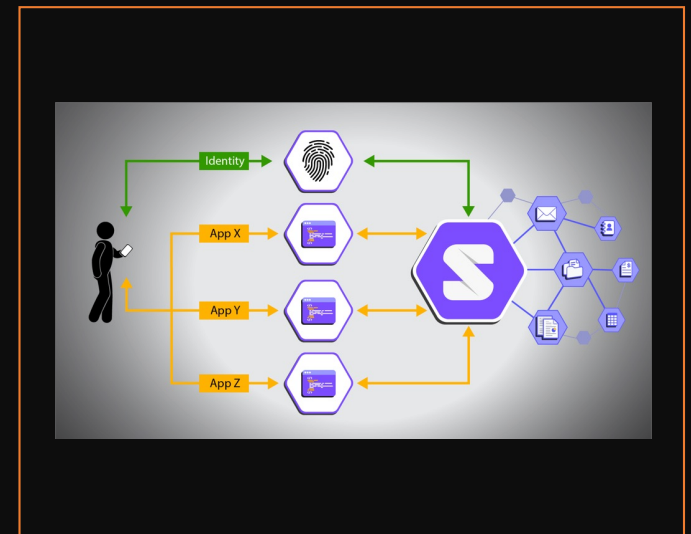
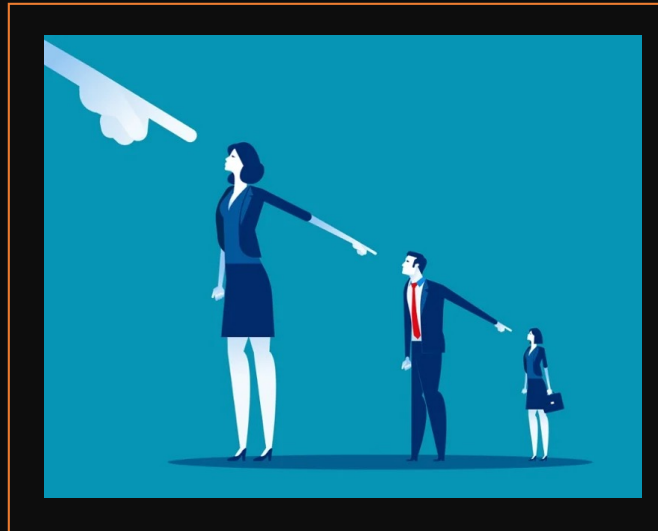
Interdisciplinary critical analysis

Controllership under the GDPR

~ Cloud Infrastructure (IaaS, PaaS, SaaS)

Responsibilities of the user?

Recommendations



GDPR and Synthetic Data Application in Medical Sector

Jarosław Greser (Warsaw University of Technology)

GDPR and Synthetic Data Application in Medical Sector 21

What is synthetic data?

Artificially generated information that maintains the attributes of the original data.

What it is used for?

Training AI algorithms e.g.: ChatGPT, deep fakes...

Synthetic Data Application in Medical Sector

22

Application in the medical sector:

1. preserving privacy;
2. augmentation of existing real datasets e.g. rare and orphan diseases;
3. clinical research;
4. predictive analysis.

GDPR and Synthetic Data

23

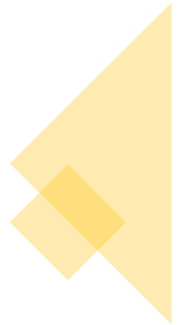
Main problem:

In theory: synthetic data is not personal data under art. 4 GDPR

In practice: the possibility of identification depends on the method of creation (tabular data is particularly susceptible)

Other problems:

1. the problem of noise in synthetic data – explainable AI (XAI), access to data
2. cybersecurity requirements – e.g. Regulation 2017/746
3. Regulation on free flow of non-personal data - scope of application?
4. data governance regulations - AI Act vs. DGA vs. Data Act



Secondary Use of Health Data: A Comparative Analysis of GDPR and European Health Data Space

Fatma Sümeýra Dođan
PhD Researcher





- The re-use of health data that were collected initially in the context of providing care, but which may later be re-used for another purpose. This is referred to as a “secondary use.”¹
- The term ‘secondary use’ is not found in the GDPR, but it is to be understood as being broadly in line with the term ‘further processing’ of data as described in the purpose limitation principle set out in Article 5(1)(b).

¹ European Commission, Johan Hansen, Petra Wilson, Eline Verhoeven, et al., ‘Assessment of the EU Member States’ rules on health data in the light of GDPR’ (2021).

European Health Data Space

- Proposal for harmonized health data governance in EU
- Also, doesn't offer a definition of secondary use
- The interplay between the EHDS and GDPR is the main crux of this study

Article 34

Purposes for which electronic health data can be processed for secondary use

Health data access bodies shall only provide access to electronic health data referred to in Article 33 where the intended purpose of processing pursued by the applicant complies with:

- (g) training, testing and evaluating of algorithms, including in medical devices, AI systems and digital health applications, contributing to the public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices;

85. **First**, the EDPB and the EDPS note a lack of proper delineation of the purposes listed under Article 34 (1) of the Proposal for which electronic health data may be further processed, and in particular express concern with regards to Articles 34(1)(f) and (g) of the Proposal, which possibly encompass **any form of** 'development and innovation activities for products or services contributing to public health or social security' or 'training, testing and evaluation of algorithms, including in medical devices, AI systems and digital health applications, contributing to public health or social security'. The EDPB and the EDPS strongly recommend for the Proposal to further delineate these purposes and circumscribe when there is a sufficient connection with public health and/or social security, in order to achieve a balance adequately taking into account the objectives pursued by the Proposal and the protection of personal data of the data subjects affected by the processing.

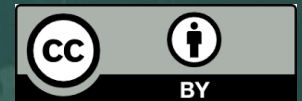
Protect

Altruistic (Re-)Use of Health Data through Semantic Policies

Beatriz Esteves, Ontology Engineering Group, Universidad Politécnica de Madrid
beatriz.gesteves@upm.es | besteves4@eupolicy.social

2nd DPSN International Data Protection Day

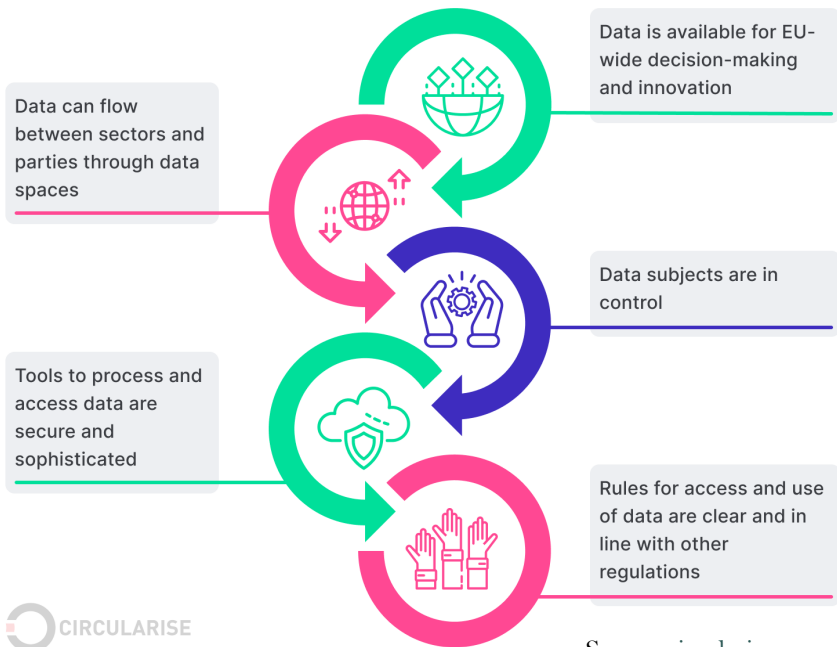
This project has received funding from
the European Union's Horizon 2020 research
and innovation programme under grant
agreement No 813497.



Motivation



European strategy for data



Sharing data for altruistic purposes



Data Holder

- Government
- Individuals
- Business

Intermediary

Data User

- Business
- Research

European Data Spaces

- | | | |
|---------------|-----------------------|--------------------|
| Manufacturing | Finance | Agriculture |
| Green Deal | Health | Open Science Cloud |
| Mobility | Public administration | Energy |
| | | Skills |

Extending DUO with ODRL and DPV for Health Data Sharing



<https://w3id.org/duodrl/repo>

H. J. Pandit, B. Esteves (2022). Enhancing Data Use Ontology (DUO) for Health-Data Sharing by Extending it with ODRL and DPV. Under review in the Semantic Web Journal. <http://www.semantic-web-journal.net/system/files/swj3127.pdf>

```
:Offer2 a odrl:Offer ;
  rdfs:label "Offer to use dataset using GDPR's Explicit Consent, and requiring a DPIA" ;
  odrl:target <https://example.com/Dataset> ;
  odrl:action dpv:Use ;
  dpv:hasApplicableLaw dpv-geo:GDPR ;
  odrl:permission [
    odrl:constraint [
      odrl:leftOperand dpv:hasLegalBasis ;
      odrl:operator odrl:isA ;
      odrl:rightOperand dpv-gdpr:A6-1-a-explicit-consent ] ] ;
  odrl:permission [
    odrl:constraint [
      odrl:leftOperand dpv:hasOrganisationalMeasure ;
      odrl:operator odrl:isA ;
      odrl:rightOperand dpv:DPIA ] ] ;
```

Future Work

- Extend DPV with concepts from the Data Governance Act, Data Act, AI Act, ePrivacy, Data Spaces, ...
- Extend Proof-of-Concept implementation to determine access to health data stored in personal data vaults such as Solid, OwnYourData, ...