Key note: The subtle differences between privacy risk and privacy breach consequences

18th IFIP Summer School on privacy and identity management, University of Oslo, Norway

Prof. Dr. Lothar Fritsch **09.Aug.2023**

OSLO METROPOLITAN UNIVERSITY
STORBYUNIVERSITETET

OSLOMET

The 28th Nordic Conference on Secure IT systems (NordSec) 2023 will be hosted by OsloMet in Norway on Nov. 16-17, 2023.

Nordic Conference on Secure IT Systems

NordSec is an annual research conference series that has been running since 1996. The NordSec conferences address a broad range of topics on IT security. The events bring together security researchers from the Nordic countries, Northern Europe, and beyond. In addition to being a venue for academic publishing, NordSec is an important meeting place for university faculty, students, and industry researchers and experts from the region.

NordSec addresses a broad range of topics within IT security with the aim of bringing together computer security researchers and encouraging interaction between academia and industry.

Key note: The subtle differences between privacy risk and privacy breach consequences

18th IFIP Summer School on privacy and identity management, University of Oslo, Norway

Prof. Dr. Lothar Fritsch **09.Aug.2023**

OSLO METROPOLITAN UNIVERSITY
STORBYUNIVERSITETET

OSLOMET

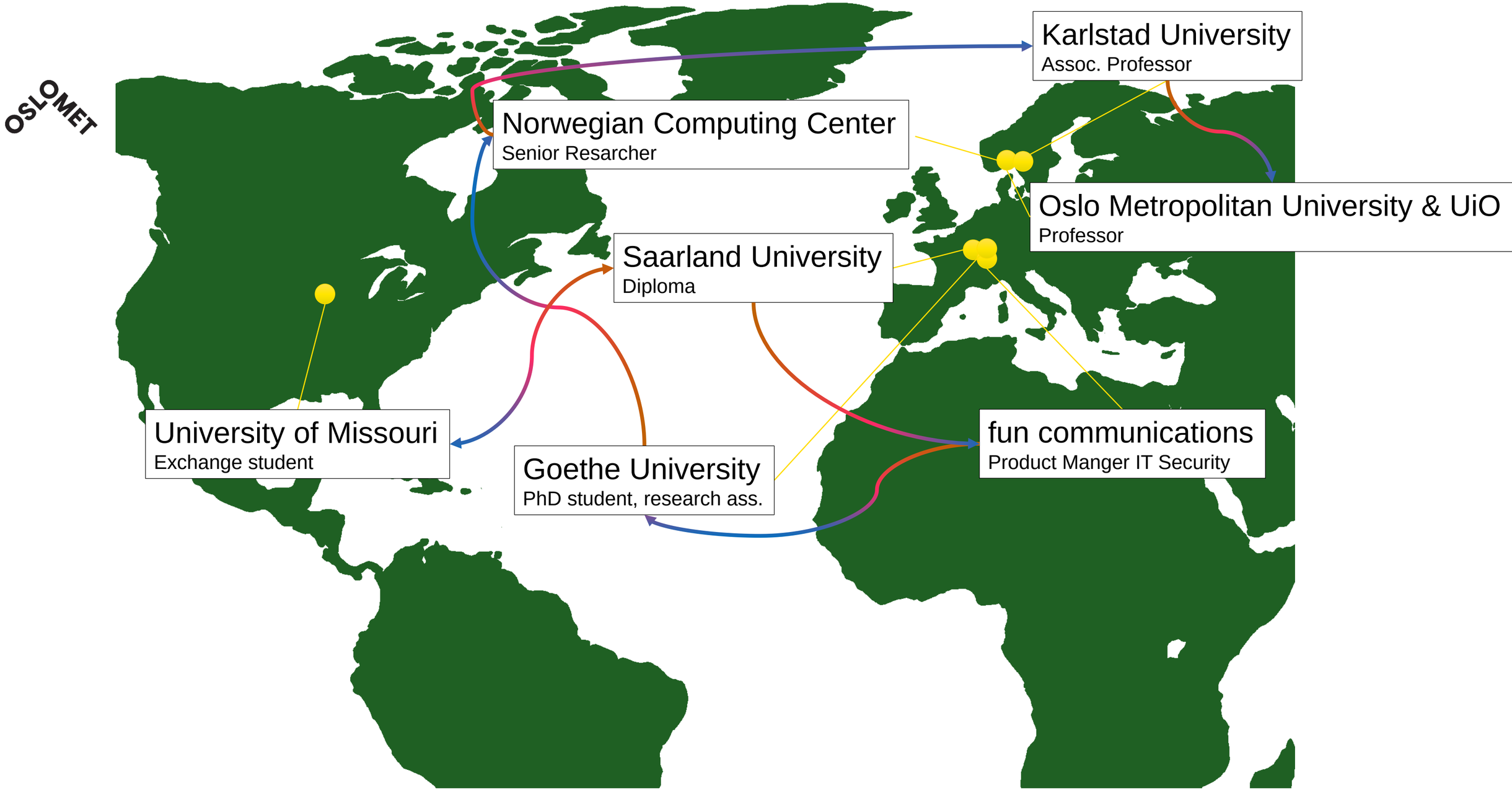
Lothar Fritsch is professor for Applied Cybersecurity at Oslo Metropolitan University and associate professor at University of Oslo. His areas of interest are information privacy, identity management, cyberwar, privacy technology, privacy risk assessment, and general cybersecurity topics.

Lothar has been part of pan-European research projects on privacy and identity management, and has worked on topics such as privacy enhanding technology, privacy risk analysis, and human factors in information security.

He teaches and supervises in many areas of computer science, among others Internet of Things, network security and Privacy by Design. He supervises PhD students, and bachelor and master thesis projects, in collaboration with industry, associations and public organizations.

lotharfr@oslomet.no

… or find me on LinkedIN!


OSLOMET
Karlstad University
Assoc. Professor
Norwegian Computing Center
Senior Resarcher
Oslo Metropolitan University & UiO
Professor
Saarland University
Diploma
University of Missouri
Exchange student
Goethe University
PhD student, research ass.
fun communications
Product Manger IT Security

This talk will examine the concept of privacy risks and their consequences. It will present the various perspectives and what they actually capture, or neglect. Listeners will gain a better understanding on risks and consequences of personal data breaches, and about the maturity of the assessment methods used to assess such risks.

Name privacy risks, please!

What about «data protection impact»?

Data breach consequences?

Concepts

- Risk Analysis – chance of event happening, and damage caused
- DPIA – Which risks to fundamental data protection rights may be created by data processing application?
- Privacy Risk Analysis – try to assess risk of data breaches occuring on systems, and mitigate or lower occurence of risk.
- Impact / consequences? Which ones? For whom?

Qualitative risk assessment

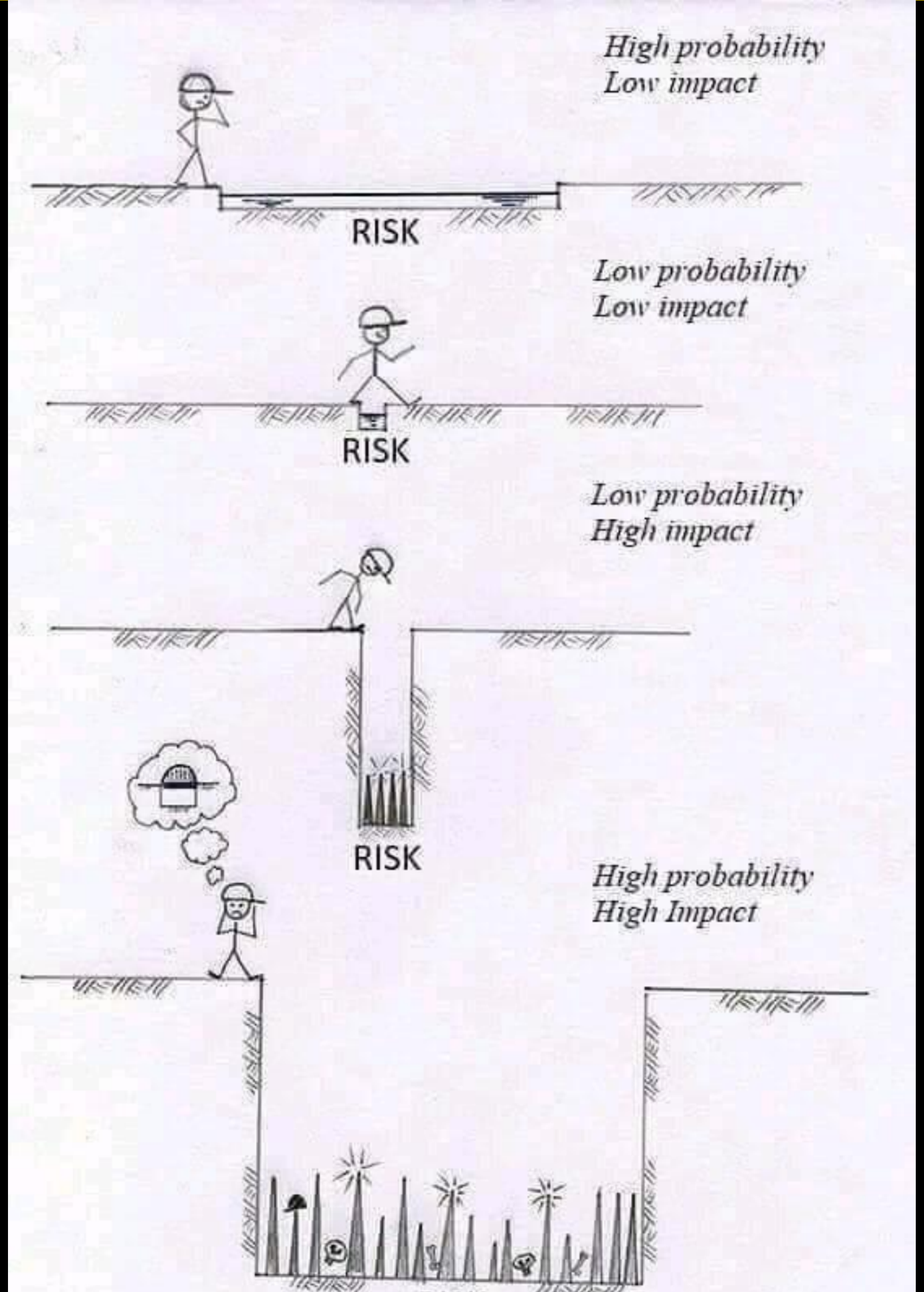
- Uses likelihood and impact of events on assets
- Based on historic data for both likelihood and impact
- In new settings often guesswork

Loss(A) = impact(T(A))*likelihood(T(A)) where T(A) is threat T effective on asset A.

Risk assessment form

Likel / Imp	Negli	V low	Low	Med	High	V High	Extr
None							
Minor							
Med							
High							
V High							
Extr							

Three levels of risk are normally adequate: low, moderate, high


High probability
Low impact
RISK
Low probability
Low impact
RISK
Low probability
High impact
RISK
High probability
High Impact

DPIA

- The DPIA process aims at providing assurance that controllers adequately address privacy and data protection risks of ‘risky’ processing operations. By providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs help organisations to comply with the requirement of ‘data protection by design’ where it is needed the most, i.e. for ‘risky’ processing operations.
- The assessment shall contain at least:
  1. a systematic description of the envisaged processing operations and the purposes of the processing;
  2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
  3. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1 of Article 39 of the Regulation 2018/1725; and
  4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Source: Data Protection Impact Assessment (DPIA) | European Data Protection Supervisor (europa.eu)

DPIA - Article 39 of the Regulation 2018/1725

Article 39

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

"the risks to the rights and freedoms of data subjects referred to in paragraph 1" ???

Please help me interpret the 39.1! What does it actually say?

DPIA - Article 39 of the Regulation 2018/1725

Article 39

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Data processing likely results in high risks to persons → Taking into account the nature, scope, context and purposes of processing → Assess impact of processing on protection of personal data

ICO DPIA template

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

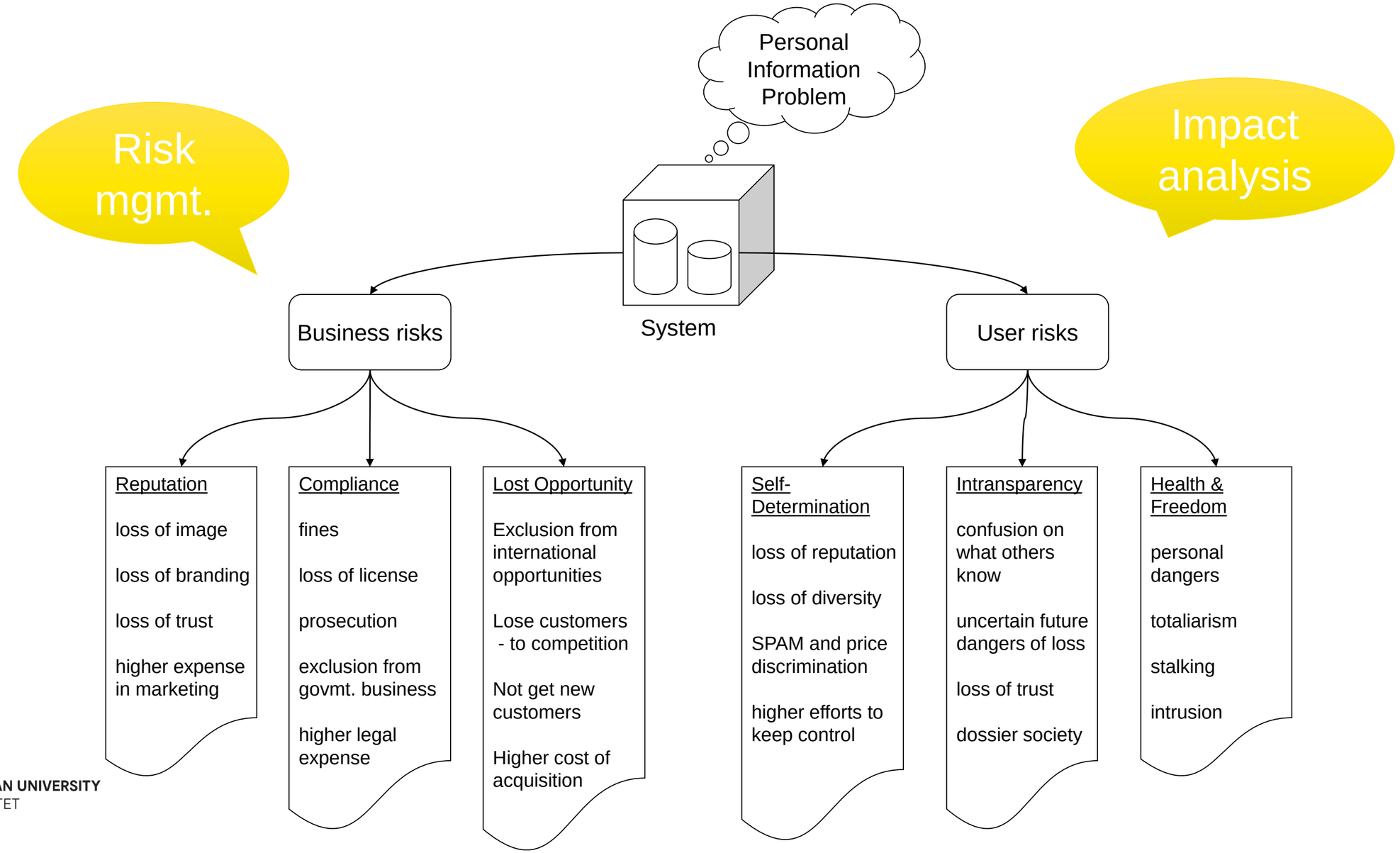
UK ICO,
https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf

Note: «potential impact on individuals»

Step 5: Identify and assess risks

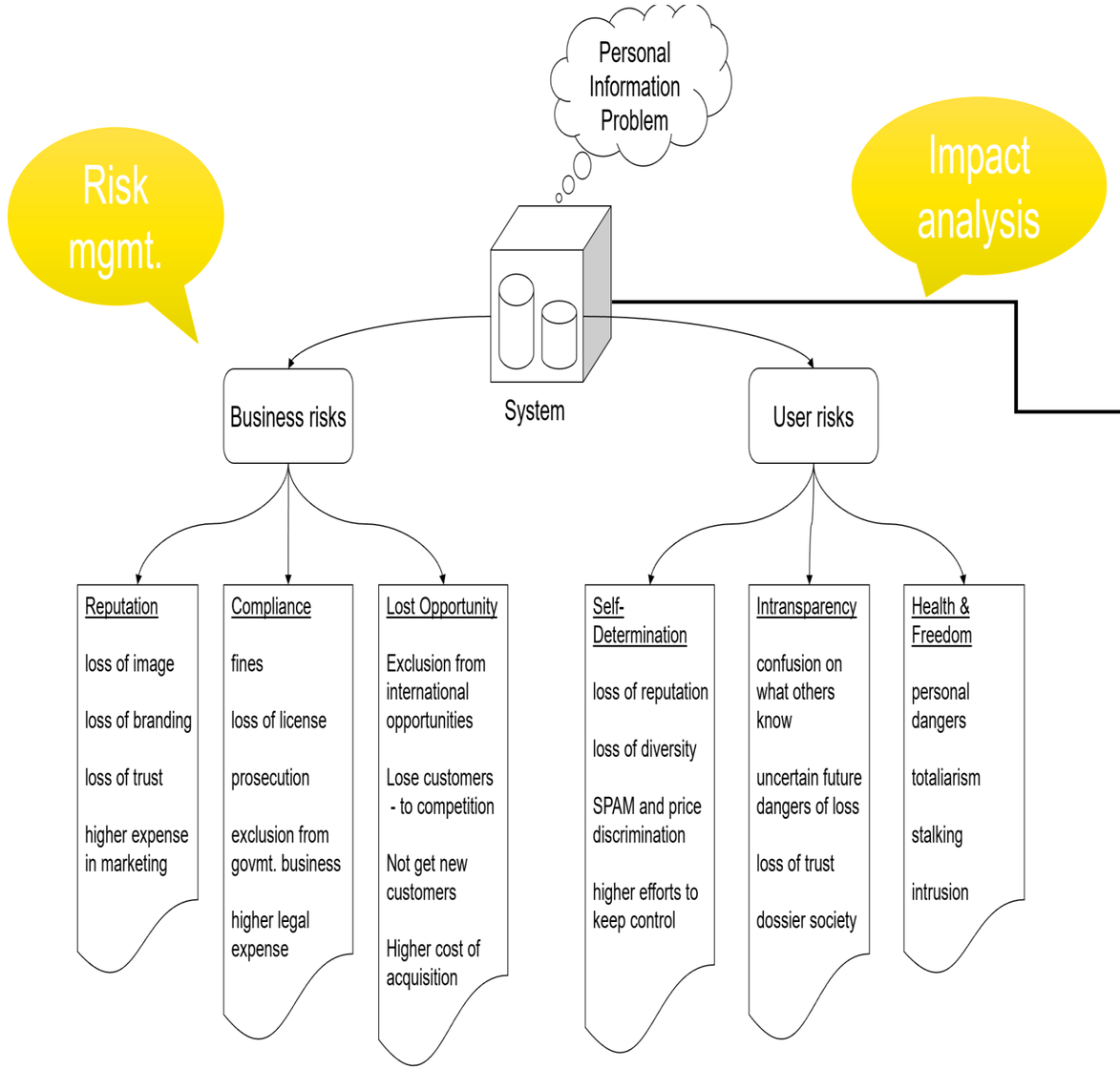
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**

Duality of Privacy Risks



Fritsch, Lothar; Abie, Habtamu (2008): Towards a Research Road Map for the Management of Privacy Risks in Information Systems. SICHERHEIT 2008

~~Du~~Triality of Privacy Risks



Threats to society

Personalized (cyber) war

?

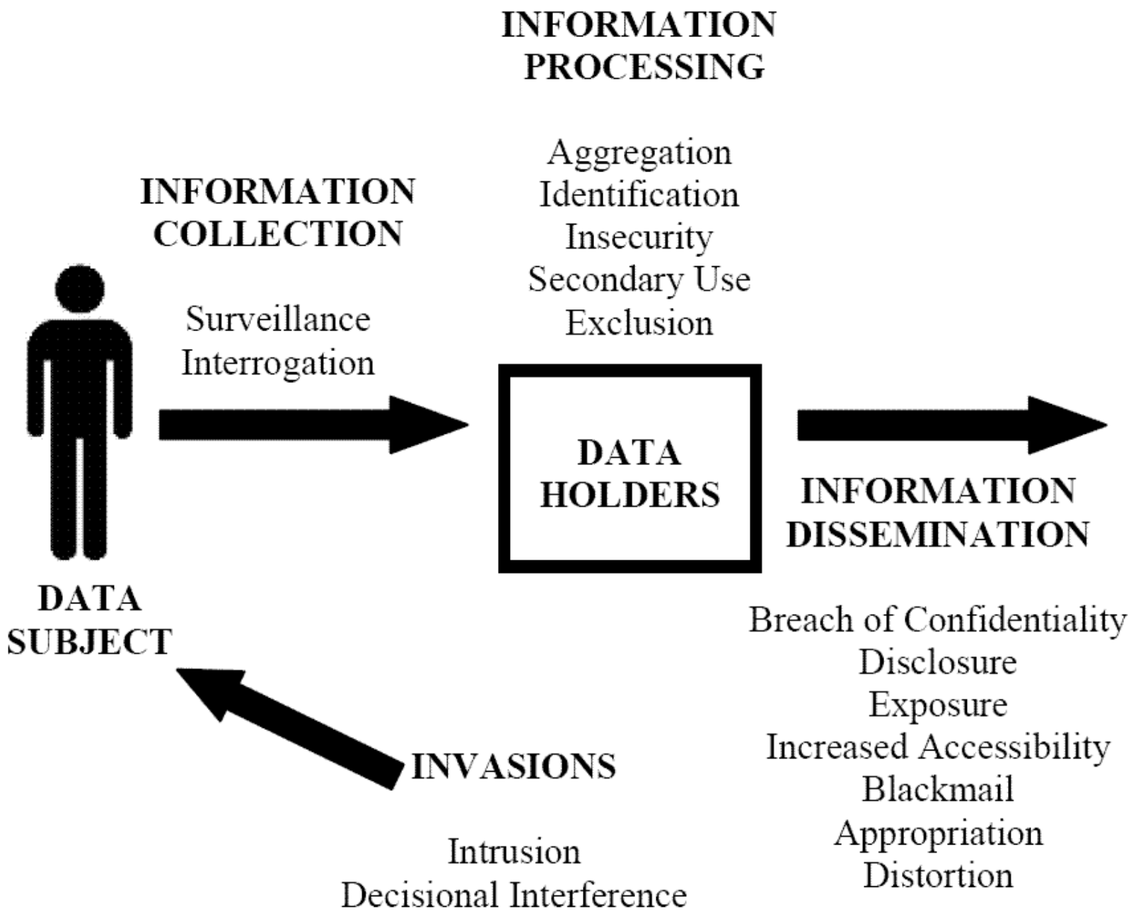
Cambridge Analytica / Facebook election manipulation

? ?

Team Jorge: Harassment as a service

Privacy harms
- «potential impact on individuals»

Solove’s privacy threat taxonomy



Daniel J. Solove *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

ENISA PIA Impact Levels

The European Union Agency For Network and Information Security (ENISA) has published guidelines for privacy risk assessment for Small and Medium Enterprises that contain guidance on privacy impact assessment focused on individual data subjects in chapter 3 on page 19. There, four levels of privacy impact are defined:

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

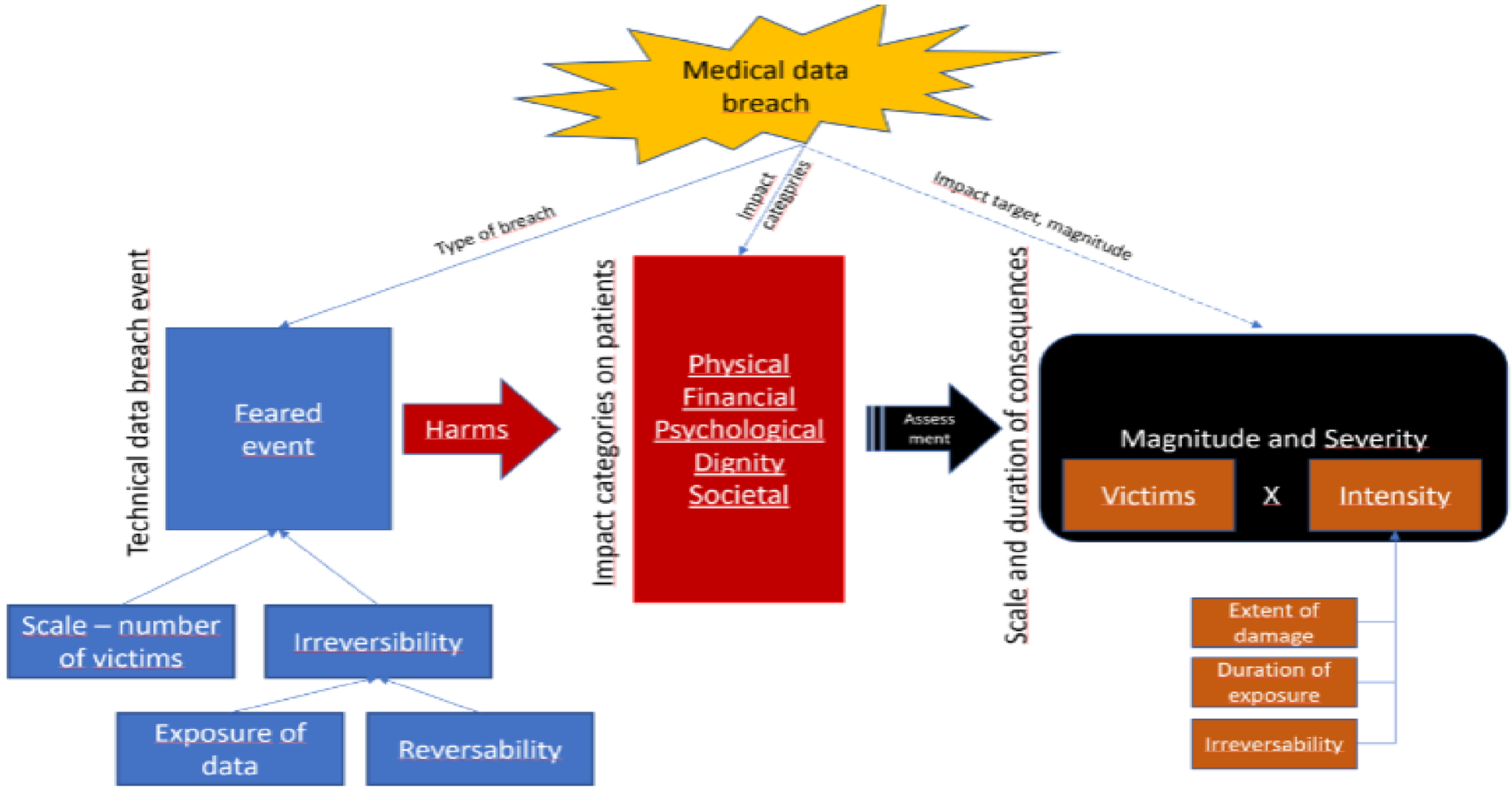
ENISA: Guidelines for SMEs on the security of personal data processing, December 2016, ISBN 978-92-9204-209-7, DOI 10.2824/867415, European Union Agency For Network and Information Security.

PRIAM privacy harms (impact)

A **privacy harm** is the negative impact on a data subject, or a group of data subjects, or the society as a whole, from the standpoint of physical, mental, or financial well-being or reputation, dignity, freedom, acceptance in society, selfactualization, domestic life, freedom of expression, or any fundamental right, resulting from one or more feared events.

pp. 28 in: Sourya Joyee De, Daniel Le Métayer. PRIAM: A Privacy Risk Analysis Methodology. [Research Report] RR-8876, Inria - Research Centre Grenoble – Rhône-Alpes. 2016. Nr. hal-01302541.

PRIAM – focus on harms to subjects



Samuel Wairimu and Lothar Fritsch. 2022. Modelling privacy harms of compromised personal medical data - beyond data breach. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). Association for Computing Machinery, New York, NY, USA, Article 133, 1–9. https://doi.org/10.1145/3538969.3544462

Real harms following medical data breach

Medical records of a Florida woman were disclosed by a nurse thus revealing her long secret

Disclosure of patient's prescription history that led to criticism from her ex-boyfriend

Medical data from the World Anti-Doping Agency concerning athletes disclosed

Disclosure of patient's sensitive status on social media

Individual targeted for medical identity theft - bills totaled to almost 20,000 US Dollars - Hackers are stealing millions of medical records – and selling them on the dark web

Medical records of a woman accessed and disclosed by ex-partner in an unauthorised manner

A NHS staff member disclosed personal medical data regarding her sister-in-law to the family members

Doctor provides an investigator with full medical records of a patient to dig dirt on him after a complaint to the Medical Board of California

Patients, including a prominent individual in Finland, received emails demanding ransom after a breach of psychotherapy records

A case in which doctors' breached the privacy of one of their colleagues after accessing into his medical records

Women targeted after a data breach at the University Hospital Crosshouse - 'Stalker' rap after hospital data breach

Exposure of patient data led to the disclosure that an influential person in politics was using an ICD (Implantable cardioverter-defibrillator). An attacker gained access to the device and manipulated the data, which led to a cardiac arrhythmia (Demonstrated)

A patient's HIV status, including his PII remained in the public open record for at least six months prior to being sealed after a lawsuit filed by collections attorney on behalf of a healthcare provider seeking payment for an unpaid debt

More incidents in:

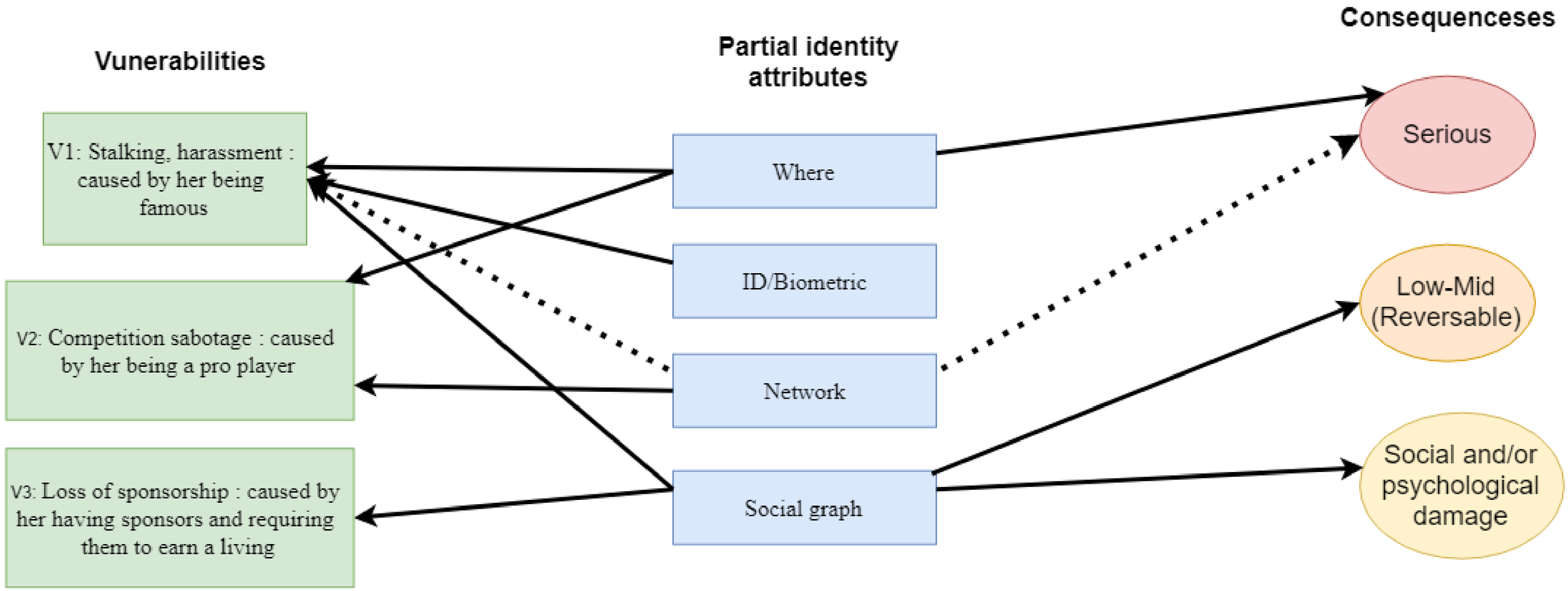
Samuel Wairimu and Lothar Fritsch. 2022. Modelling privacy harms of compromised personal medical data - beyond data breach. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). Association for Computing Machinery, New York, NY, USA, Article 133, 1–9. https://doi.org/10.1145/3538969.3544462

Privacy in contexts

Privacy, risks and harms must be viewed in contexts!

- Individual’s contexts
- Group contexts
- Society’s and competing societies’ context

PISA: Risk vs. Impact



Toresson, L., Shaker, M., Olars, S., Fritsch, L. (2020). PISA: A Privacy Impact Self-assessment App Using Personas to Relate App Behavior to Risks to Smartphone Users. In: Stephanidis, C., Antona, M. (eds) HCI International 2020 - Posters. HCII 2020. Communications in Computer and Information Science, vol 1226. Springer, Cham. https://doi.org/10.1007/978-3-030-50732-9_79

PISA: personas with vulnerabilities

Lina Odinsson

- **Background**
  - Streamer/Youtuber
  - E-sports professional
  - Has a following of more than 10 000 000
  - 16-24 years old
  - Female
  - Uses an alias while being online
- **Technology expertise level**
  - High level of computer habit, but not a super user
  - Have an good understanding of what could happen if information is leaked but

not of how the attack would be performed

- **Technology use**
  - Consoles for gaming purposes
  - Computer and phone for social networking
- **Access location**
  - Home network
  - Public network
- **Threats from technology use**

1. Reachable on electronic platforms for messaging
2. Traceable throgh game traffic.

- **Vulnerabilities**

1. Stalking, harassment : caused by her being famous
2. Competition sabotage : caused by her being a pro player
3. Loss of sponsorship : caused by her having sponsors and requiring them to

earn a living

N.B for graph: Add one from ID to stalking, Add one from Network to Sabotage

- **Needs**
  - To be able to stay anonymous
  - To not be spied upon
  - For her career to continue.

Toresson, L., Shaker, M., Olars, S., Fritsch, L. (2020). PISA: A Privacy Impact Self-assessment App Using Personas to Relate App Behavior to Risks to Smartphone Users. In: Stephanidis, C., Antona, M. (eds) HCI International 2020 - Posters. HCII 2020. Communications in Computer and Information Science, vol 1226. Springer, Cham. https://doi.org/10.1007/978-3-030-50732-9_79

The real privacy risks and impact

- Threat of individual rights being violated
- Threat to organization/business (compliance perspective)
- Threat to society’s mechanisms or societal architecture
- Actual impact on individual data subject’s life
  - where threats and harms are defined by individual context!
  - Mind: Irreversible harms and hard-to-reverse harms!

Data is the new oil … what about the oil spills?

- Massive data collection, analysis and distribution capacity
- ”Big Data” promises near-magic self learning, knowledge-discovering and artificially intelligent computers – if they just get fed enough information.
- Data leakage, data sabotage, espionage and poor data quality are serious threats
- Hard to revert a ”data spill” once data has leaked, been stolen or published.
- Potential for personal compromise as well as a threat to IT product vendors – or endangering national security and sovereignty

Disclose Data
a person, process, or system creates and publishes/shares data

Manipulate Data
a person, process, or system transforms, moves, or analyzes data

Consume Data
a person, process, or system benefits from manipulated data

Acquire
Ingest data from sensors, systems, or humans, recording its provenance and consent for use wherever possible.

Store
Record data to a trusted location that is both secure and easily accessible for further manipulation.

Aggregate
Combine disparate datasets to create a larger dataset that is greater than the sum of its parts.

Analyze
Examine and transform data with the purpose of extracting information and discovering new insights.

Use
Apply the insights gained from data analysis toward making decisions, affecting change, or delivering a product or service.

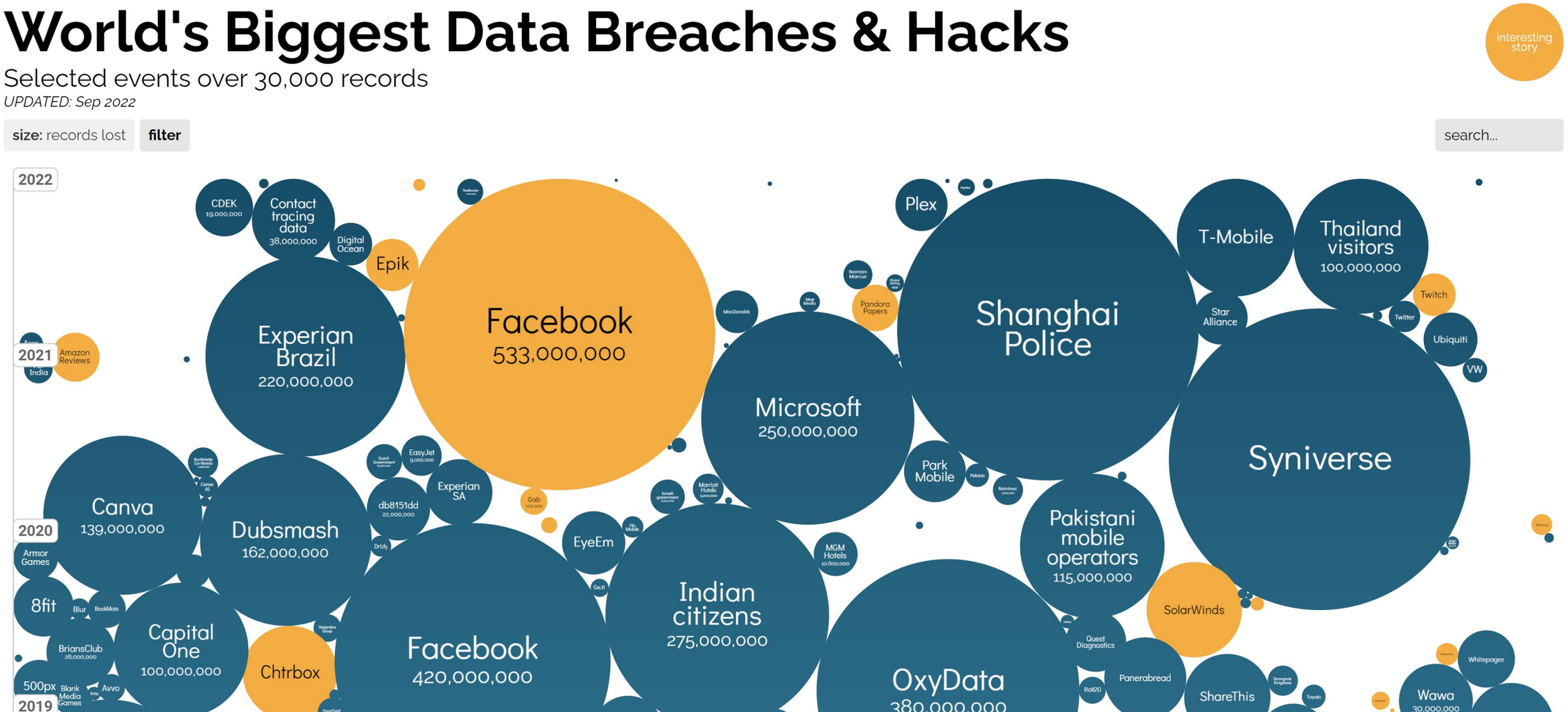
Share/Sell
Provide access to datasets or data insights to new sets of data manipulators or consumers.

Dispose
Remove data from servers to prevent future release or use.

Accenture report: Building digital trust: The role of data ethics in the digital age, https://www.accenture.com/us-en/insight-data-ethics , accessed April 2018

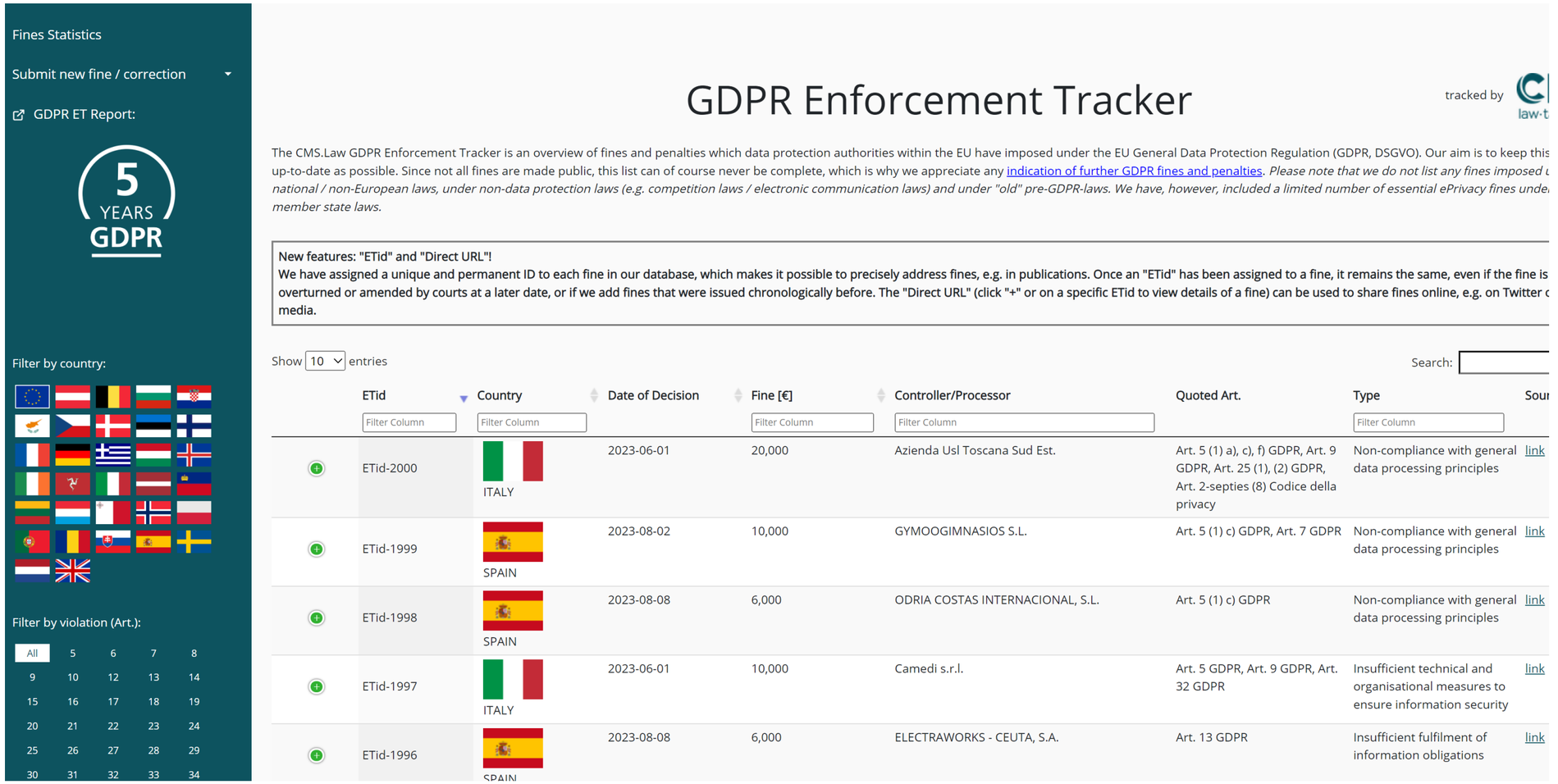
The World’s Biggest Data Breaches

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



GDPR enforcement tracker (fines)

https://www.enforcementtracker.com/



Questions / Discussion

LOTHARFR@OSLOMET.NO

OSLO METROPOLITAN UNIVERSITY
STORBYUNIVERSITETET