Engaging Content
Engaging People

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

IRISH RESEARCH COUNCIL
An Chomhairle um Thaighde in Éirinn

NGI TRUST

(Re-)Inventing the Wheel: Privacy Risks of Technology

Harshvardhan J. Pandit

Postdoctoral Research Fellow
ADAPT Centre, Trinity College Dublin

https://harshp.com/research
pandith@tcd.ie

FRIDAY
WU-SC ~~Monday~~ 21-MAY-2021

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund
Science Foundation Ireland

The ADAPT Centre is funded under the SFI Research Centres Programme (Grant 13/RC/2106_P2) and is co-funded under the European Regional Development Fund.

What is Technology?

Technology is anything invented after you were born, everything else is just stuff

Alan Kay

Human-Computer Interface pioneer

What is a Risk?

Uncertainty ? → operational → IMPACT

→ functional →

→ economic →

Is it always 'negative' ? For whom?

Does risk always need 'harm' ? To whom? - - → IMPACT

What relationship(s) exist between:

- artefacts and risk → is the risk inherent? proportional?
- people and risk →
- context and risk → environment
- consequence and risk → more -ve ≡ more severe risk?
- time and risk → will it go away? is it temporal?

What is Privacy?

→ Who/What is a 'Person' (entity)?

individual
groups
society
entity

company
group
country

→ What is 'Private' to that entity?

→ own / self / shared

→ What 'Controls' or 'Choices' does that entity have to enforce or maintain the boundaries of what is private to them?

→ who provides controls?
fundamental rights?
enforced?
agreed & shared?

What is Privacy Risk?

Naive :: A 'risk' to 'privacy' → vague, abstract, universal

↳ arbitrary definition

Security :: Determining access to 'private' artefacts → protection

safeguard prevent mitigate

Social :: Establishment of 'boundaries' and 'private domains'

shared agreed

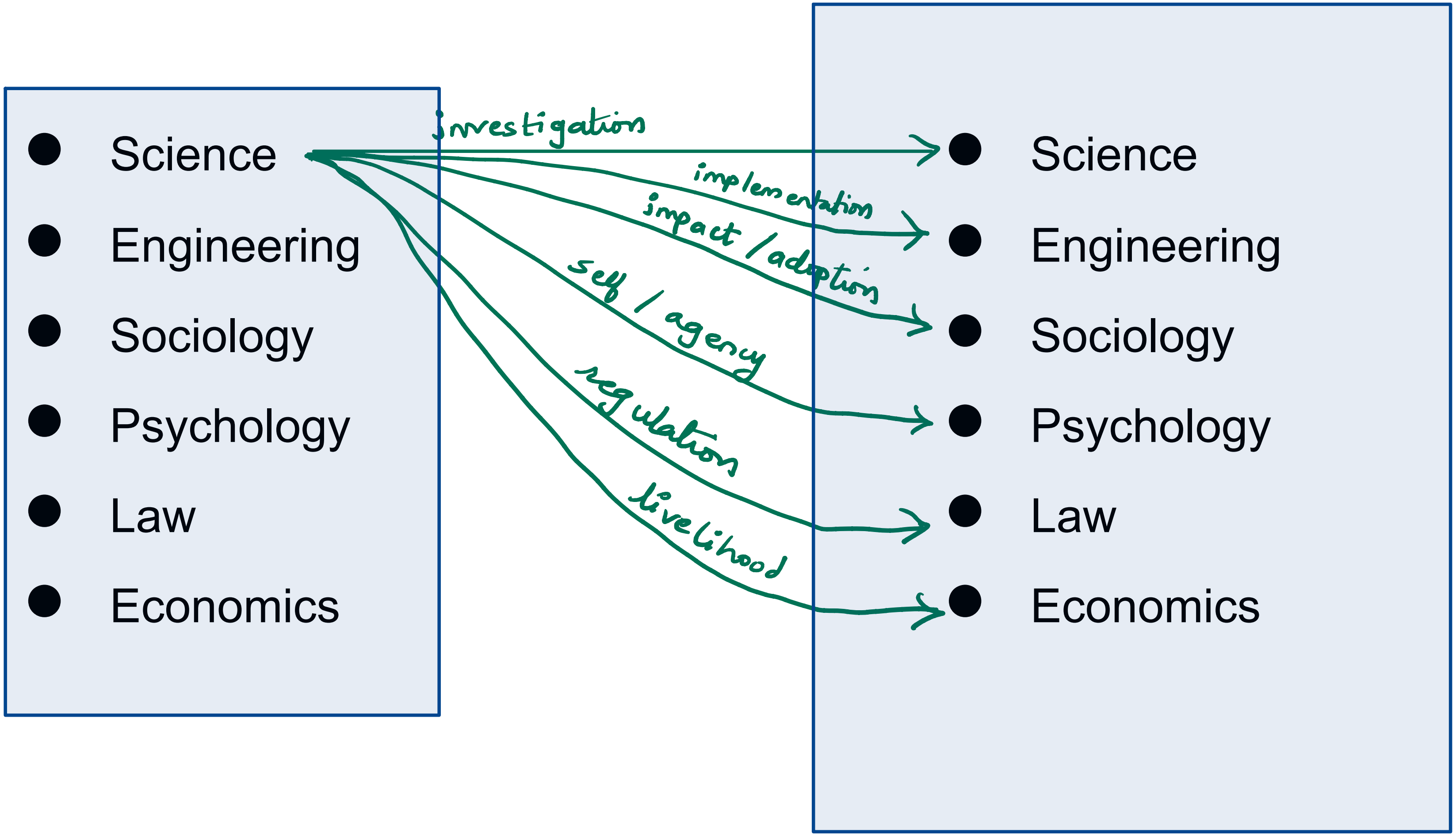
Psychological :: Control over 'personal space'

self identity ↳ "human"

Legal :: Notion of harm or violation of norms for privacy

PERMIT vs. PROHIBIT

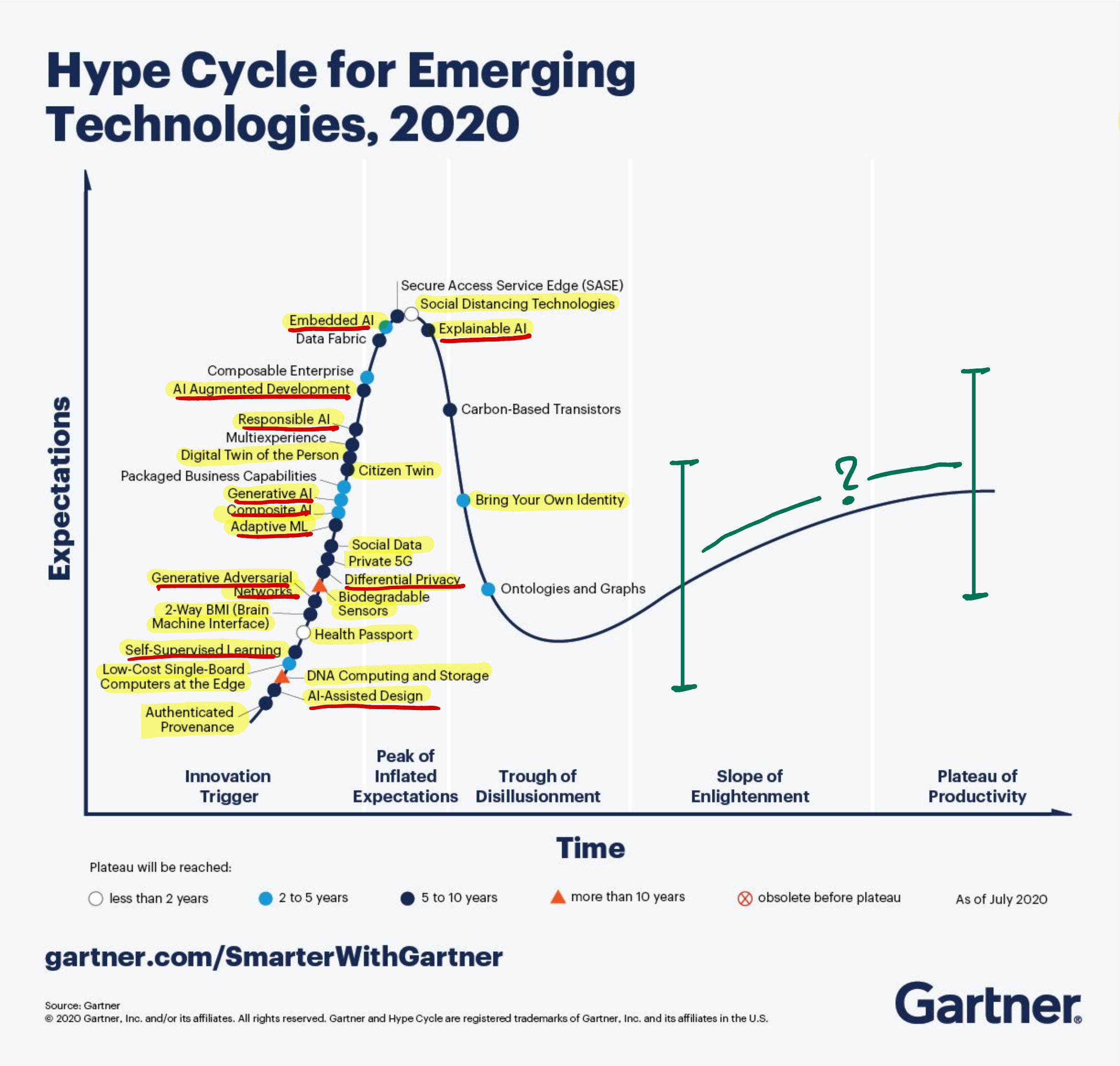
Inter-Perspectives in Society



- Science
- Engineering
- Sociology
- Psychology
- Law
- Economics

- Science
- Engineering
- Sociology
- Psychology
- Law
- Economics

Gartner's Hype Cycle - Emerging Technologies

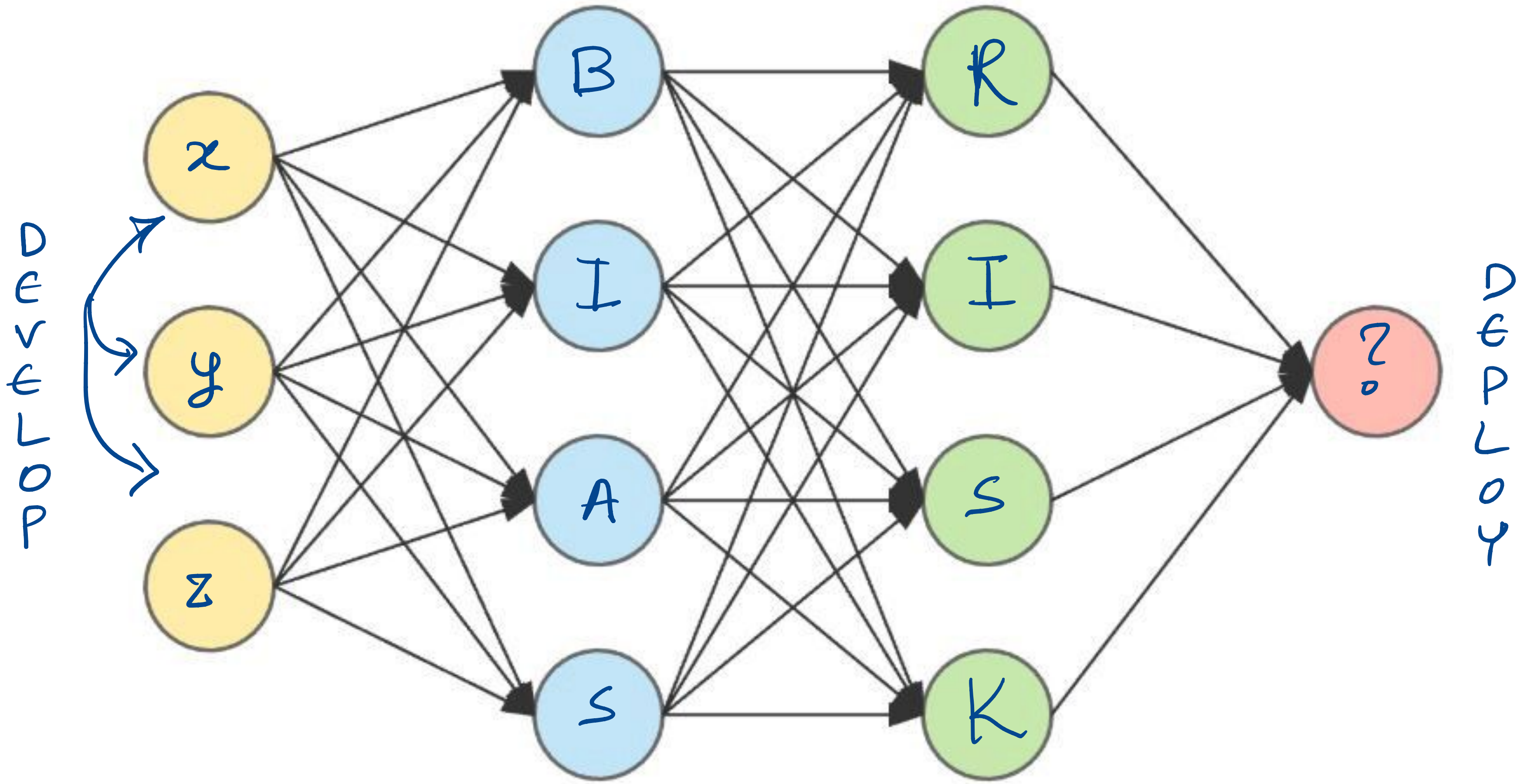


Source: Gartner

Areas with active exploration of privacy risks

Areas that are AI or use AI

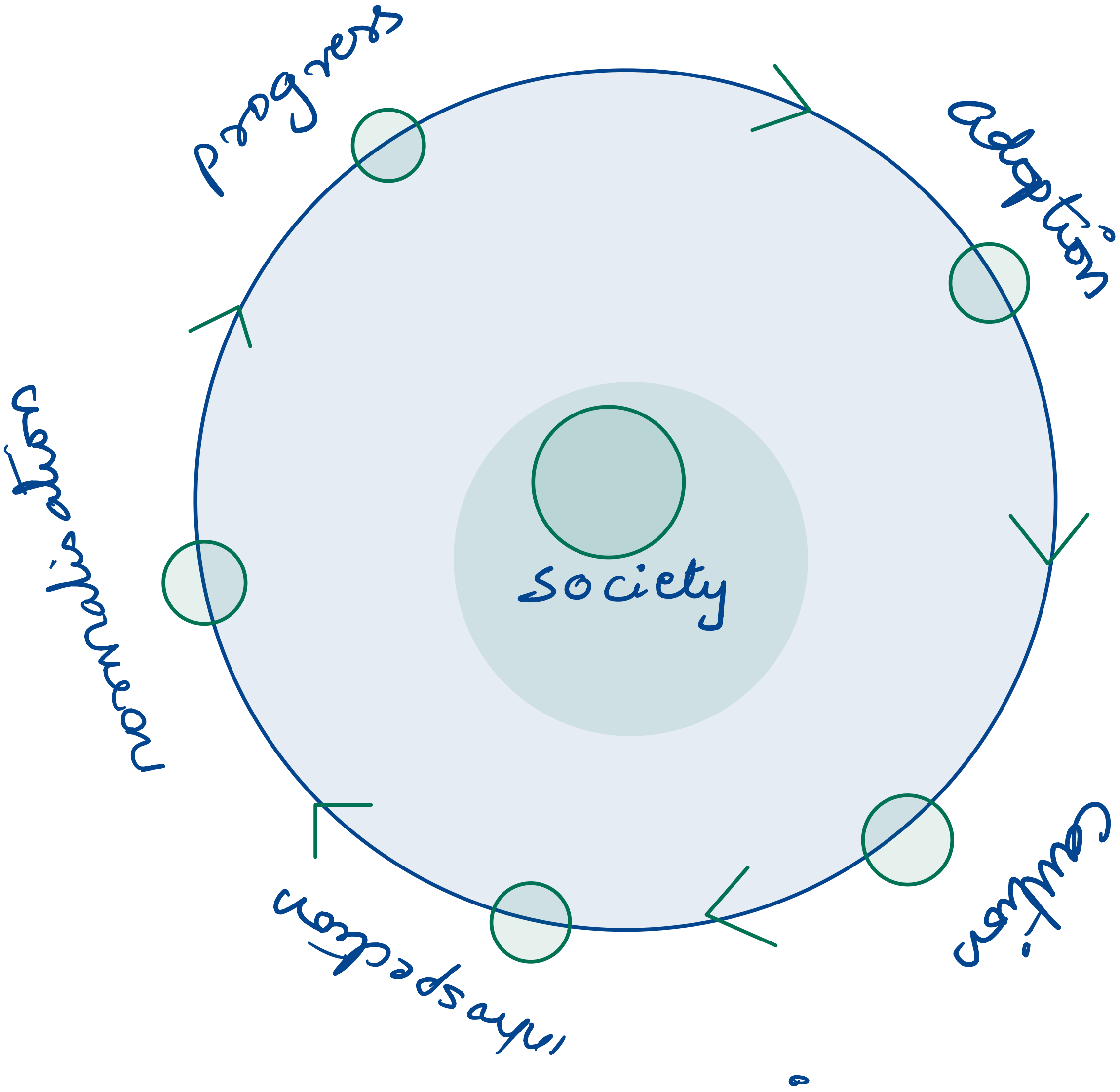
The AI bandwaggon



B - behaviour
I - introspection
A - artificial
S - systematic

R - resolvable
I - inherent
S - serendipity
K - knowledge

Bringing it together - Re-Invention of the Wheel



PROGRESS
ADOPTION
CAUTION
INTROSPECTION
NORMALISATION

RISKY propositions

How to 'find privacy risks' for a given scenario?

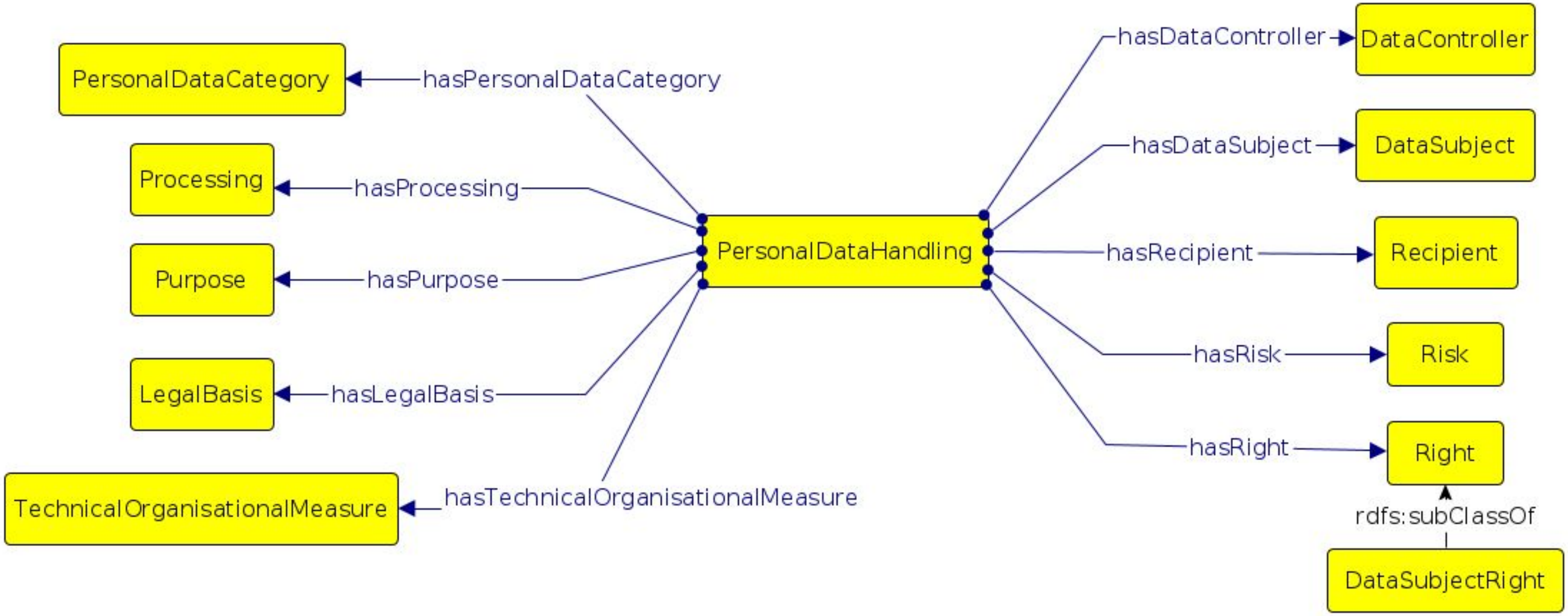
Can we re-apply lessons learned in developing one area of technology to another?

RISKY :: Exploring Privacy Risks of Technologies using Knowledge Graphs

- Funded by Irish Research Council for 2 years
- Create a vocabulary of known risks (using DPV)
- Associate risks with scenarios, technologies, concepts
- For 'new' situation, discover risks from existing knowledge

Machine-readable Metadata

Data Privacy Vocabulary[1] (DPV), v0.2, 2021 https://w3.org/ns/dpv



Machine-readable vocabulary for creation of technological solutions and enhancing interoperability

(A) Existing information → DPV

e.g. NLP[2] to analyse privacy policies → extract terms → perform legal analysis

(B) DPV → Generate Information

e.g. Utilise DPV to generate common ROPA[3] documentation for GDPR compliance

[1] Creating A Vocabulary for Data Privacy (alt: Data Privacy Vocabulary (DPV)). Pandit, Polleres et al. 2019. https://zenodo.org/record/3934476

[2] The Role of Vocabulary Mediation to Discover and Represent Relevant Information in Privacy Policies. Leone et al. 2020 https://ebooks.iospress.nl/volumearticle/56164

[3] A Common Semantic Model of the GDPR Register of Processing Activities. Ryan et al. 2020 https://doi.org/10.3233/FAIA200876

Why Knowledge Graph? Why Law?

Knowledge Graph: → existing research

- Abundance of resources, too little time (also mortality)
- Continuity, Extendibility → progress is inevitable
- Formalism → lingua franca
- Annotate, Query, Validate, Explore → practicality

Law: → soft → hard

→ encoded responsibility accountability

- Enforceable -- we are a *lawful* society rather than a *lawless* one
- Commonality in Framework e.g. PIA, DPIA, AI-IA — algorithmic/AI

  privacy data protection
- Personhood and Accountability

  → duties fiducaries

Preliminary Pattern: Control Level I

Three situations where there are different risks associated with face recognition, have different actors, and different accountability.

```
Phone|App → camera → Facial recognition
Shop CCTV → camera → Facial recognition
Traffic analyser → camera → Facial recognition
```

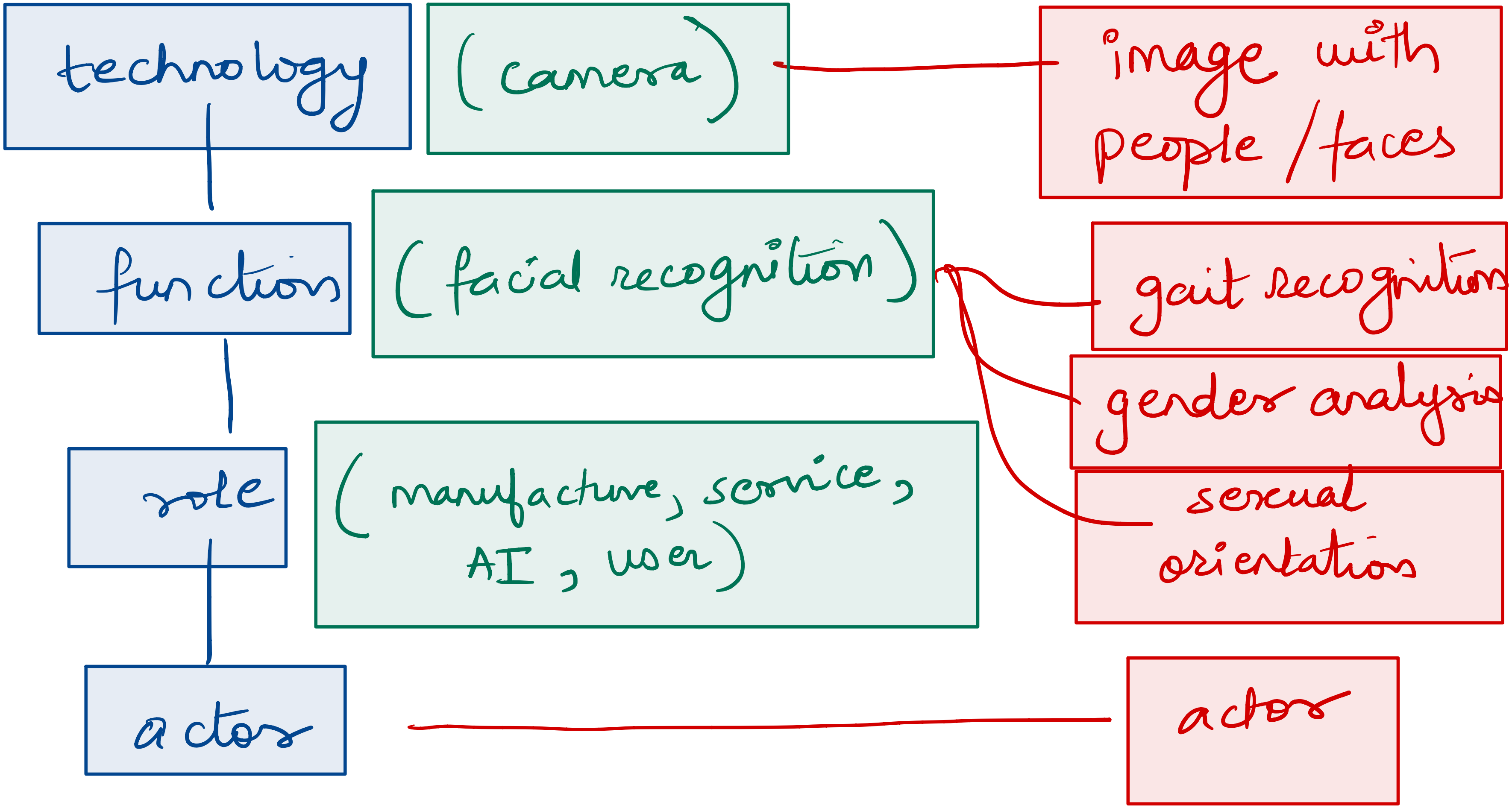
Does `have(camera)` imply `does(facial_recognition)` ???

Preliminary Pattern: Control Level II

Control Pattern:

1. (Law) Who controls the artefact (i.e. camera) and the function (i.e. face recognition)? → Phone manufacturer, Shop, Govt. Department
2. (Social) What is accessible to respond away from the artefact? → helpline, complaint procedure, authority, leaflet, website
3. (Security) What controls are provided/possible? → tape/cover it up, setting or control, warning (notice)
4. (Human-centric) Is there comprehension of function? → boundary box around face, notice, awareness of entities
5. (Psycho-social) Does the function only work for specific contexts? → demographics, sex/gender, groups, individuals

Preliminary Pattern: Control Level III



CPVE: Common Privacy Vulnerability and Exposures

- Common Vulnerabilities and Exposures (CVE) is a common, open, and public list of registered references for information-security vulnerabilities and exposures
- Used widely and successfully to share common information about risks, vulnerabilities, and address mitigations. E.g. every ‘fix’ in your phone’s OS is given a CVE (either internal or external)
- Similar or related, are ‘manufacturing standards’ that require adherence to ‘quality’ control for materials and products

Can we adopt this as a practice for privacy risks?

The six sides of a loaded dice

1. ‘Common’ individuals - society at large
2. Aware/Knowledgeable/Expert/Benefit groups
3. Technology (as itself)
4. Producers/Enablers/Developers/Manufacturers
5. Corporations/Companies
6. Law

In conclusion, and in preparation for discussion

1. The Future is Mutli-Disciplinary
2. We may never agree on what ‘privacy’ means exactly
3. There will always be a gap between technology creators and knowledge regarding privacy risks and impacts
4. The law will never cover most of the use-cases or will take too long
5. We’ve reached here collectively as a ‘responsible society’ - how?
6. The more knowledge, the more difficult it is to find it and apply it.