Digital Security:
How your protection impacts our research work

The interplay between Governance, Technology, and Policy

Afonso Ferreira
Centre National de la Recherche Scientifique
CNRS-IRIT
Toulouse, France

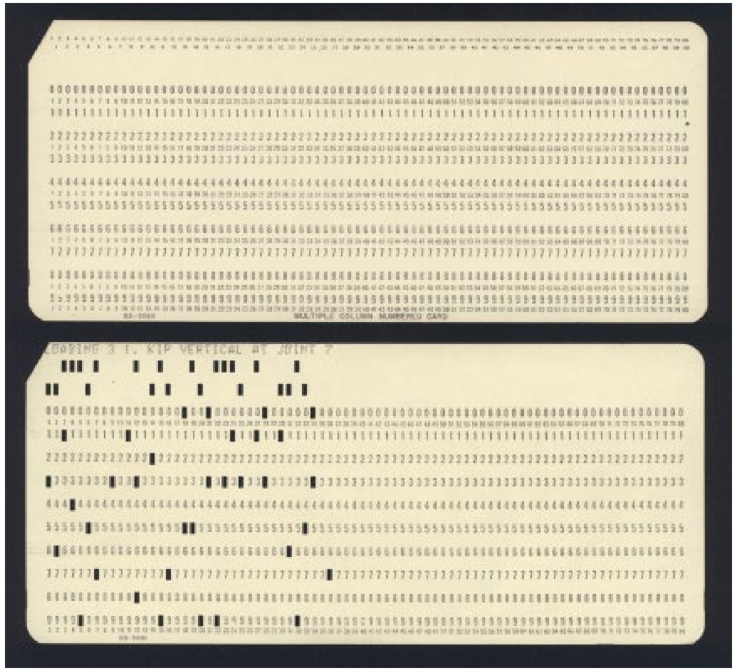
This work was partially supported by the European research projects H2020 CyberSec4Europe (GA 830929) and LeADS (GA 956562), Horizon Europe DUCA (GA 101086308) , and CNRS EU-CHECK

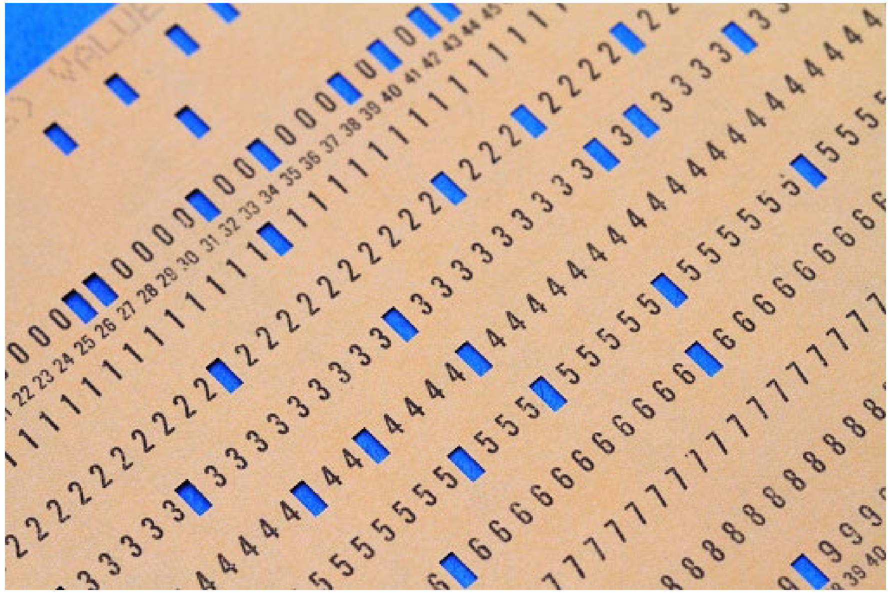
Today your journey is about to start

(Btw, who are you?)

March 1982 – My journey started

Our interaction with computers was different

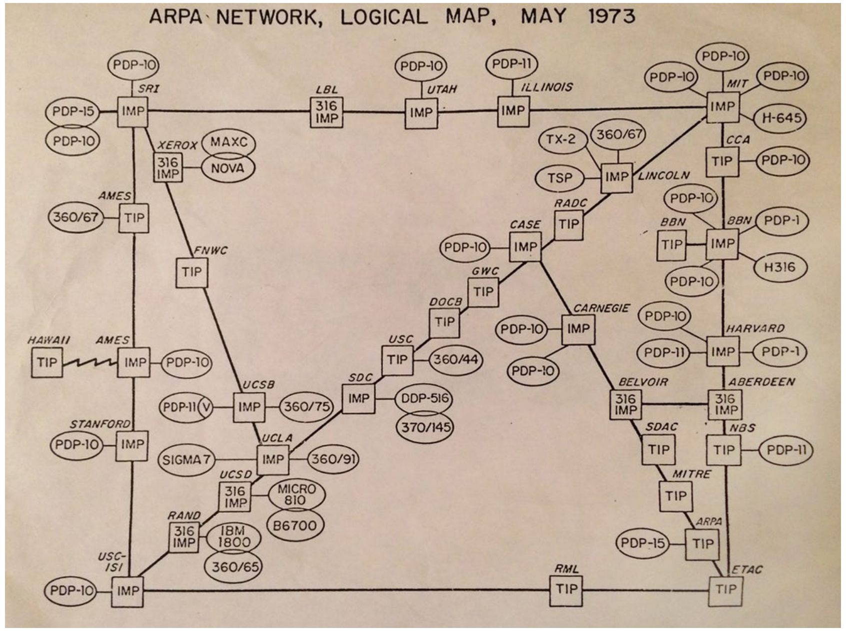




Computers were different
Mainframes – Burroughs

But 40 years ago we already had networks

The Internet (ARPANET) in 1973



Source: By ARPANET - ARPANET, Public Domain,
https://commons.wikimedia.org/w/index.php?curid=54039329

Adapted from E. Markatos - FORTH

40 years ago

- We had computers
  - Mainframes, mini computers were being sold, micros were starting to appear
- We had programming languages
  - Pascal and the C programming languages were there
- We had networks - the Internet
  - It was called ARPANET, but still…
- We had software
- We had freedom of design

Adapted from E. Markatos - FORTH

Computer Sciences in 1982

- Existed but not a big deal
- Probably because:
  - **Boring applications**
    - mostly scientific applications – numerical analysis
  - **Closed Community**
    - mostly academics had access to Arpanet
  - Even compromised computers **did not have a lot of value**
    - No data
    - No financial value
  - **Small scale**:
    - Arpanet had just a few tens of nodes

Adapted from E. Markatos - FORTH

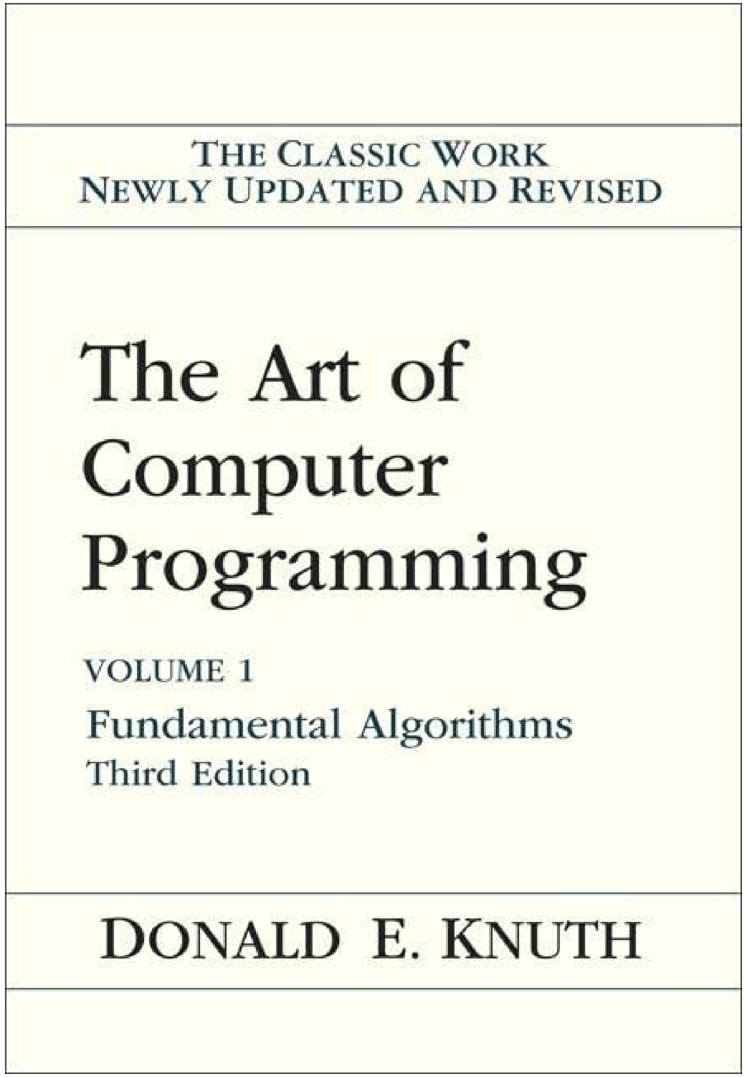
1 2022

Computer Sciences in 1982 were like teenagers

- Computing was not a major issue
- Thus, the **design of computing techniques was not constrained**
  - Small Academic community
  - Restricted physical (and virtual) access to networks
  - Restricted access to computers

Adapted from E. Markatos - FORTH

We were artists!



THE CLASSIC WORK
NEWLY UPDATED AND REVISED

The Art of Computer Programming

VOLUME 1

Fundamental Algorithms

Third Edition

DONALD E. KNUTH

Years of good feelings

- For ±15 years computers and the Internet kept on being
  - Boring or unknown for most of the population
    - Mostly scientific applications
  - Closed Community
    - Mostly academics had access to open networks
- There was an occasional computing issue
  - But people (out there) did not take notice…
  - They did not have an Internet connection
  - They did not have a facebook account…
  - They did not have a smartphone…

Adapted from E. Markatos - FORTH

And then..
Something changed!

- People started connecting to the Internet
  - The ISPs started offering Internet Connections
- People of all realms – not only academics
- Computers **started storing data**
  - Lots of data!
  - Interesting data!
  - Personal Data: Email - Gossip!
  - Financial data: Credit card numbers

Adapted from E. Markatos - FORTH

And then things changed even more

- People started doing
  - Online banking
  - Online stock market transactions
  - Online purchases
- The money went on the Internet!
- People started
  - Watching movies online
  - Reading newspapers online
  - Chatting with friends online
- The advertisement money went on the Internet!

Adapted from E. Markatos - FORTH

So…

- Activities started migrating to the Internet
  - Entertainment, news, movies, television
- Money started moving to the Internet
  - Web banking, stock market, on-line trading

and obviously

- Crime started moving to the Internet
  - Fraud, thefts, phishing, attacks, money laundering, …

Adapted from E. Markatos - FORTH

The result

- We had an Internet designed for a small community of academics
  - Who knew and trusted each other

Being used by

- Billions of people who
  - did not know each other
  - did not trust each other
  - may be hostile to each other

Adapted from E. Markatos - FORTH

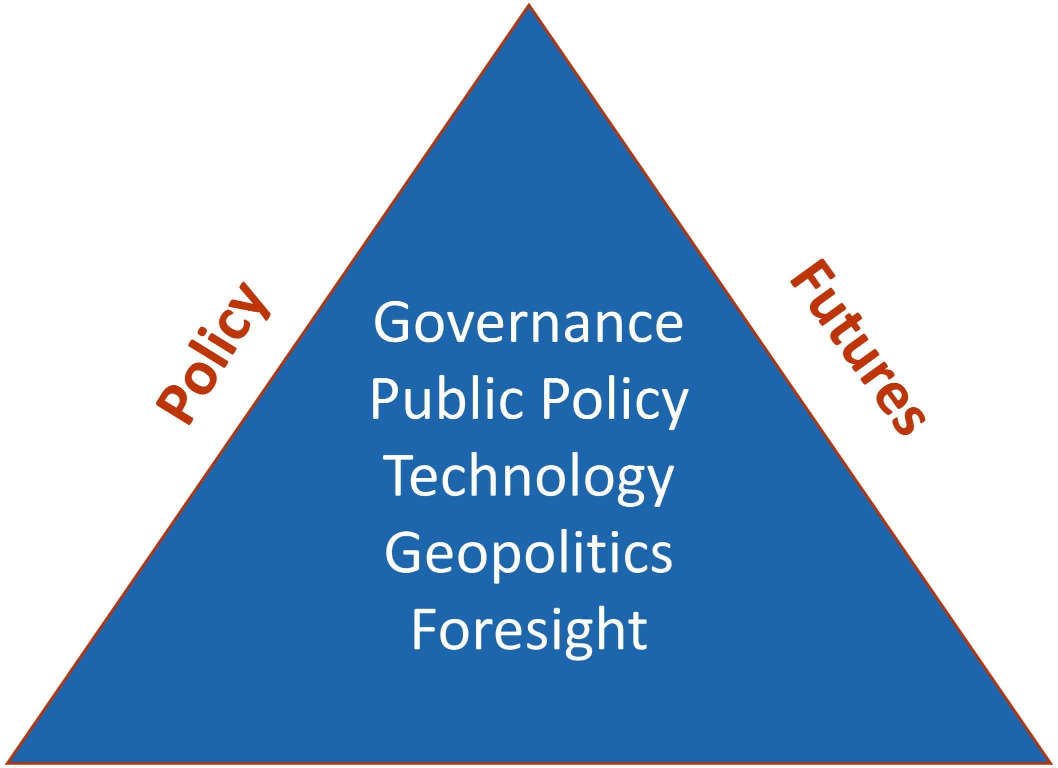
Well, now …you need protection!

- Personal data must be protected
- Data of all kinds must be protected from theft
- Systems that store data must be protected
- Systems that may have an impact on you must be regulated
- The whole software design eco-system must be regulated

- The fun is over…
  - Computing has grown up and needs to pay taxes
  - Geopolitics comes into play

The nexus of
Policy / Technology / Futures

(and its impact on software design)



Digital Technologies

Digital Sovereignty as a matter of EU Governance

- 'Digital sovereignty' refers to **Europe's ability to act independently in the digital world** and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies). (EP)

Governance in the EU (Gov 101)

European Parliament

Co-legislators

Council of the European Union

European Commission

Proposals and Executive

Policy & Legislation in the EU

- Plenty on Digital matters since 2016

- Eg Europe’s Digital Decade: digital targets for 2030, whose proposed principles are:
  - Putting people and their rights at the centre of the digital transformation
  - Supporting solidarity and inclusion
  - Ensuring freedom of choice online
  - Fostering participation in the digital public space
  - Increasing safety, security and empowerment of individuals
  - Promoting the sustainability of the digital future

…And it needs your attention

- Why European Union’s policy and legislation are important
  - They’ll come to a law near you sooner than later

- The EU’s drive to export its values through regulation of the digital world
  - Digital technologies underpin most of the economy and societal relations
  - Mostly beneficial for individuals across the world
  - Constrains software design: Need to be compliant-by-design

- Risk-based approach

- Huge fines in case of non-compliance

EU Legislation framing your research
(Selected)

I. (Personal) Data Protection

Data and IoT

- GDPR
- European data strategy
  - Regulation on European data governance
  - The Data Act

II. Markets and Competition

Big Tech / IoT / Software markets

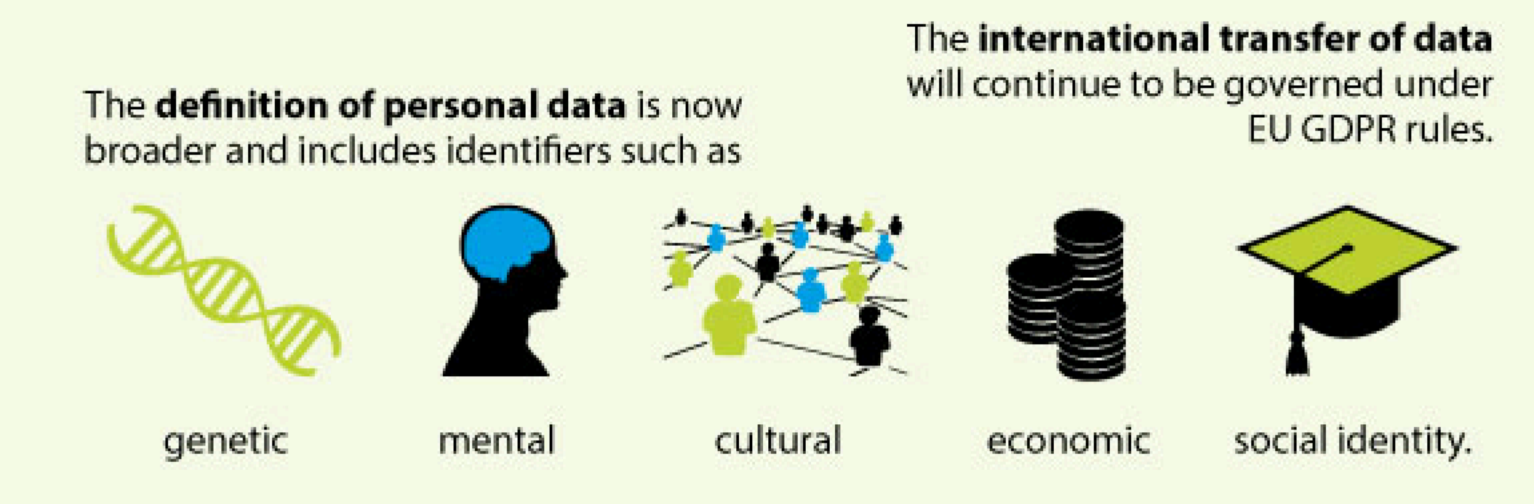
- Digital Services Package for the European Digital Single Market
  - Digital Services Act
  - Digital Markets Act
- The Digital Content Directive (Also here)
- The Sale of Goods Directive

III. (Cyber)Security

The thin line between National Security and EU Security

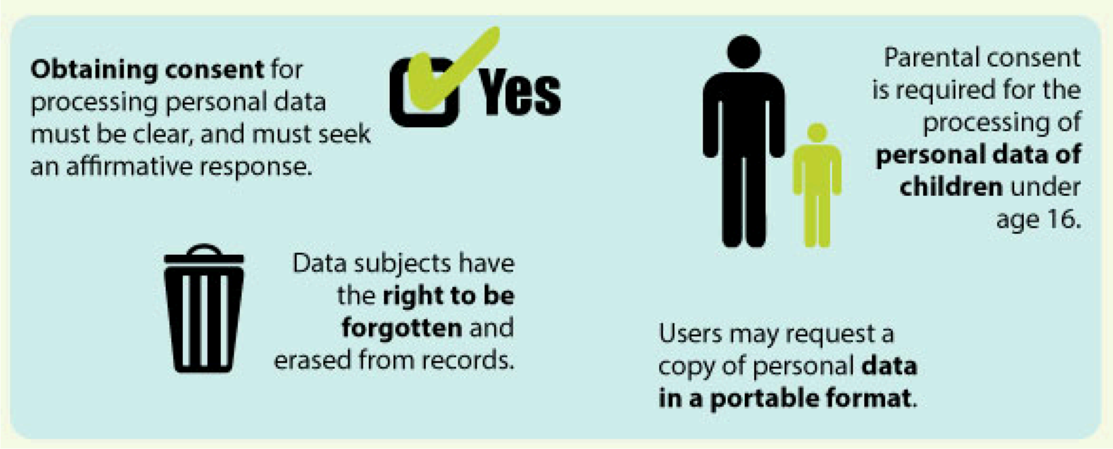
- (GDPR)
- NIS2 Directive
- CER
- DORA
- eID Regulation Revision and also here
- Artificial Intelligence
  - A European legal framework for AI to address fundamental rights and safety risks specific to the AI systems ;
  - Liability rules on products and AI
    - An AI liability directive - adapting liability rules to the digital age and AI ;
    - A Proposal for a product liability directive
- IoT
  - EU Cyber Resilience Act

The EU General Data Protection Regulation - GDPR
A new order started in May 2018



The **definition of personal data** is now broader and includes identifiers such as

The **international transfer of data** will continue to be governed under EU GDPR rules.



Obtaining consent for processing personal data must be clear, and must seek an affirmative response.

Parental consent is required for the processing of **personal data of children** under age 16.

Data subjects have the **right to be forgotten** and erased from records.

Users may request a copy of personal **data in a portable format**.

ISO 27001 and other certifications will help demonstrate "**adequate technical and organisational measures**" to protect persons' data and systems.

GDPR
A game-changer

Controllers must **report a data breach** no later than

72 hours

after becoming aware of the breach, unless the breach has a low risk to the individual's rights.

Privacy risk impact assessments will be required for projects where privacy risks are high.

Products, systems and processes must consider **privacy-by-design** concepts during development.

Tough penalties:
fines of up to

4% of annual global revenue

or

€20 million, whichever is greater.

New rules on AI – (Example of High risk AI)

Proposed April 2021 / Status: pending decision at the EU Council

- AI systems identified as **high-risk** include AI technology used in:
  - **Critical infrastructures**
  - **Educational or vocational training**
  - **Safety components of products**
  - **Employment, workers management and access to self-employment**
  - **Essential private and public services** (e.g. loans)
  - **Law enforcement**
  - **Migration, asylum and border control management**
  - **Administration of justice** and **democratic processes**

- Subject to **strict obligations** before they can be put on the market:
  - **Adequate risk assessment and mitigation systems**
  - **High quality of the datasets**
  - **Logging of activity to ensure traceability of results**
  - **Detailed documentation**
  - **Clear and adequate information**
  - **Appropriate human oversight**
  - High level of **robustness**, **security** and **accuracy**
  - **All remote biometric identification** systems are forbidden in **live use in publicly accessible spaces for law enforcement purposes in principle**

EU Cyber Resilience Act: Measures

- Aims to **safeguard consumers and businesses** buying or using products or software with a digital component (**IoT**)

- **Cybersecurity** is taken into account in **planning, design, development, production, delivery and maintenance** phase
- All **cybersecurity risks are documented**
- Manufacturers will have to **report actively exploited vulnerabilities and incidents**
- Once sold, **manufacturers must ensure that for the expected product lifetime or for a period of five years (whichever is the shorter), vulnerabilities are handled effectively**
- Clear and understandable instructions for the use of products with digital elements
- **Security updates to be made available for at least five years**

Europe intentions to be fit for the Digital Age

- Artificial Intelligence
- Connectivity
- Cybersecurity
- EU Cyber Resilience Act
- Digital Markets Act
- Digital Services Act
- European data strategy
- European industrial strategy
- European Chips Act
- High Performing Computing (HPC)
- European Digital Identity
- Contributing to European Defence
- Space
- Digital skills
- EU-US Trade and Technology Council

How to navigate the Future

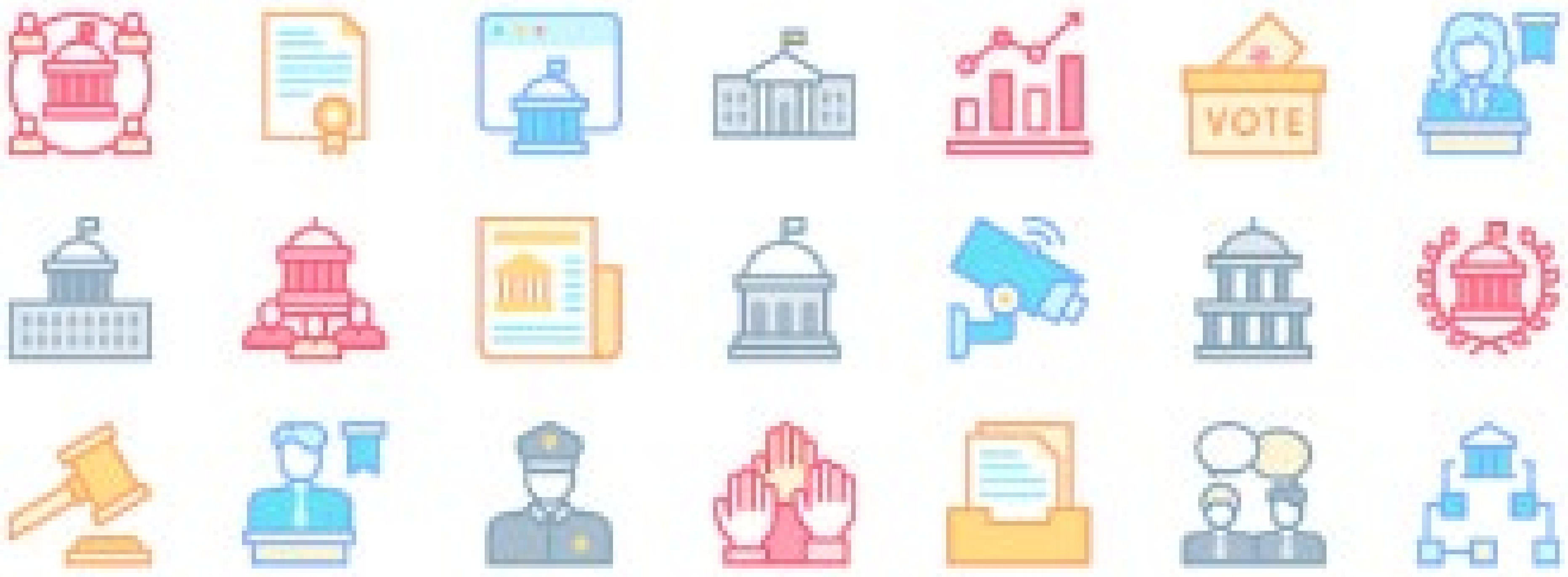
- **Metaverses**

© Business Advice

Metaverses: The full pack

- **Massive:** They can host an unlimited number, or at least a very high number of concurrent users
- **Immersive:** They offer three-dimensional and embodied experiences
- **Persistent:** Metaverses will never stop or reset. Or at least that will be the perception of their users
- **Open:** Anyone can go into metaverses, move within them as an avatar, interact with other avatars, socialise, trade, build, produce intellectually, and so on.
- **Economically developed:** There will be extensive trade in goods and services within the metaverses, which may or may not have an impact in the physical world outside them

Metaverse Governance & Legislation



Metaverse Governance & Legislation

- A metaverse is a digital world. It needs governance ***inside***

- In this new technological frontier that are metaverses, it is not clear *what* will be regulated, *who* will establish and enforce rules, or *how* this will be done

- But any place, physical or digital, at some point of population density will need some kind of order maintenance, including the notion of fundamental rights

- In the EU, as we saw, the rule-of-law is dominant and its institutions are mostly fit for purpose. **Are they enough for new, privately-owned digital worlds?**

Research questions – Technology & Policy

- The technologies needed to build metaverses, as envisioned here, are just emerging
  - A great deal of **technological and integration research** will be required in the next few years

- Many metaverses already exist, representing parallel universes
  - How to ensure **interoperability, portability, security, and data protection**
  - How to build your metaverse in a **compliant** manner
  - **Awareness of impact on climate change** (huge data centres, high performance computing, blockchains, etc)

- The policy in the making is also encompassing
  - From the governance viewpoint, there will be a need to **protect fundamental rights**
  - Protection of avatars and citizens from **surveillance vs technological needs in bio/neuro-metrics**
  - **Identity and Authentication**
  - Questions may address future concepts, like **whether avatars should be given citizen status**
  - Questions may be simple extensions of existing concerns, like **should metaverses be subject to existing laws for the physical world?** If so, how not to hinder innovation and creativity

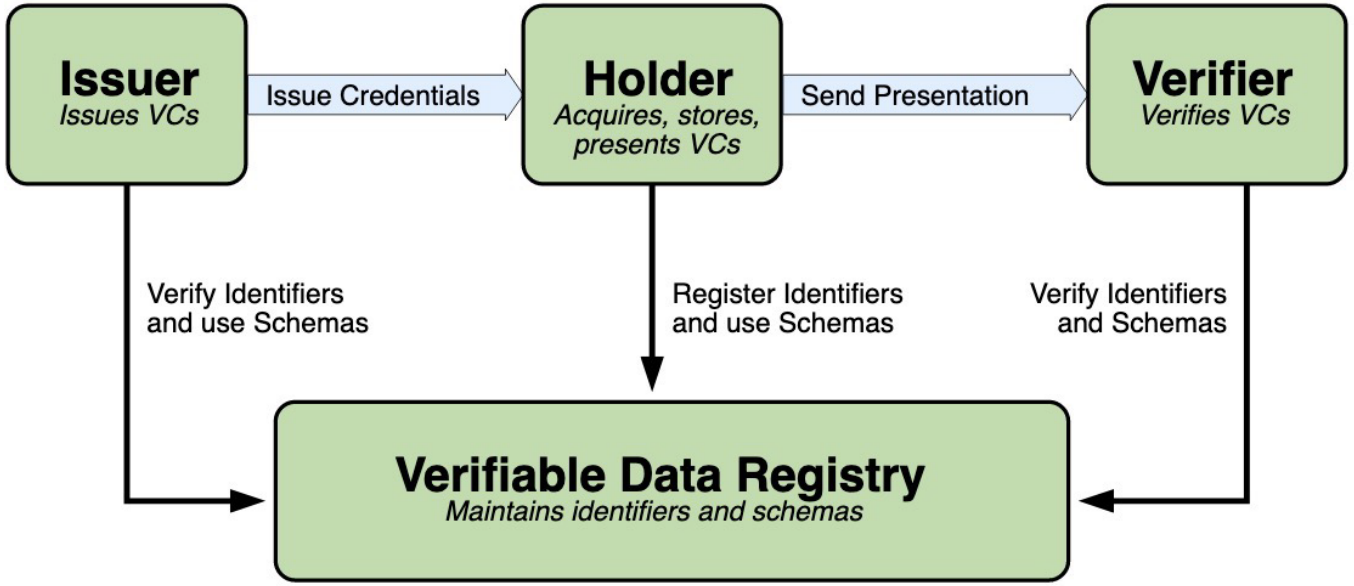
Example of technical questions directed by policy

Interoperability between Metaverses

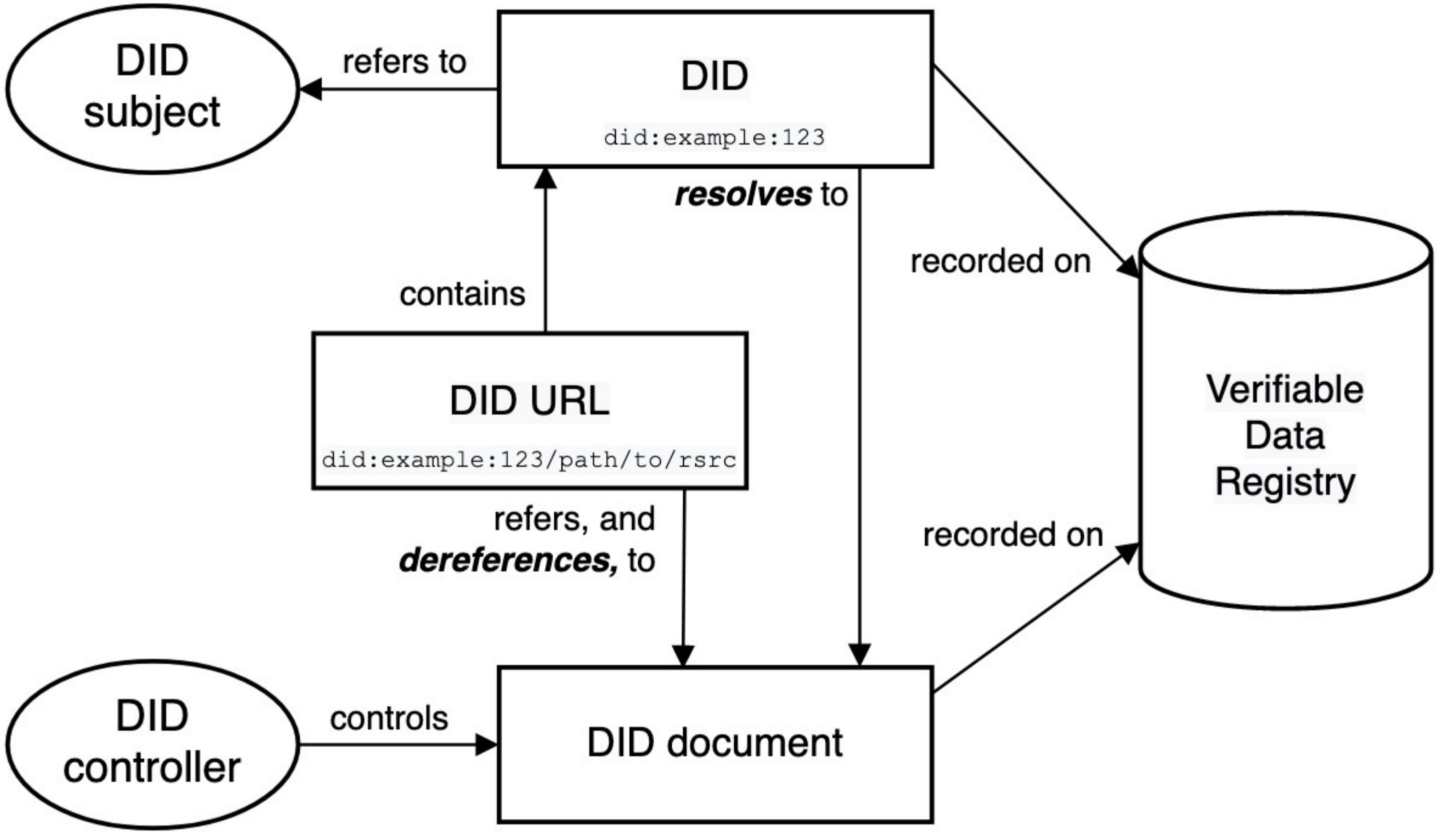
How can an Avatar securely travel between Metaverses? (*with R. Laborde*)

- **Digital Identity**
  - In a wide sense encompasses every attribute of the user, i.e., any characteristic or property of an entity that can be used to describe its state, appearance, or other aspects
- **Data interoperability**
  - Data formats that can be processed and ensure the same meaning across Metaverses
- **Self-Sovereign Digital Identity**
  - Aims to give people control of personal information
  - A new decentralized identifiers (DID) model where the user is at the center and controls the sharing of his or her identity
  - W3C Verifiable Credentials
- **Authentication**
  - Guaranteeing unicity of presence in a single Metaverse
- **The Schengen of Metaverses – Governance**
  - Trade-offs between online technical solutions and offline governance agreements

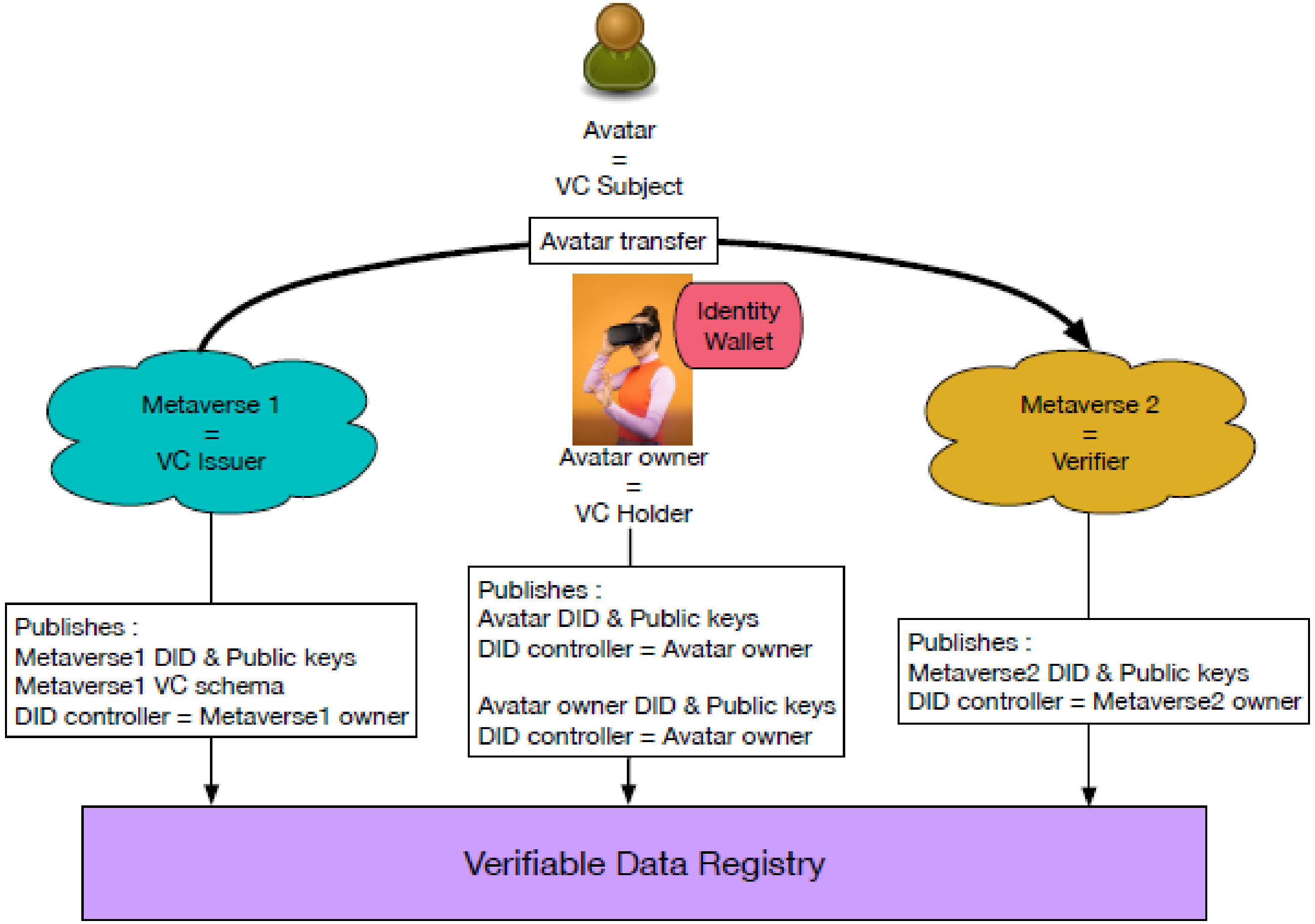
The W3C Verifiable Credentials architecture


Issuer
Issues VCs
Issue Credentials
Holder
Acquires, stores, presents VCs
Send Presentation
Verifier
Verifies VCs
Verify Identifiers and use Schemas
Register Identifiers and use Schemas
Verify Identifiers and Schemas
Verifiable Data Registry
Maintains identifiers and schemas

The W3C DID (Decentralized Identifiers) architecture



Proposal for travel identification between metaverses



Key takeaways

- **This journey of yours is full of promises!**
- **The discipline you chose to advance is at the centre of attention around the world**

- EU policies in the digital sphere have a large impact on our research in Computer Science
- EU policies in the digital sphere have a large impact on your future both as students and as individuals
  - Be aware
- The core fun may be over, but there are still great opportunities for our work!

- A new **International Research Centre** to be created at USP
  - CNRS
  - USP
  - FAPESP
- Interested graduate students and post-docs may apply for collaboration!

Obrigado pela atenção
e
Boa continuação na sua jornada!!

About the speaker and his institution

The French CNRS

- 30.000++ staff (**11.000 researchers**)
- 3 billion++ € annual budget
- 1.000++ research units
- 1.500++ **start-ups** since 2010
- 200++ **joint labs with industry**

- 20++ **Nobel** prizes / 10++ Medal **Fields**
- 1.1 billion++ € won in H2020
  - **1st beneficiary** of the Programme
- 70++ joint **laboratories in the world**
- All scientific domains
  - **Multidisciplinary** by design

Quick background of mine

- ✓**Director of research** in Algorithms, Optimisation, Networks, Cybersecurity, AI
- ✓Leading my lab in **three European projects**
- ✓**Head, European relations** for Digital matters at CNRS
- ✓**Policy maker** in Future and Emerging Technologies, Cybersecurity, and Privacy at the European Commission (until end March 2017)
- ✓**Foresight designer** and practitioner, mainly on the impact of the Digital Revolution and Digital Transformation
- ✓Working at the nexus of **Technology / Policy / Futures**
- ✓**Consulting** for Foreign Companies, EU Institutions, and European Projects