Data Protection by Design and Security by Design

Liane Colonna

Fall 2024

Overview

1. Technological revolution and the growing gap between emerging technolgies and the law
2. Potential models of governance that can help address the so-called “pacing problem”
3. Rulemaking through technical architecture
4. Data protection by design
5. Case study I
6. Security by design
7. Case study 2

Part I: Technological revolutions and the growing gap between emerging technolgies and the law

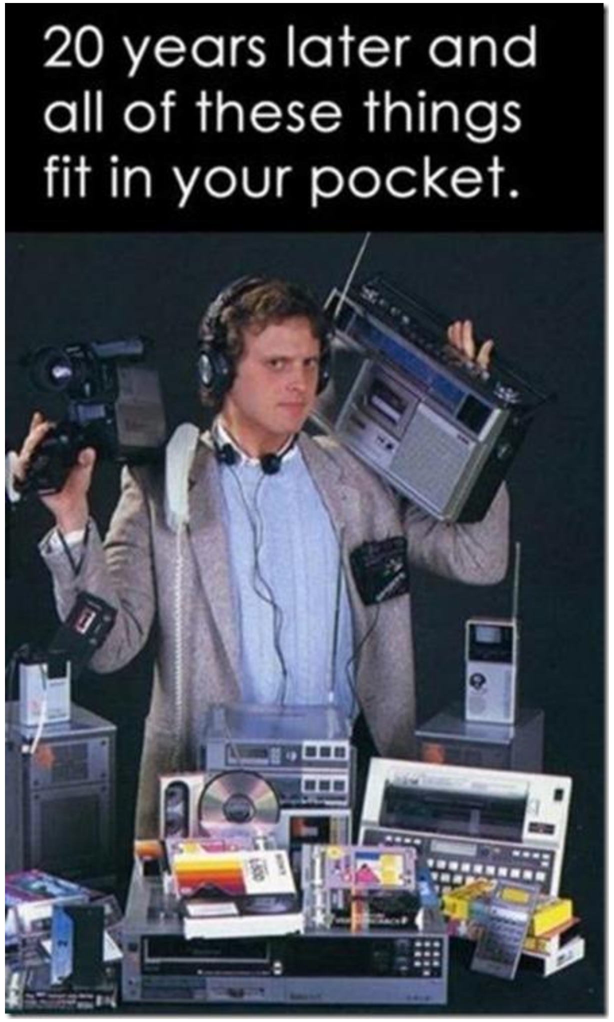
- information technologies,
- communication technologies,
- nanotechnologies,
- biotechnology,
- regenerative and reproductive medicine,
- robotics,
- neuroscience,
- surveillance technologies, and
- synthetic biology.

Moore’s Law

“computer chips are halving in price, or doubling in power every 18 months.”

- named for Gordon Moore, an Intel employee to whom this principle is attributed.

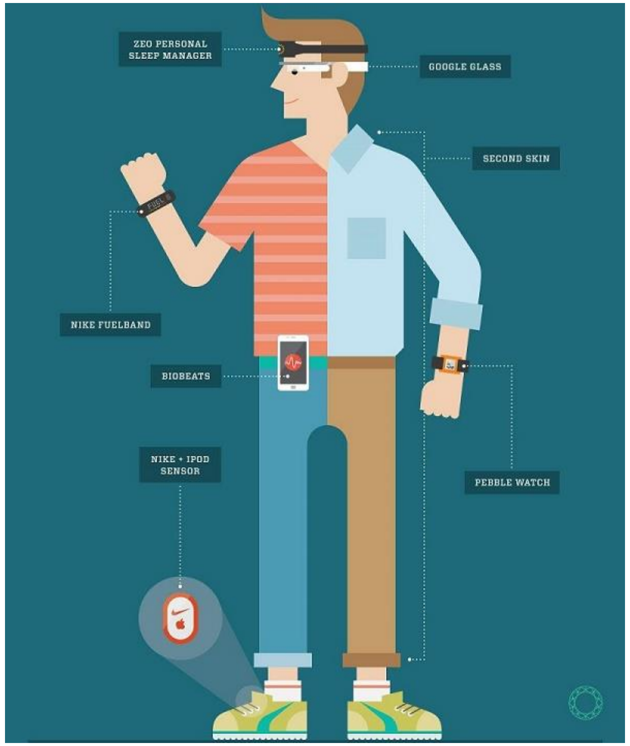
NOTE: Moore’s law *might* be dead



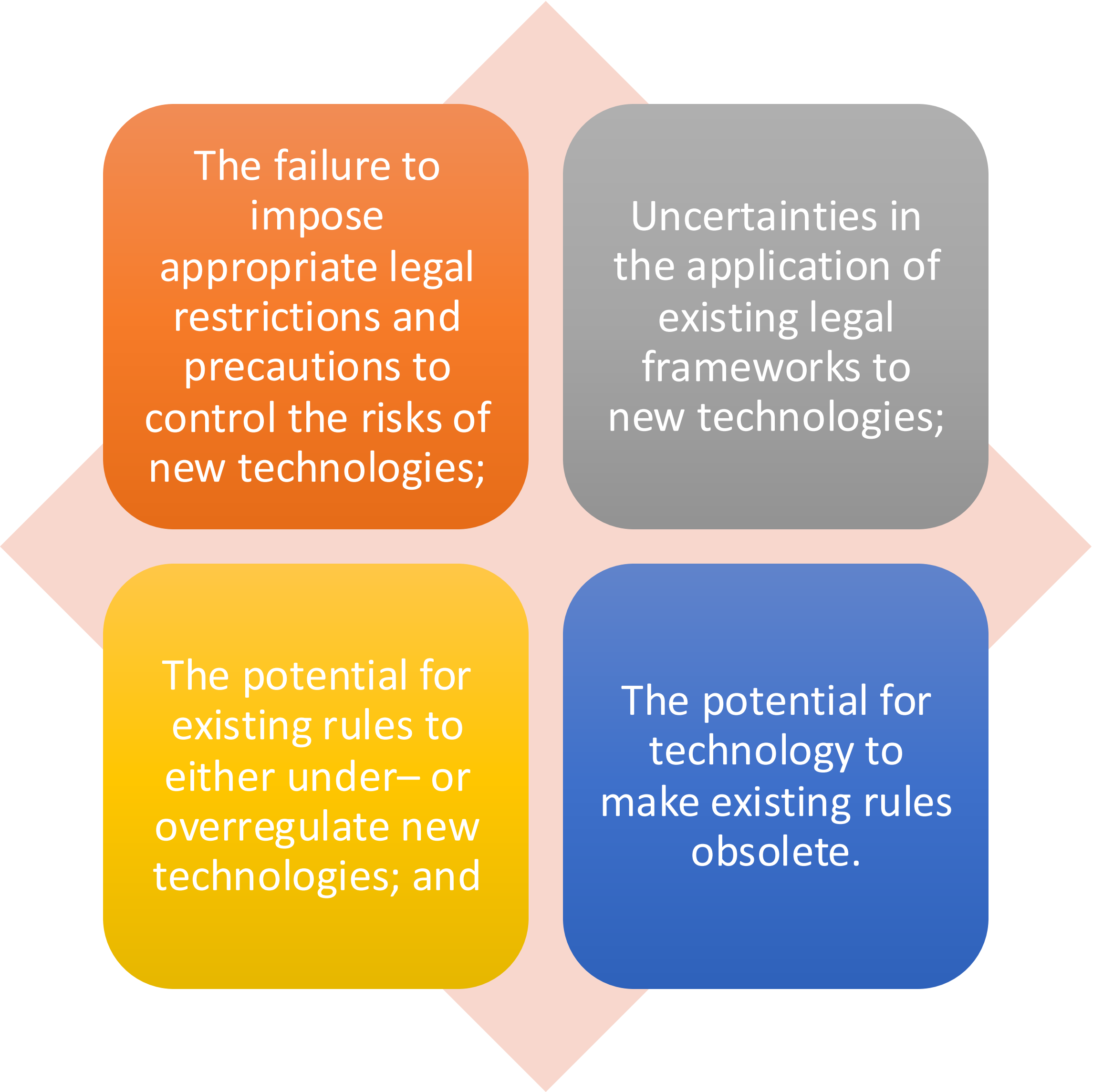
The growing gap between emerging technolgies and the law

- There is a growing gap between the rate of technological change and management of that change through legal mechanisms.
- The traditional legal tools of notice-and-comment rulemaking, legislation and judicial review are being left behind by emerging technologies

Example: Lifelogging



Problems that may result from the failure of law to keep pace with technology



The failure to impose appropriate legal restrictions and precautions to control the risks of new technologies;

Uncertainties in the application of existing legal frameworks to new technologies;

The potential for existing rules to either under– or overregulate new technologies; and

The potential for technology to make existing rules obsolete.

Part II: Models of regulation

- No regulation: let anarchy reign?
- Traditional government regulation
- International agreements and cooperation
- Self regulation
- Rule making through technical architecture
- Adaptive governance
- Soft law
- Institutional reform

No regulation: let anarchy reign?

“Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.” – John Perry Barlow (1996)

Models of regulation: traditional government regulation

- The traditional way of setting provisions and standards is that of government regulation by national legislators. This has the advantage of a legislative process and produces norms that at least theoretically are enforceable.

BUT

- The legislator often lacks sufficient technical knowledge for the preparation and enactment of legal provision. As such, the legislator is open to influence from the industry and there is a risk that legal norms will be shaped by lobbyists.
- The legislative democratic process is long and cumbersome in most countries, therefore, there is a risk that legal norms will be enacted and implemented only at a time when technical developments have advanced to a certain level (regulatory lag).
- Legislative norms are seldom flexible, since a change of law must be approved by democratically appointed bodies.

Models of regulation: International agreements and cooperation

- The global nature of communication networks invites realization of a legal framework on a global level.
- Four potential sources of law: international treaties and agreements, customary legal practices, general principles of law and traditional decisions.

BUT

- Very complex to do
- There are substantial differences that exist in the value-making processes of the participating nations
- Major poltical hurdles

Models of regulation: Self-regulation

- Allow private groups which – on their own initiative – makes decisions that limit their behavior, bound only by broad laws of general application
- Respond to real needs and mirror the technology , provides the opportunity to adapt the legal framework to changing technology in a flexible way, self-regulation can usually be implemented at reduced costs.
- BUT the creation of self regulatory provisions are not generally binding in legal terms and often lack enforcement procedures

Models of regulation: Adaptive governance

Implement processes that permit frequent and ongoing reevaluation and revisions of regulatory programs to address changing facts and circumstances.

Models of regulation: Soft law I

- Soft-law approaches involve a variety of instruments that establish substantive goals or norms that are not directly enforceable
- Examples of soft law include recommendations, guidelines, codes of conduct, non-binding resolutions, and standards.

Models of regulation: Soft law II

Soft law/governance approaches to oversight offer a number of potential advantages, including:

- they are usually based on cooperative models of engagement;
- they can be adopted or revised relatively quickly;
- many different soft law/governance concepts can be attempted simultaneously; and
- such measures can be gradually “hardened” into more formal regulatory instruments.

(Abbott and Snidal 2000; Gersen and Posner 2008).

Models of regulation: Institutional reform

- Various types of institutional reforms can also help to address the Pacing Problem
- E.g. structural changes within existing agencies, such as creating a safety reporting system for reporting and studying errors

Models of regulation:Collaborative governance

- Middle Ground Approach: Collaborative governance serves as a balanced alternative between strict command-and-control regulation and self-regulation, seeking to leverage the strengths of both approaches.
- Involvement of Multiple Stakeholders: It involves collaboration between public and private sectors, as well as other stakeholders, to create more effective and adaptable regulatory frameworks.
- Enhanced Compliance and Efficiency: By engaging those directly affected by regulations, collaborative governance can lead to greater buy-in, adherence, and a more efficient regulatory process.

“The post regulatory state”(Scott)

Rulemaking is shifting from a substantive and centralized approach (“command and control”) towards one that is decentralized, adaptable and reflexive!

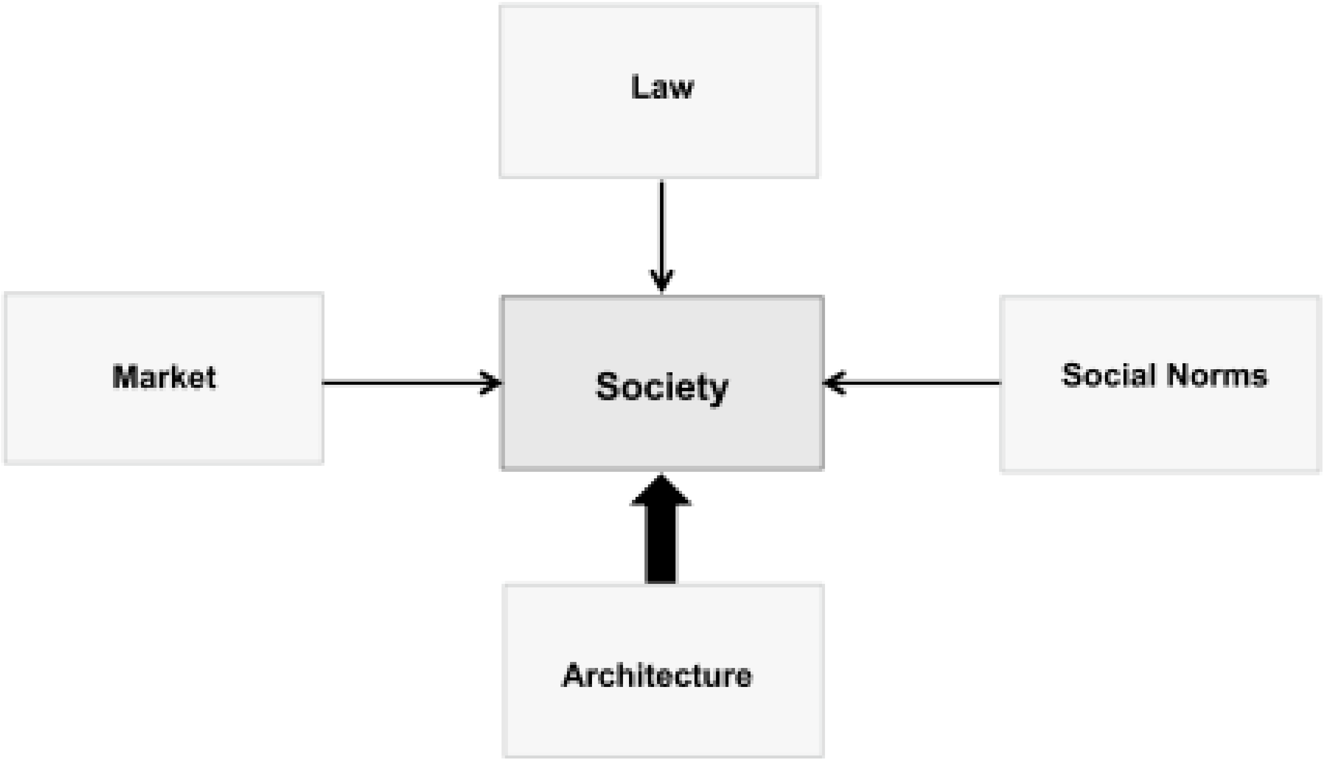
Part III: Rulemaking through technical architecture

- The legal framework needs to pay serious attention to the technological environment.
- Code-based regulation
- Lex informatica

Law of the horse

Internet-specific approaches are tantamount in irrationality to suggesting a “law of the horse.”

Four modalities comprising cyber law



Law

Regulates behavior through commands of the form: If you do X (or fail to do X), you will incur penalty Y.

Market forces

“Market forces encourage architectures of identity to facilitate online commerce. Government needs to do very little -- indeed, nothing at all -- to induce just this sort of development. The market forces are too powerful; the potential here is too great."

Social norms

"Talk about Democratic politics in the alt knitting newsgroup, and you open yourself to flaming, "spoof" someone's identify in a MUD, and you may find yourself... "toaded" (take off and die) filter.

Architecture (computer software and hardware)

“The code or software or architecture or protocols set these features, which are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it too is regulation, just as the architectures of real-space codes are regulations."

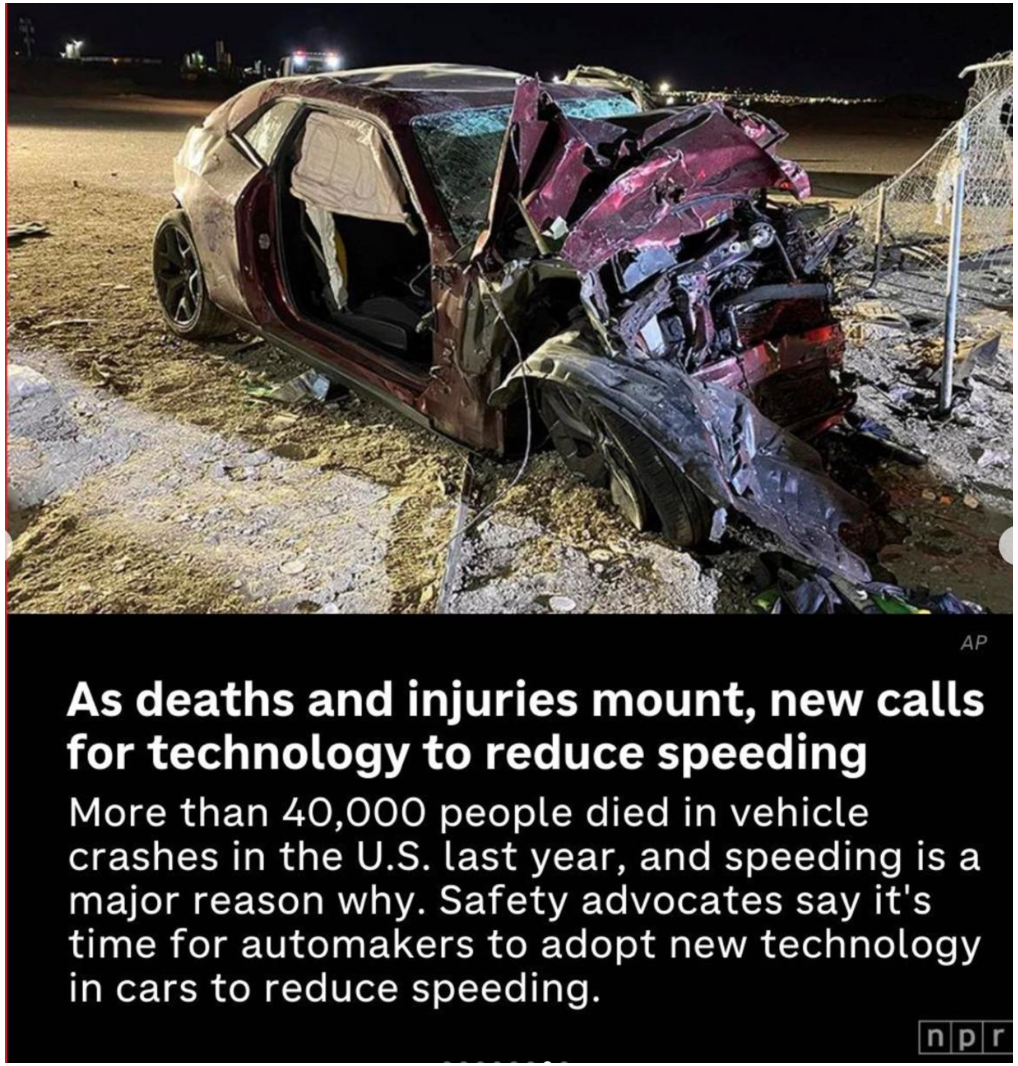
Code is law

The programmers writing the code that runs the Internet have become lawgivers-setting the rules of permissible behavior on the Internet.

- Code "can, and increasingly will, displace law", leading to a world in which "effective regulatory power (shifts) from law to code, from severance to software.”

Lessig in a nutshell

Governments should not impose regulation for problems that could be solved otherwise, particularly if complex technology drives the processes. However, cyberspace cannot function without a minimal legal framework



AP

As deaths and injuries mount, new calls for technology to reduce speeding

More than 40,000 people died in vehicle crashes in the U.S. last year, and speeding is a major reason why. Safety advocates say it's time for automakers to adopt new technology in cars to reduce speeding.

Law Merchant

A distinct set of rules that developed with the new, rapid boundary-crossing trade of the Middle Ages.

Lex informatica

	Legal Regulation	***Lex Informatica***
Framework	Law	Architectural standards
Jurisdiction	Physical territory	Networks
Content	Statutory/court expression	Technical
Capabilities	Customary	Practice
Sources	State	Technologist
Customized rules	Contract	Configurations
Customization process	Low Cost Moderate Cost Standard Form High Cost Negotiation	Off-the-Shelf Configuration Installable Configuration User Choice
Primary Enforcement	Court	Automated Self-execution

Techno-regulation

- “The intentional influencing of individuals’ behaviour by embedding norms into technological systems and devices.” (Bayamlıoğlu and Leenes)
- Examples:
  - driving controls in cars
  - internet filtering,
  - Digital Rights Management systems
  - speed bumps

Part IV: Data Protection by Design

Privacy Enhancing Technologies

“Technologies designed to provide privacy protection from untrusted and potentially adversarial data controllers” (Diaz, Tene, and Gürses)

Hard and soft PETs Rubinstein and Good (2020)

Another classification of PETs used by Rubinstein and Good (2020) differentiates between hard and soft PETs.

- Hard PETs avoid placing any trust on any third party, which means that the data is minimized to the fullest extent possible, and data sharing is avoided.
- On the other hand, soft PETs ask how data can be shared with trusted parties only and manage such trusted data sharing practices.

ENISA

PETs are “a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system”.

- Truth-preserving
- Intelligibility-preserving
- Operable Technology

UK Information Commissioner’s Office (ICO) guidance on PETs (2023)

It provides information on a number of key PETs, including:

- Differential privacy: generates anonymous statistics, usually by randomising the computation process that adds noise to the output.
- Synthetic data: provides realistic datasets in environments where access to large real datasets is not possible.
- Homomorphic encryption: provides strong security and confidentiality by enabling computations on encrypted data without first decrypting it.
- Zero-knowledge proofs (ZKP): provide data minimisation by enabling parties to prove private information about themselves without revealing what it actually is.
- Trusted execution environments: enhance security by enabling processing by a secure part of a computer processor that is isolated from the main operating system and other applications.
- Secure multiparty computation (SMPC): provides data minimisation and security by allowing different parties to jointly perform processing on their combined information, without sharing all information with each other.
- Federated learning: trains machine learning models in distributed settings while minimising the amount of personal information shared with each party, usually in combination with other PETs.

Privacy by Design AKA Cavoukian’s commandments

- “Be proactive, not reactive; preventing privacy issues before they arise, rather than remedying them afterward.”
- “Embed privacy into the very design of technologies, processes, and practices, making it an integral and inseparable aspect.”
- “Strive for full functionality, achieving both privacy and other objectives in a positive-sum manner, instead of compromising one for the other.”
- “Respect user privacy, keeping it usercentric, and providing individuals with control and choices regarding their personal information.”
- “Secure personal information end-to-end, protecting it throughout its entire lifecycle from collection to disposal”
- "Maintain visibility and transparency, keeping privacy practices open and verifiable for all stakeholders.”

Data Protection by Design

An existing concept evolving

Privacy enhancing technologies (PETS)

Privacy by design (technology PLUS organizational tools)

Privacy by default

Different philosophies at work: Technical AND organizational principle

New emphasize on the design stage (timing)

As a policy issue highly complex

Today: Article 25 GDPR, Data protection by design and by default + new requirements in AI Act

Article 25 Data protection by design and by default

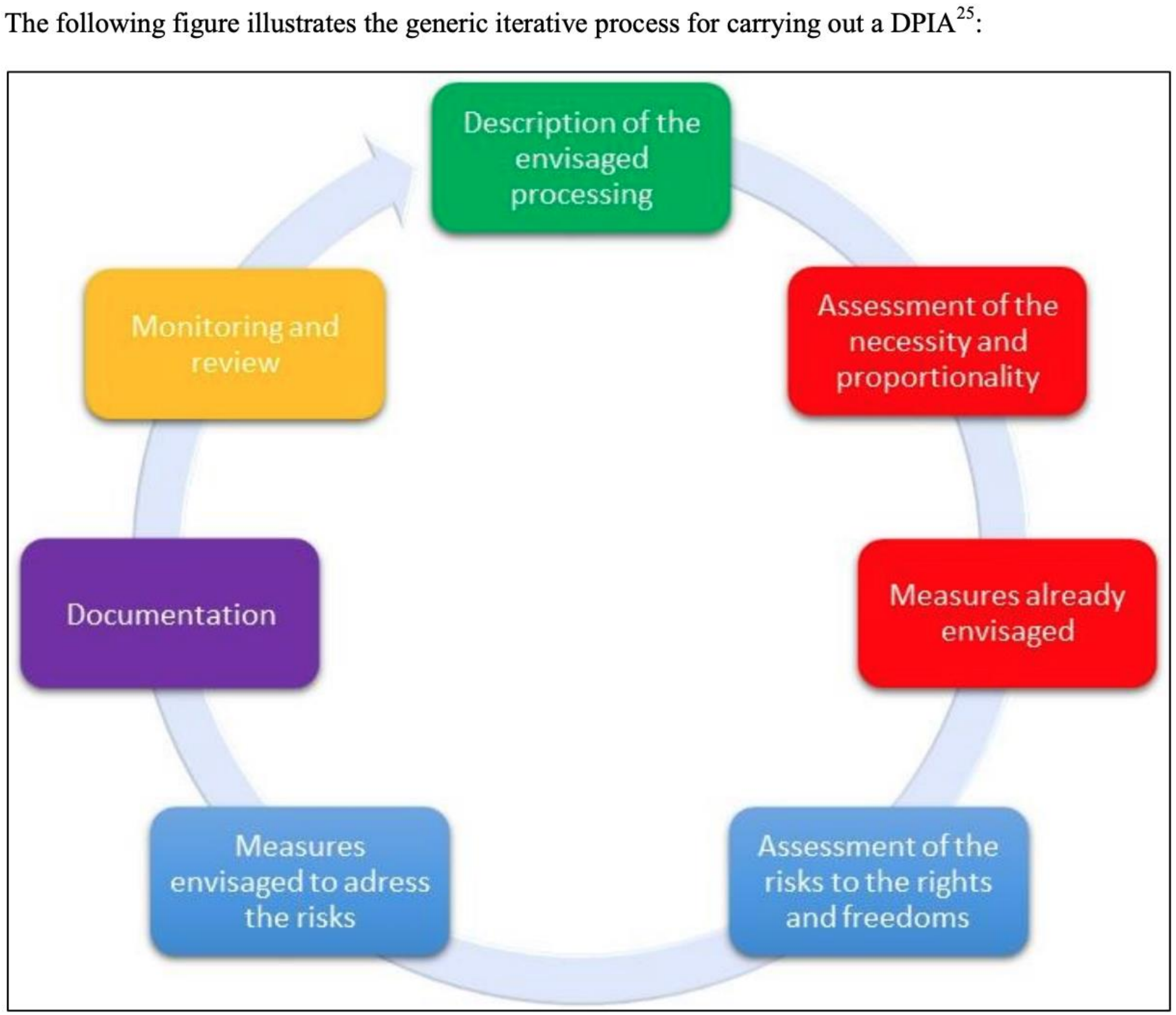
1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Data protection by default

- DPbDf involves “minimising the amount of personal data collected and restricting their dissemination, independently of data subjects’ intervention.” (Bygrave)
- DPbDf denotes “making choices regarding configuration values or processing options that are set or prescribed in a processing system, such as a software application, service or device, or a manual processing procedure that affect the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility." (EDPB)

Organizational means to protection privacy

- Data Protection Impact Assessments
- Employee trainings
- Data breach response plans
- Regular audits to e.g. uncover security vulnerabilities
- Security risk assessment



The following figure illustrates the generic iterative process for carrying out a DPIA[25]:

Description of the envisaged processing
Assessment of the necessity and proportionality
Measures already envisaged
Assessment of the risks to the rights and freedoms
Measures envisaged to adress the risks
Documentation
Monitoring and review

4 clusters of different technical means to protect privacy Tamò-Larrieux (2018)

- Security tools
- Anonymity tools
- Autonomy tools
- Transparency tools

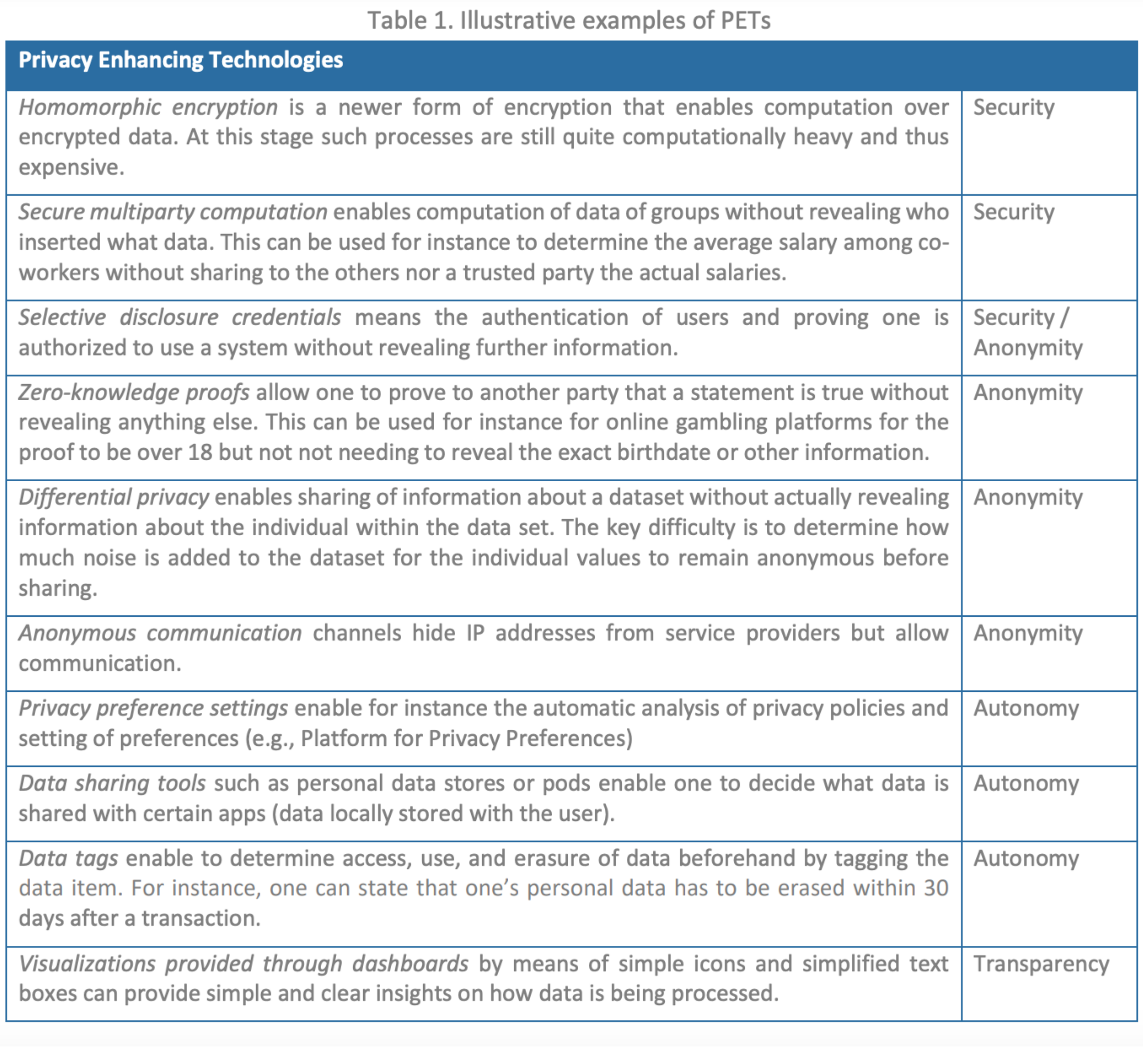


Table 1. Illustrative examples of PETs

Privacy Enhancing Technologies	
Homomorphic encryption is a newer form of encryption that enables computation over encrypted data. At this stage such processes are still quite computationally heavy and thus expensive.	Security
Secure multiparty computation enables computation of data of groups without revealing who inserted what data. This can be used for instance to determine the average salary among co-workers without sharing to the others nor a trusted party the actual salaries.	Security
Selective disclosure credentials means the authentication of users and proving one is authorized to use a system without revealing further information.	Security / Anonymity
Zero-knowledge proofs allow one to prove to another party that a statement is true without revealing anything else. This can be used for instance for online gambling platforms for the proof to be over 18 but not not needing to reveal the exact birthdate or other information.	Anonymity
Differential privacy enables sharing of information about a dataset without actually revealing information about the individual within the data set. The key difficulty is to determine how much noise is added to the dataset for the individual values to remain anonymous before sharing.	Anonymity
Anonymous communication channels hide IP addresses from service providers but allow communication.	Anonymity
Privacy preference settings enable for instance the automatic analysis of privacy policies and setting of preferences (e.g., Platform for Privacy Preferences)	Autonomy
Data sharing tools such as personal data stores or pods enable one to decide what data is shared with certain apps (data locally stored with the user).	Autonomy
Data tags enable to determine access, use, and erasure of data beforehand by tagging the data item. For instance, one can state that one's personal data has to be erased within 30 days after a transaction.	Autonomy
Visualizations provided through dashboards by means of simple icons and simplified text boxes can provide simple and clear insights on how data is being processed.	Transparency

Anonymous data

- Any information from which the person to whom the data relates cannot be identified, whether by the company processing the data or by any other person (Is that even possible?)
- Outside the scope of EU data protection law.
- “The principles of data protection should … not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.” (Recital 26)

Anonymization versus De-identification

- Data anonymization is often considered synonymous with de-identification.
- In fact, the Article 29 Working Party defines anonymization as “a technique applied to personal data in order to achieve **irreversible** *de-identification*.” (the zero-risk test)
    - However, it is important to note that the key word is “irreversible” as, according to the ISO, “any process of reducing the association between a set of identifying data and the data subject” is considered de-identification.
    - The Working Party's approach is so stringent that it equates anonymization with the complete erasure of data.

In order to achieve “anonymization,” the process must be irreversible, at least according to the Article 29 Working Party (now the European Data Protection Board (EDPB))

Does the GDPR perceive anonymization as a risk management process?

“reasonableness” standard

- allows for risk-based assessments or an “**impossibility**” standard

New approaches are needed to quantify the risk of re-identification in an effort to understand the impact of different options for data release!!!

“impossibility” standard

- data may be rendered anonymous only when it is zero (or near-zero) probability of reidentification

The Article 29 Working Party recognizes that there is an “inherent residual risk of re-identification linked to any technical-organizational measure aimed at rendering data ‘anonymous’ yet italso states, anonymization must ‘achieve irreversible deidentification.’”

Data Utility

“Data can be either useful or perfectly anonymous but never both” – Ohm

Pseudonymization

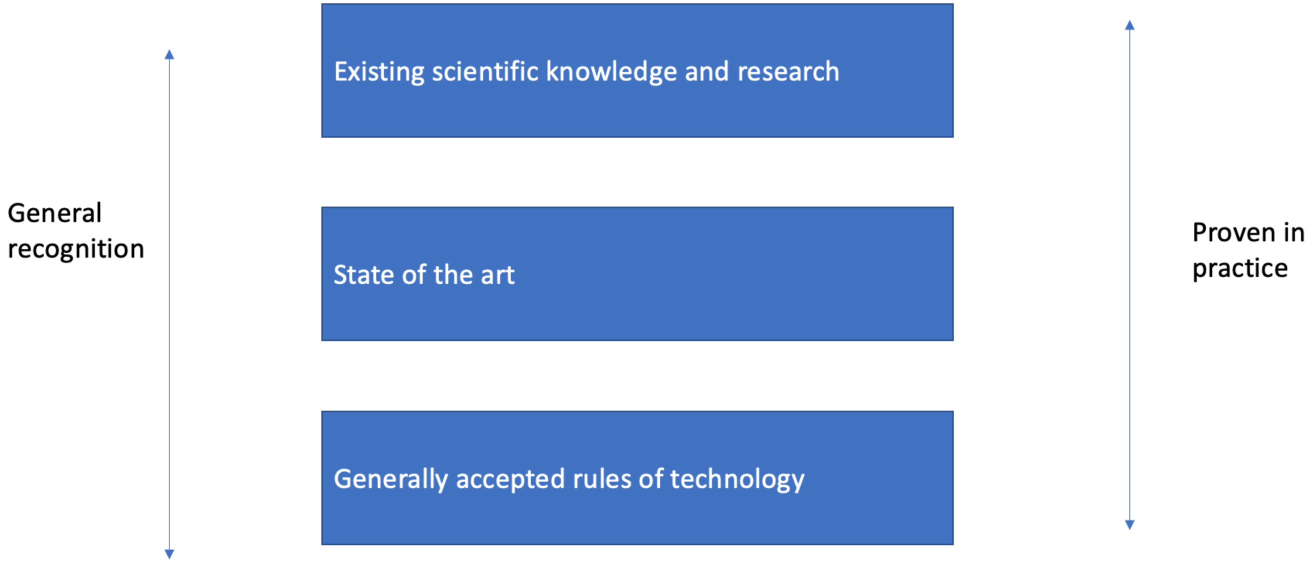
"'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is **kept separately** and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" -- Article 4(5) GDPR

Encryption

Encryption seems to be included within the ambit of pseudonymization so long as the encryption “key” is kept separate and secure, and data administrators implement appropriate measures to prevent the “unauthorized reversal of pseudonymization.”(GDPR, Recital 75)

OBS!!! Encryption is not an anonymization technique, but it can be a powerful pseudonymisation tool.

The State of the Art



General recognition

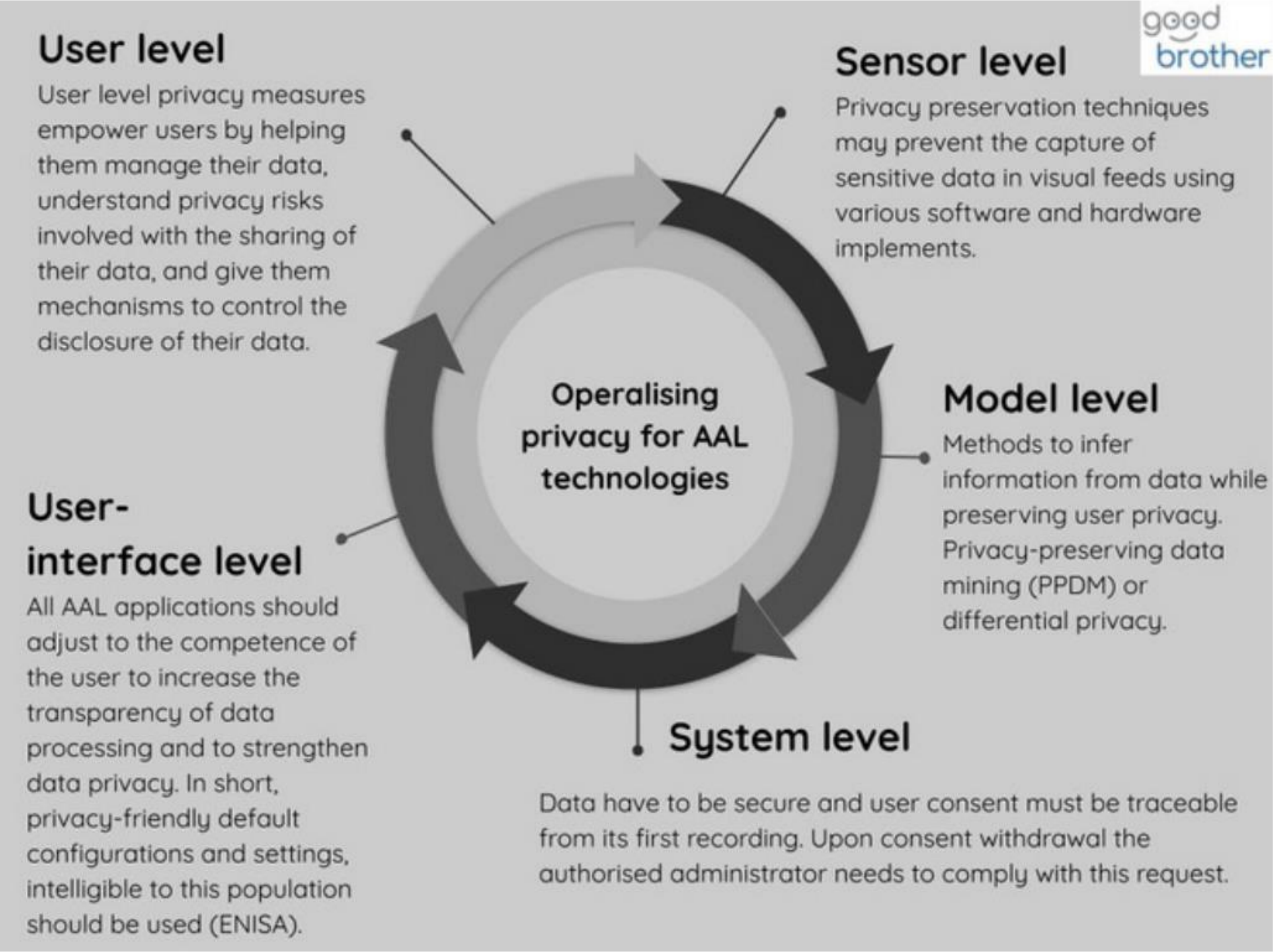
Existing scientific knowledge and research

State of the art

Generally accepted rules of technology

Proven in practice

Federal Constitutional Court’s Kalkar decision (1978)
Source: TeleTrusT – IT Security Association Germany, Guidelines State of the Art, 2020
(in co-operation with ENISA)



Operalising privacy for AAL technologies

User level

User level privacy measures empower users by helping them manage their data, understand privacy risks involved with the sharing of their data, and give them mechanisms to control the disclosure of their data.

Sensor level

Privacy preservation techniques may prevent the capture of sensitive data in visual feeds using various software and hardware implements.

Model level

Methods to infer information from data while preserving user privacy. Privacy-preserving data mining (PPDM) or differential privacy.

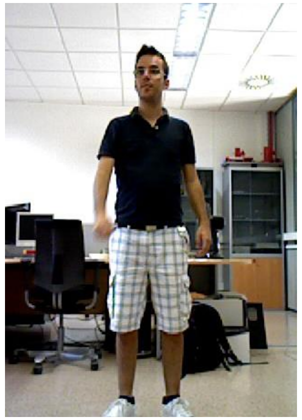
System level

Data have to be secure and user consent must be traceable from its first recording. Upon consent withdrawal the authorised administrator needs to comply with this request.

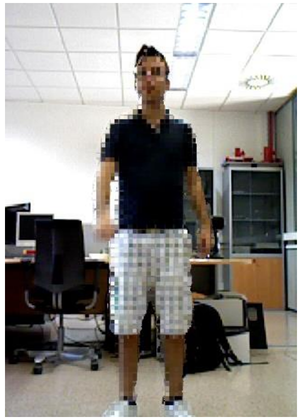
User-interface level

All AAL applications should adjust to the competence of the user to increase the transparency of data processing and to strengthen data privacy. In short, privacy-friendly default configurations and settings, intelligible to this population should be used (ENISA).

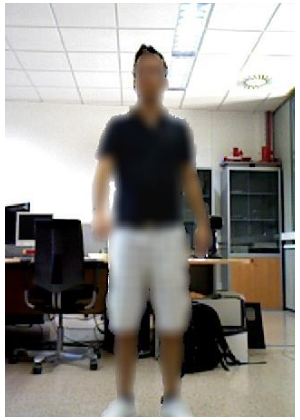
Alex Mihaildis and Liane Colonna, A Methodological Approach to Privacy by Design within the Context of Lifelogging Technologies



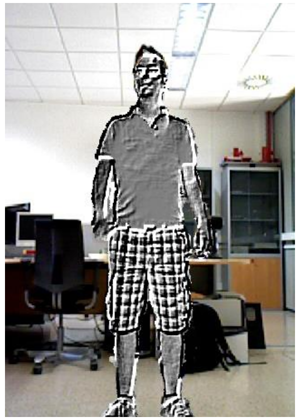
Original



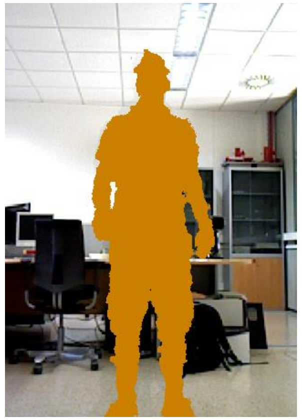
Pixelate



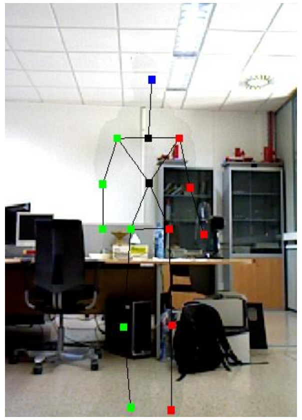
Blur



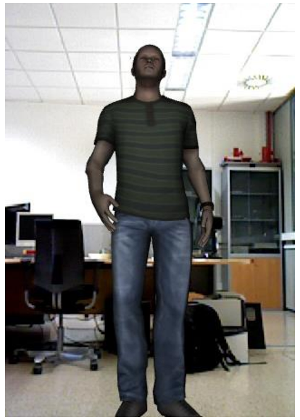
Emboss



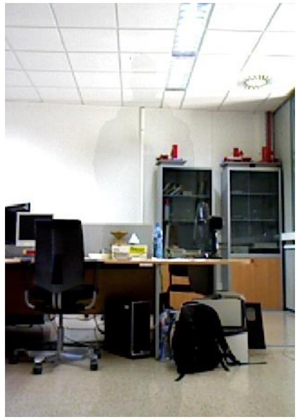
Silhouette



Skeleton



Avatar



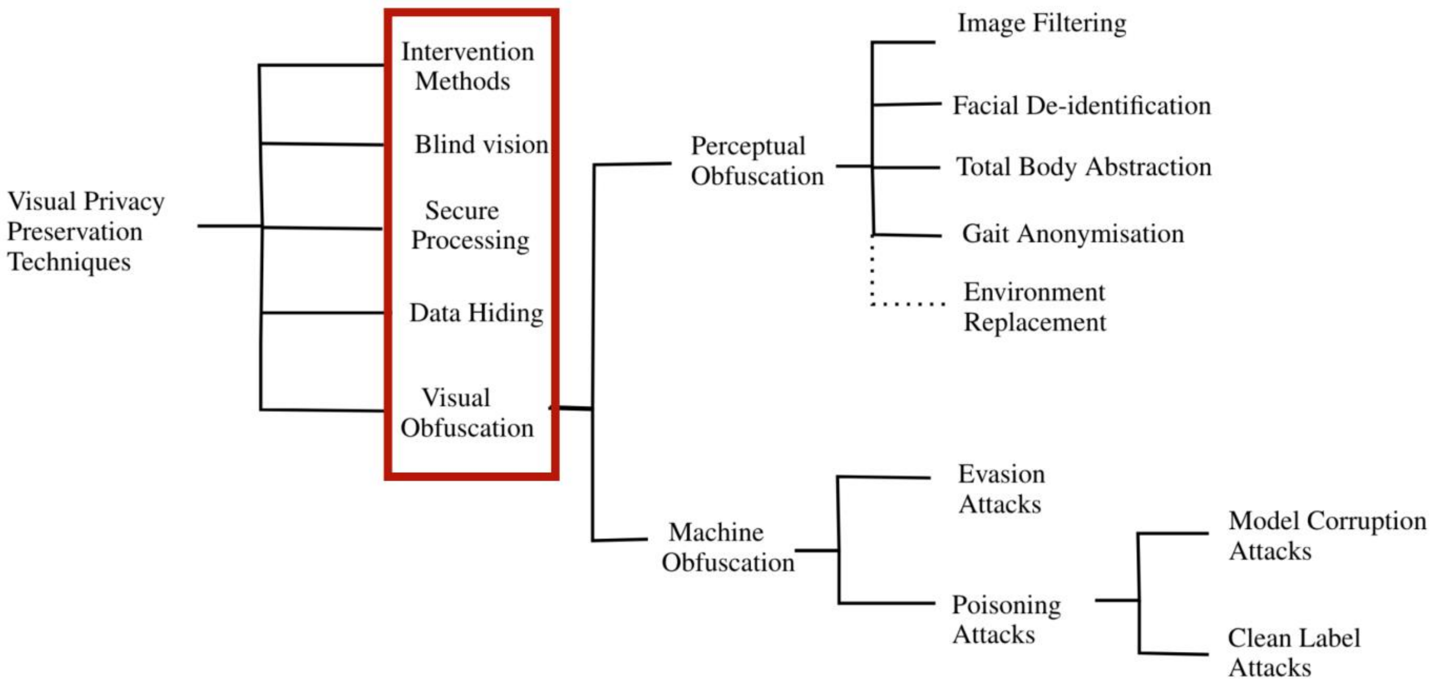
Invisibility

paal
Privacy-Aware and
Acceptable Lifelogging
services for older and frail people

Francisco
Florez-
Revuelta

A taxonomy of VPETs

- A taxonomy of Visual Privacy Enhancing Technologies (VPETs) was created during literature review (Ravi et al., 2021).
- 5 major categories.
- Connected to the taxonomy for privacy by design proposed in Mihailidis & Colonna (2020).



Sources:
Ravi, S., Climent-Pérez, P., & Florez-Revuelta, F. (2021). A Review on Visual Privacy Preservation Techniques for Active and Assisted Living *(arXiv:2112.09422). arXiv. (To appear in Multimedia Tools and Applications)*
Mihaildis, A., & Colonna, L. (2020). A Methodological Approach to Privacy by Design within the Context of Lifelogging Technologies. *Rutgers Computer and Technology Law Journal, 46, 1.*

V: Case Study I

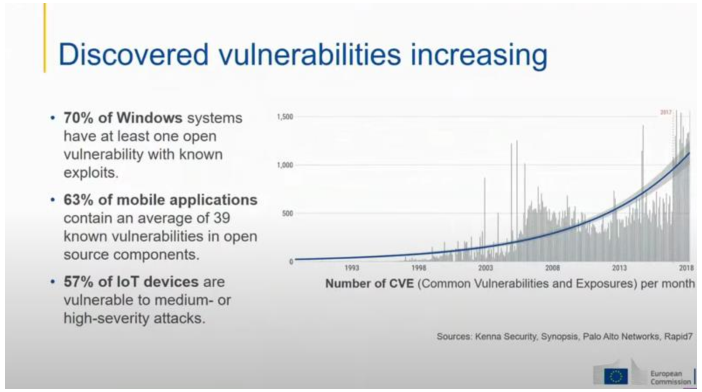
Elsa, a 77-year-old retired widow, lives alone in an urban area of Stockholm. She uses an analogue mobile phone and is not very familiar with modern technology. Elsa has a history of falls, particularly in the bathroom at night, which raises concerns for her safety.

Her son, Hans, who lives in Copenhagen, is worried about her well-being and has decided to install a video monitoring system in her home. This system is designed to detect falls and automatically send an alarm signal, along with an image, to Hans and Elsa's healthcare provider if a fall occurs.

However, Elsa is deeply concerned about her privacy and the security of the device. She is afraid that the camera in the bathroom will allow someone to see her naked and that hackers could access and misuse these images. Elsa is also uncomfortable with the idea of having a camera in her home, as it makes her feel like she is being watched constantly. Additionally, she is worried about the reactions of her friends, who frequently visit her home. She fears they will feel uncomfortable or avoid visiting altogether, leading to increased loneliness.

What legal obligations must be considered when implementing this video monitoring system under GDPR, particularly in terms of data protection by design and by default? How would you ensure that the system complies with these regulations while respecting Elsa's privacy? What rights does Elsa have if something goes wrong?

Part VI: Security by Design of non personal data in the proposed EU Cyber Resilience Act (+ AI Act)

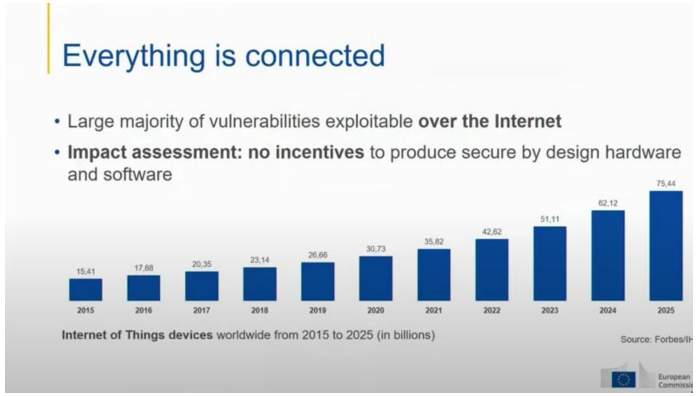


Discovered vulnerabilities increasing

- **70% of Windows** systems have at least one open vulnerability with known exploits.
- **63% of mobile applications** contain an average of 39 known vulnerabilities in open source components.
- **57% of IoT devices** are vulnerable to medium- or high-severity attacks.

Number of CVE (Common Vulnerabilities and Exposures) per month

Sources: Kenna Security, Synopsis, Palo Alto Networks, Rapid7

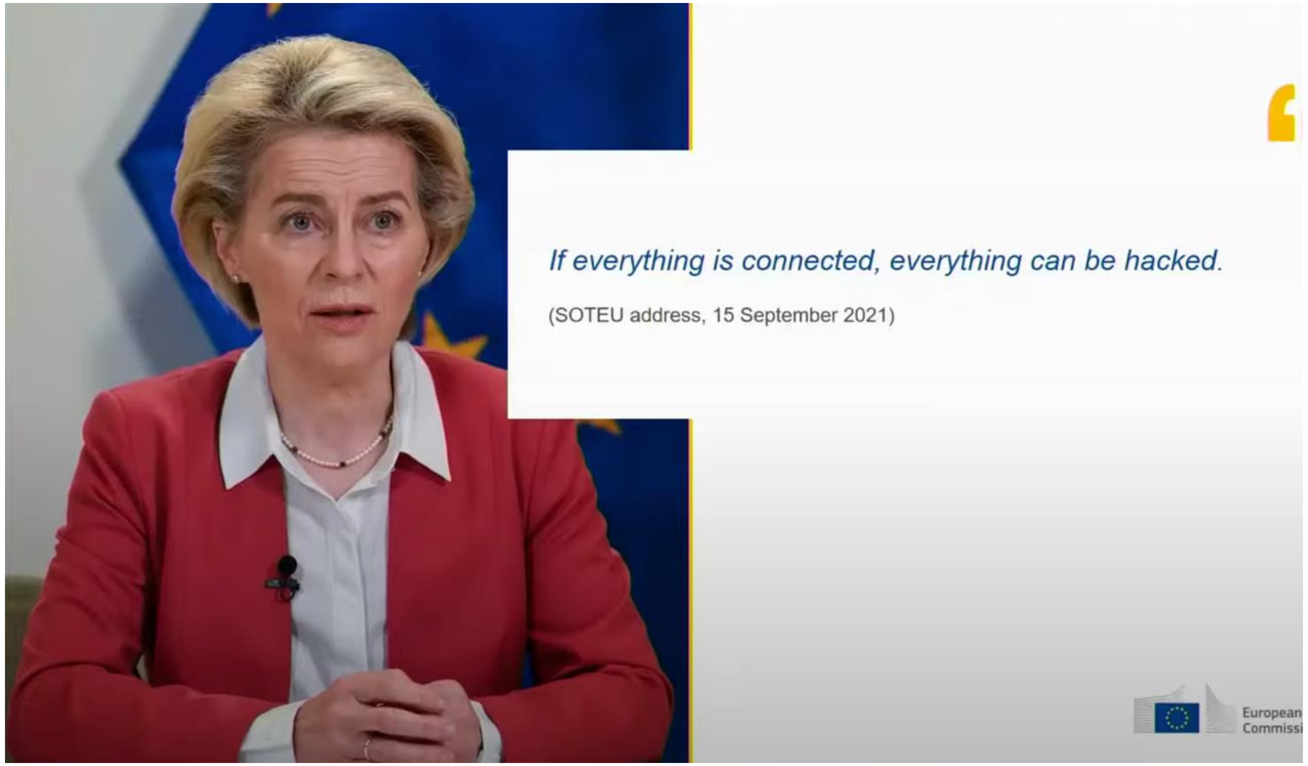


Everything is connected

- Large majority of vulnerabilities exploitable **over the Internet**
- **Impact assessment: no incentives** to produce secure by design hardware and software

Internet of Things devices worldwide from 2015 to 2025 (in billions)

Source: Forbes/IH



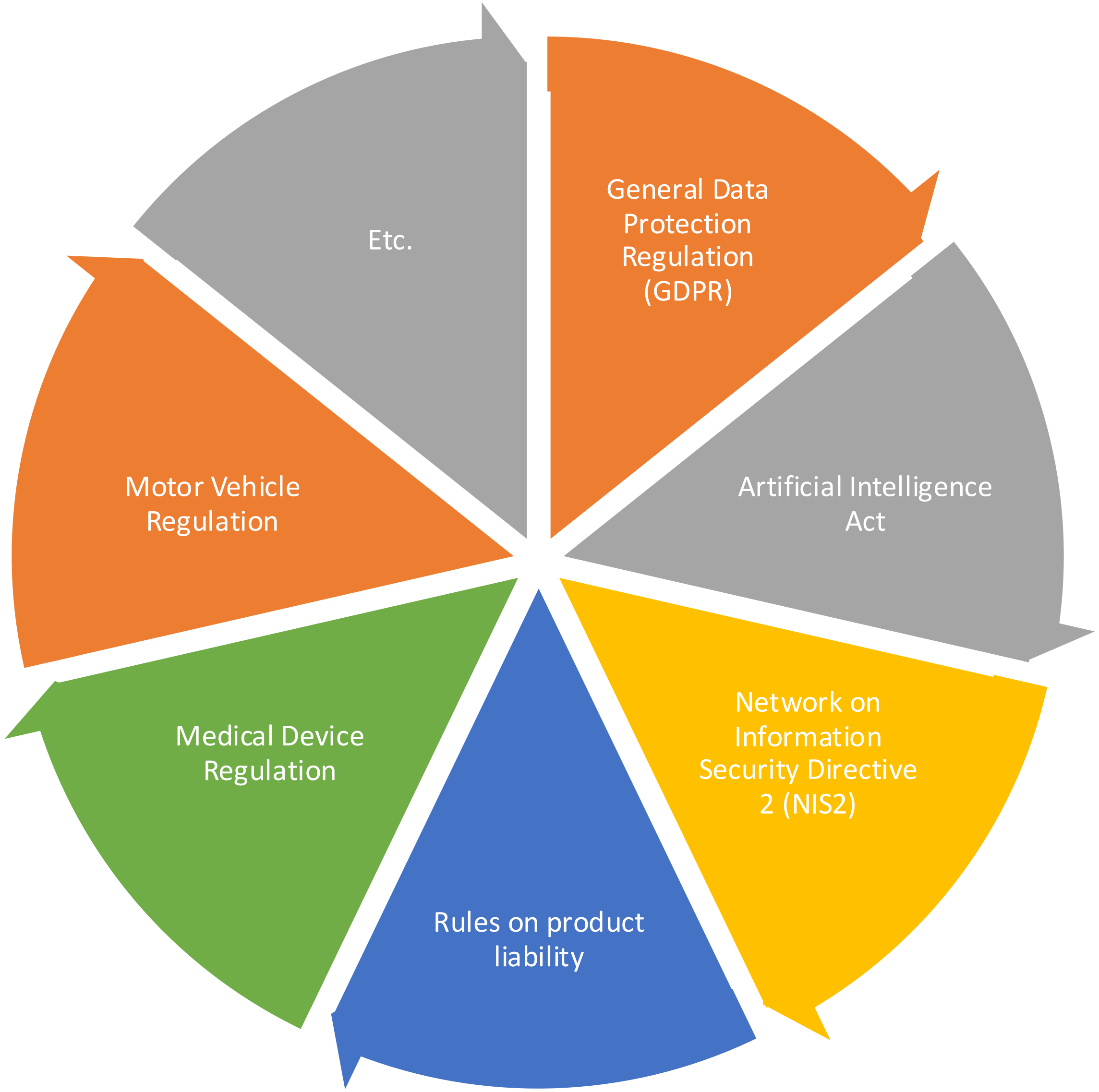
If everything is connected, everything can be hacked.

(SOTEU address, 15 September 2021)

CRA in a nutshell

Main elements of the proposal

Overlap and interaction:


General Data Protection Regulation (GDPR)
Artificial Intelligence Act
Network on Information Security Directive 2 (NIS2)
Rules on product liability
Medical Device Regulation
Motor Vehicle Regulation
Etc.

Scope

Products with digital elements:

- Hardware products and components placed on the market separately, such as laptops, smart appliances, mobile phones, network equipment or CPUs
- Software products and components placed on the market separately, such as operating systems, word processing, games or mobile apps
- The definition of "products with digital elements" also includes remote data processing solutions

- Not covered:
  - non-commercial projects, including open source in so far as a project is not part of a commercial activity
  - services, in particular cloud/software as a service - covered by NIS2
- Outright exclusions:
  - certain products sufficiently regulated on cybersecurity (cars, medical devices, in vitro, certified aeronautical equipment) under the new and old approach

ANNEX III: Important Products with Digital Elements

Class I

1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
2. Standalone and embedded browsers
3. Password managers
4. Software that searches for, removes, or quarantines malicious software
5. Products with digital elements with the function of virtual private network (VPN)
6. Network management systems
7. Security information and event management (SIEM) systems
8. Boot managers
9. Public key infrastructure and digital certificate issuance software
10. Physical and virtual network interfaces
11. Operating systems
12. Routers, modems intended for the connection to the internet, and switches …

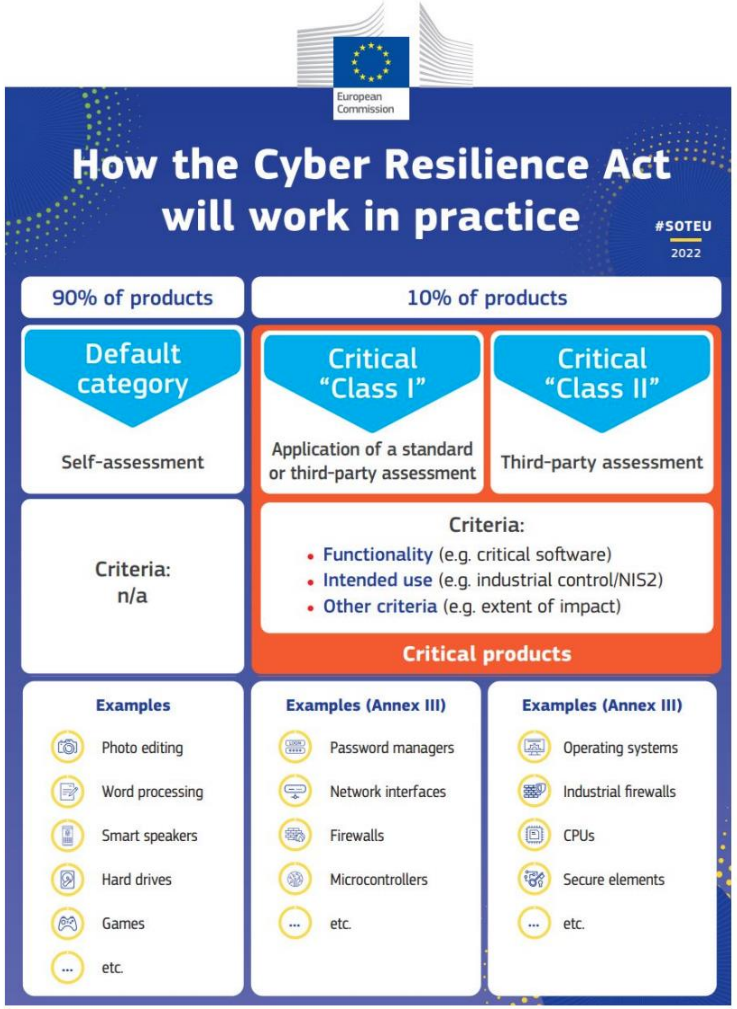
Class II

1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
2. Firewalls, intrusion detection and prevention systems
3. Tamper-resistant microprocessors
4. Tamper-resistant microcontrollers

ANNEX IV Critical Products with Digital Elements

1. Hardware Devices with Security Boxes
2. Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) and other devices for advanced security purposes, including for secure cryptoprocessing
3. Smartcards or similar devices, including secure elements

Risk based approach



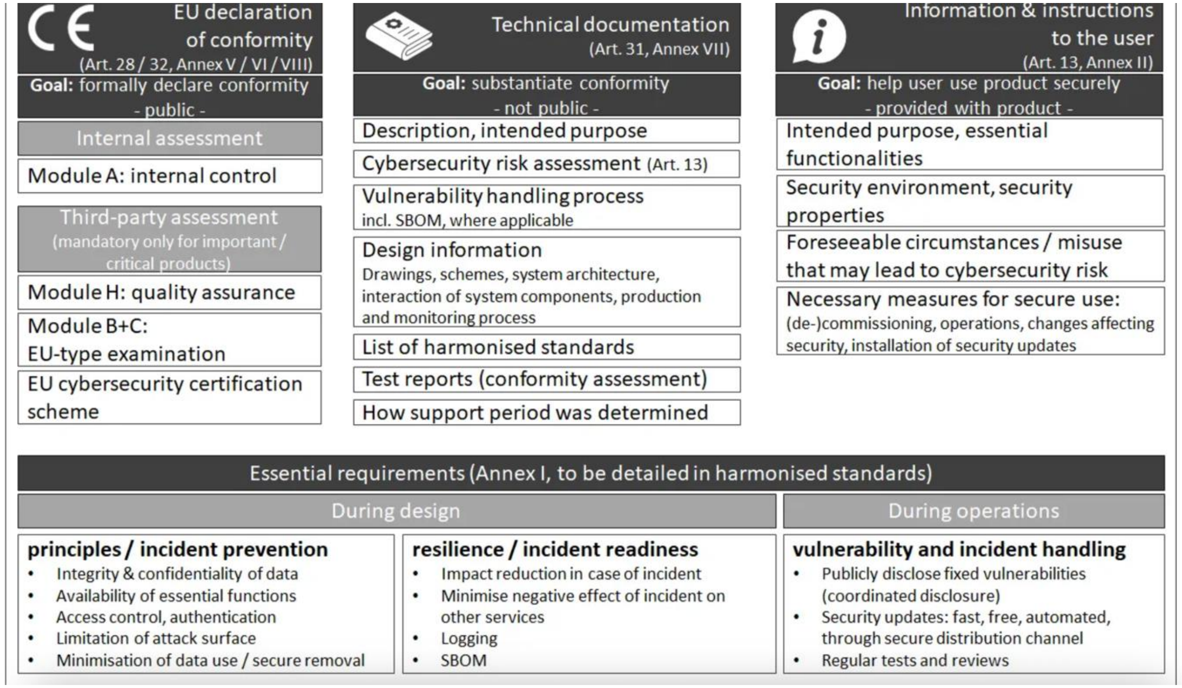
European Commission

How the Cyber Resilience Act will work in practice

#SOTEU 2022

90% of products	10% of products	
Default category Self-assessment	**Critical "Class I"** Application of a standard or third-party assessment	**Critical "Class II"** Third-party assessment
Criteria: n/a	Criteria: • **Functionality** (e.g. critical software) • **Intended use** (e.g. industrial control/NIS2) • **Other criteria** (e.g. extent of impact) **Critical products**	
Examples Photo editing Word processing Smart speakers Hard drives Games etc.	**Examples (Annex III)** Password managers Network interfaces Firewalls Microcontrollers etc.	**Examples (Annex III)** Operating systems Industrial firewalls CPUs Secure elements etc.

CRA stakeholders and responsibilities: Manufacturers



EU declaration of conformity (Art. 28 / 32, Annex V / VI / VIII)

Goal: formally declare conformity - public -

Internal assessment

- Module A: internal control

Third-party assessment (mandatory only for important / critical products)

- Module H: quality assurance
- Module B+C: EU-type examination
- EU cybersecurity certification scheme

Technical documentation (Art. 31, Annex VII)

Goal: substantiate conformity - not public -

- Description, intended purpose
- Cybersecurity risk assessment (Art. 13)
- Vulnerability handling process incl. SBOM, where applicable
- Design information: Drawings, schemes, system architecture, interaction of system components, production and monitoring process
- List of harmonised standards
- Test reports (conformity assessment)
- How support period was determined

Information & instructions to the user (Art. 13, Annex II)

Goal: help user use product securely - provided with product -

- Intended purpose, essential functionalities
- Security environment, security properties
- Foreseeable circumstances / misuse that may lead to cybersecurity risk
- Necessary measures for secure use: (de-)commissioning, operations, changes affecting security, installation of security updates

Essential requirements (Annex I, to be detailed in harmonised standards)

During design

principles / incident prevention

- Integrity & confidentiality of data
- Availability of essential functions
- Access control, authentication
- Limitation of attack surface
- Minimisation of data use / secure removal

resilience / incident readiness

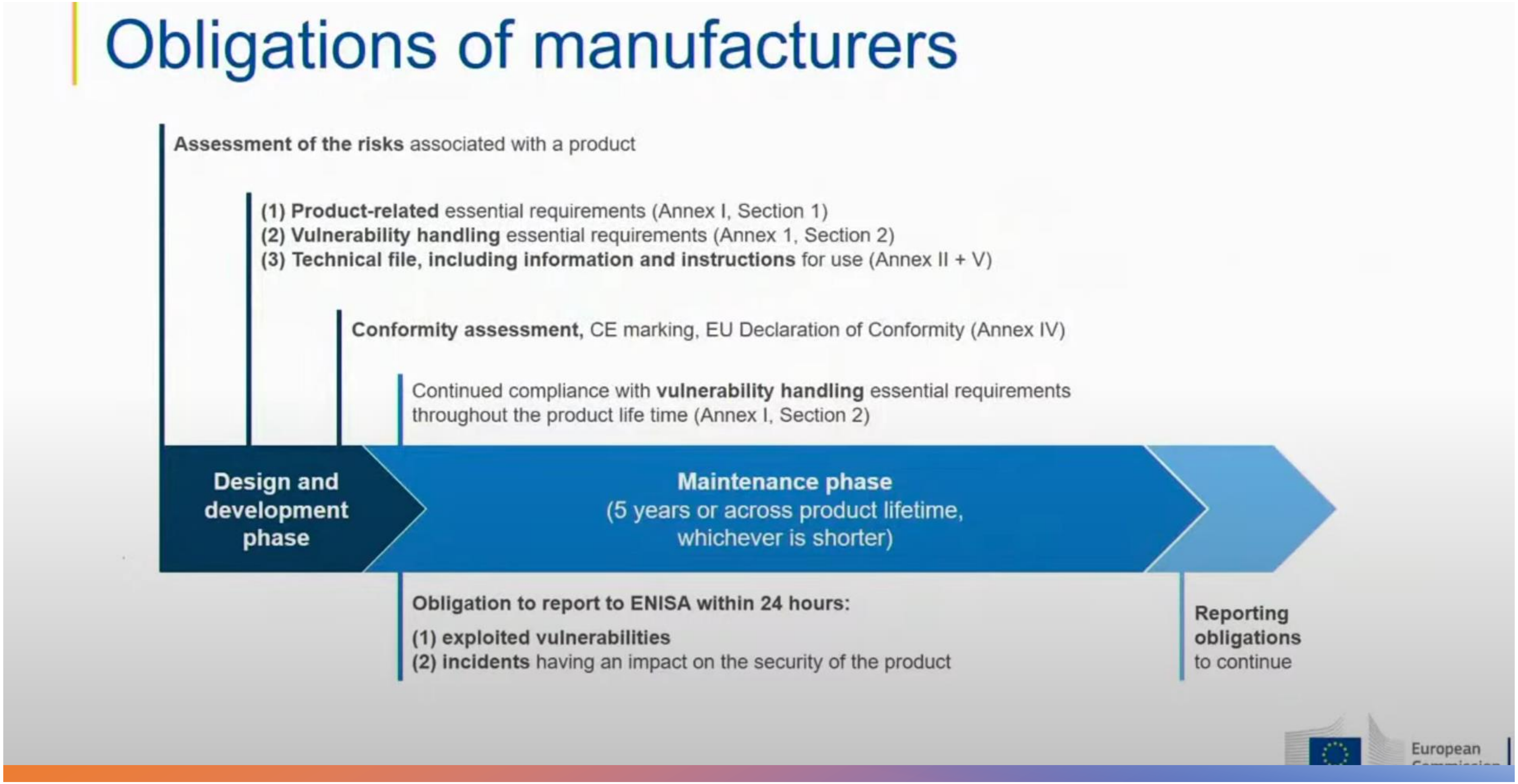
- Impact reduction in case of incident
- Minimise negative effect of incident on other services
- Logging
- SBOM

During operations

vulnerability and incident handling

- Publicly disclose fixed vulnerabilities (coordinated disclosure)
- Security updates: fast, free, automated, through secure distribution channel
- Regular tests and reviews

Sarah Fluchs



Obligations of manufacturers

Assessment of the risks associated with a product

(1) **Product-related** essential requirements (Annex I, Section 1)
(2) **Vulnerability handling** essential requirements (Annex 1, Section 2)
(3) **Technical file, including information and instructions** for use (Annex II + V)

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product life time (Annex I, Section 2)

Design and development phase

Maintenance phase
(5 years or across product lifetime, whichever is shorter)

Obligation to report to ENISA within 24 hours:

(1) **exploited vulnerabilities**
(2) **incidents** having an impact on the security of the product

Reporting obligations to continue

Essential cybersecurity requirements - Security requirements relating to the properties of products with digital elements (Annex I, part 1)

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities;

(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means …

Essential cybersecurity requirements – Vulnerability handling requirements (Annex I, part 2).

Manufacturers of products with digital elements shall:

(1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;

(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

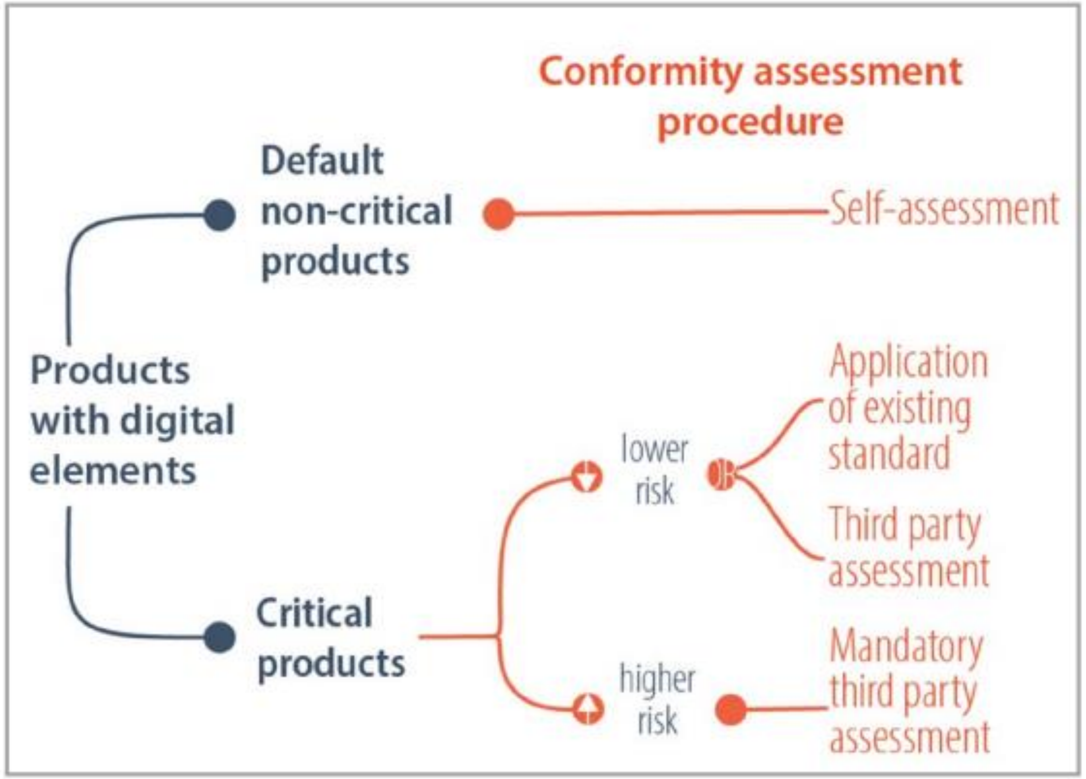
(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner; (8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Conformity with the essential requirements

Figure 1 – Cyber-resilience conformity assessment


Conformity assessment procedure
Products with digital elements
Default non-critical products
Self-assessment
Critical products
lower risk
Application of existing standard
Third party assessment
higher risk
Mandatory third party assessment

Source: European Commission.

Which conformity assessment to follow?

90% of products	10% of products		
Default category	**Critical "Class I"**	**Critical "Class II"**	**Highly critical**
Self-assessment	Application of a standard or third party assessment	Third party assessment	Mandatory EU certification
Criteria: n/a	**Criteria:** • **Functionality** (e.g. critical software) • **Intended use** (e.g. industrial control/NIS2) • **Other criteria** (e.g. extent of impact)		**Additional criteria:** • Used by **NIS2** entities • Resilience of **supply chain**
	To be amended/specified via delegated acts		
Examples: Photo editing, word processing, smart speakers, hard drives, games etc.	**Examples (Annex III):** Password managers, network interfaces, firewalls, microcontrollers etc.	**Examples (Annex III):** Operating systems, industrial firewalls, CPUs, secure elements etc.	**Examples:** **n/a** (empowerment to future-proof the CRA)

Market surveillance powers and sanctions

- Tools for checks at the disposal of market surveillance authorities (MSAs): documentary checks, requests for information, inspections, laboratory checks etc.
- When non-compliance found, MSAs have powers to:
  - require manufactures to bring non compliance to an end and eliminate risk
  - to prohibit/restrict the making available of a product or to order that the product is withdraw/recalled
  - Impose penalties
  - In exceptional circumstances, COM may require ENISA to conduct an evaluation and, based on the results, establish a corrective or restrictive measure is necessary at Union level via an Implementing Act (and following MS consultations)

Costs and benefits

Costs

- Compliance costs up to EUR 29 billion (2 percent of the total market turnover)
- Costs for publica authorities for monitoring and enforcement
- SMEs and public authorities benefit from DEP and Horizon Europe

Benefits

- More transparent and secure products
- Reduction of cybersecurity incidents for business, roughly 180 - 290 billion Euro annually
- Prevention of internal market fragmentation
- Reduction of compliance costs for NIS2 entities
- Enhanced reputation for EU and non EU manufactures
- EU as first mover to shape global standards

VII: Case Study 2

EcoManage Solutions, a company specializing in smart building technologies, is developing a new IoT-based system called "EcoControl" designed to optimize energy usage and environmental conditions in commercial buildings. The EcoControl system integrates various sensors and devices to monitor and control heating, ventilation, air conditioning (HVAC), lighting, and security systems. It collects data on building occupancy, energy consumption, and environmental factors like temperature and air quality to adjust settings in real-time, thereby improving energy efficiency and reducing costs.

Michael, a 45-year-old facility manager, is responsible for overseeing a large corporate office building in Stockholm. He is considering implementing the EcoControl system to better manage the building's operations and meet sustainability goals. Michael appreciates the potential cost savings and environmental benefits of the system, but he is also aware of the legal responsibilities that come with processing the data collected by EcoControl. Does Michael have anything to be concerned about under the GDPR, if so what and how should he respond to the legal requirements?

Meanwhile, EcoManage Solutions, as the manufacturer of the EcoControl system, must ensure that the product complies with the Cyber Resilience Act (CRA). Does EcoManage Solutions have anything to be concerned about under the GDPR, if so what and how should he respond to the legal requirements?

Conclusion

- Modern law and its regulatory potentials are limited to a great deal by its embedment in a written tradition.
- The law should acquire new forms and new regulatory potentials

Thank you!

Liane.colonna@juridicum.su.se