



Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

Cyber Security Law and Policy – week four

NIS (III): the security dimension of privacy and data protection, personal data breaches and ‘by design’ approaches

Dr Maria Grazia Porcedda

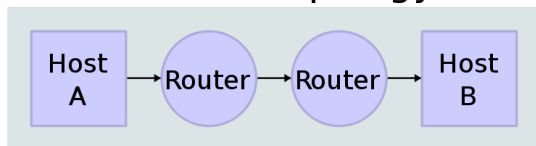
Assistant Professor in IT Law

2021/2022

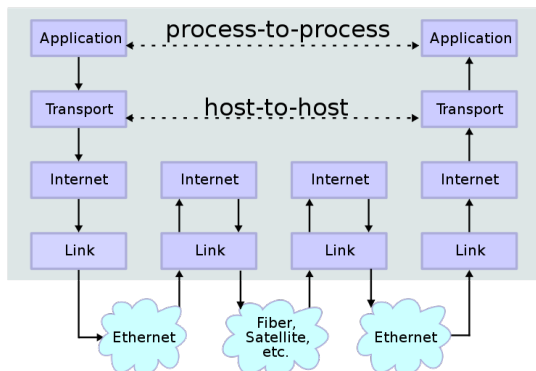
Surely the law will have the answers

Which law?

Network Topology



Data Flow



Source: en:User:Kbrose CC BY-SA 3.0

Content → many «IT» laws

- **Data protection & privacy**, data retention
- copyright law
- e-commerce law (ECD)

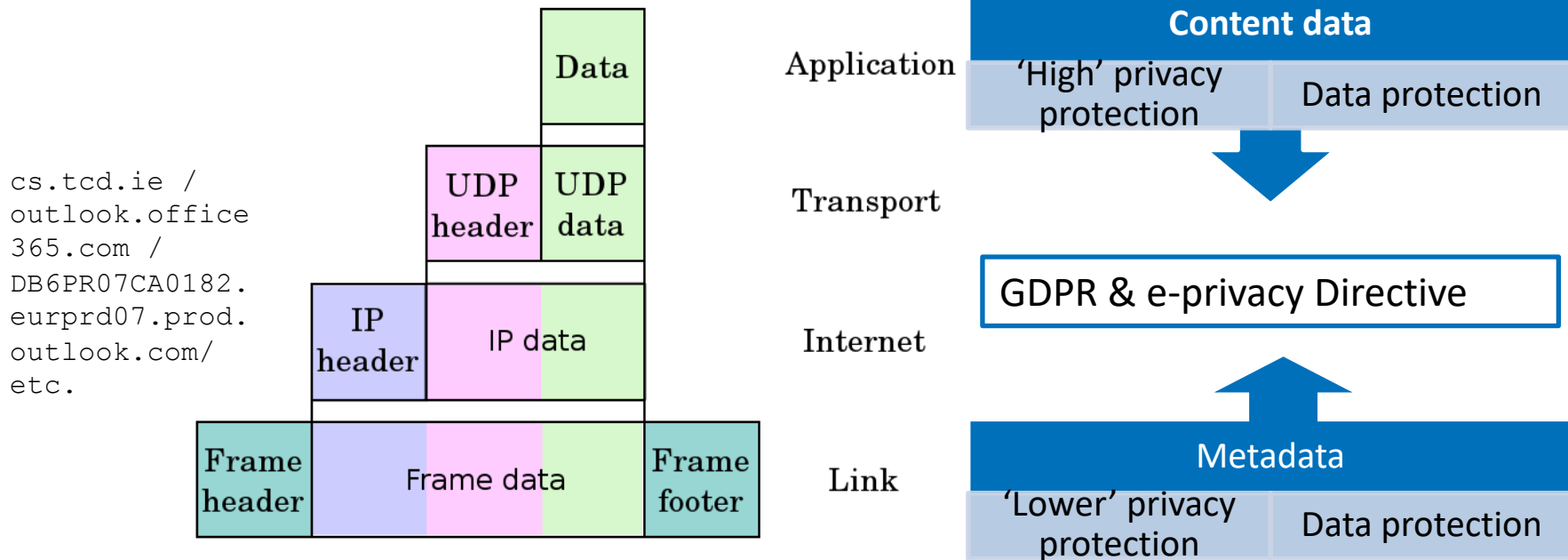
Infrastructure → Telecom Law

Public networks: EECC, but also NIS on DNS, IXPs)

Private networks: e.g. NIS Directive)

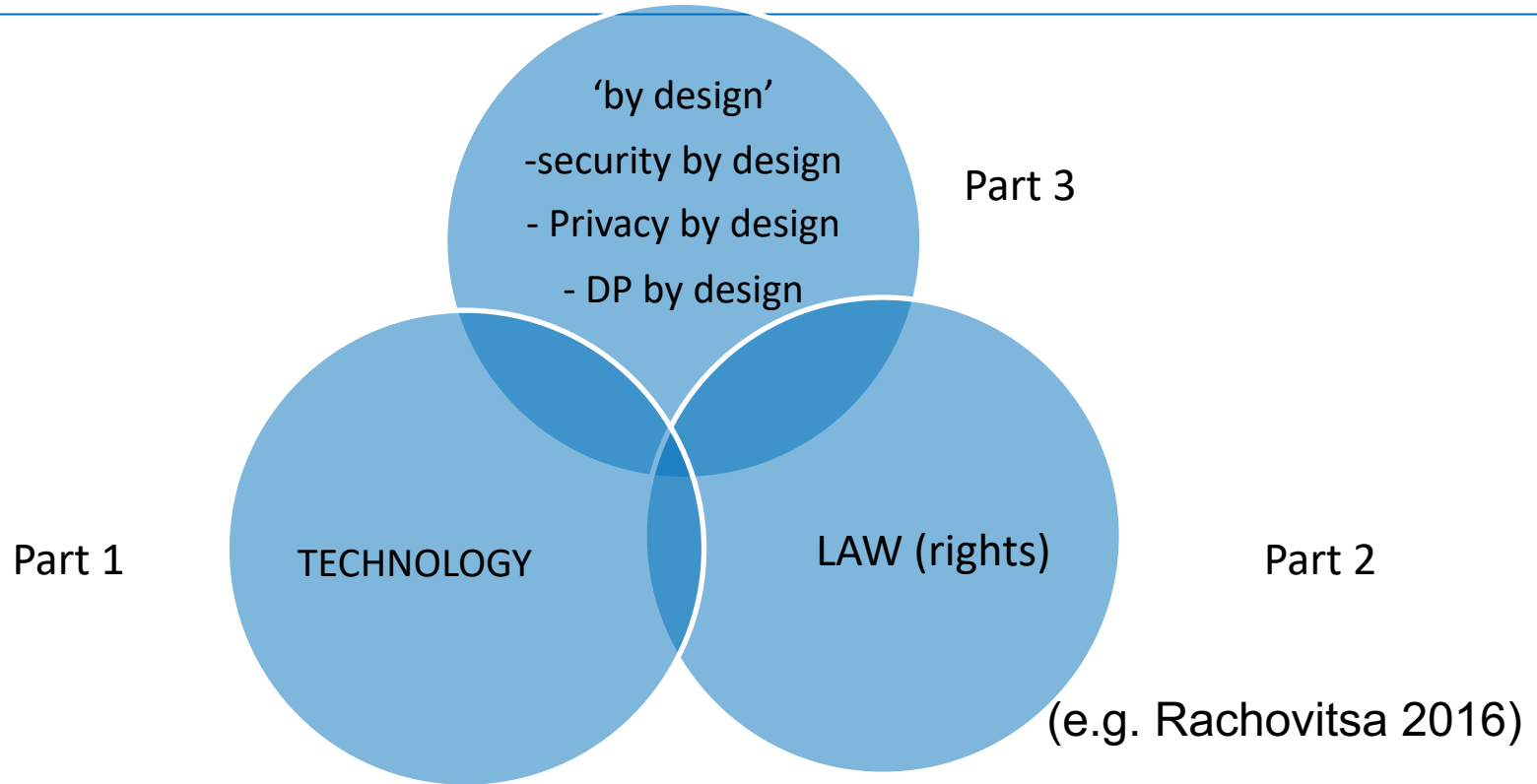
Stephen's email journey: 'correspondence' and 'data'

Many instruments

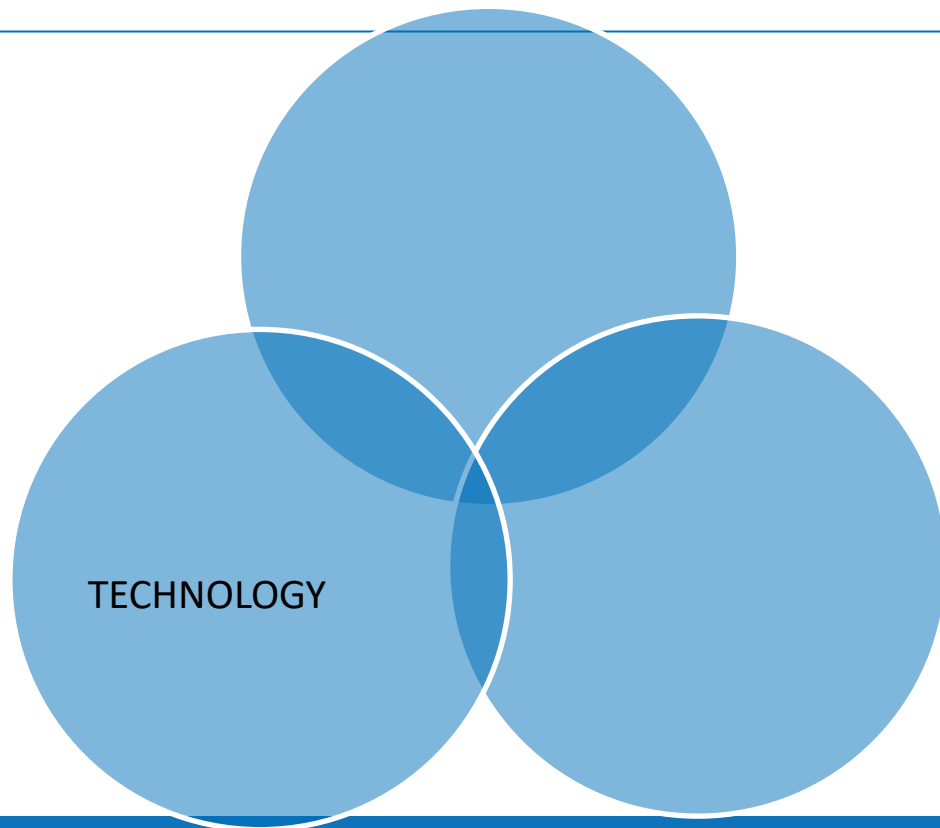


Author: en:User:Cburnett; Source: https://en.wikipedia.org/wiki/File:UDP_encapsulation.svg

Contents: interplay of tech, privacy & DP



Part 1



IETF definition of privacy - IETF RFC 4949

<https://tools.ietf.org/html/rfc4949>

1. «right of

- entity ... to determine degree to which it will interact with its environment, including ...willing[ness] to share its personal information with others [FP041]
- 2. " individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed." [I7498-2]

TUTORIAL → ...expected to address **only communication privacy**, defined primarily by "data confidentiality" and secondarily by "data integrity".

data confidentiality=
property that

1. **data not disclosed to system entities unless ...authorized to know the data.**
2. **information not made available or disclosed to unauthorized individuals, entities, or processes [I7498-2].**

CIA triad + others (NIS II) [check ITU 2021]

		ISO 27000 (freely available)	ITU-T Security in Telecommunications and Information Technology (2015, 6 th edition), Annex A
C	confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities, or <i>processes</i> (3.54)	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ITU-T X.800]
I	integrity	property of accuracy and completeness	The property that data has not been altered in an unauthorized manner.(See also data integrity [ITU-T H.235] <ul style="list-style-type: none"> • The property that data has not been altered or destroyed in an unauthorized manner [ITU-T X.800]
A	availability	property of being accessible and usable on demand by an authorized entity	The property of being accessible and useable upon demand by an authorized entity [ITU-T X.800]
	authentication	property that an entity is what it claims to be	The process of corroborating an identity (→ provision of assurance of the claimed identity) [ITU-T X.800, X.811]
	Non-repudiation	ability to prove the occurrence of a claimed <i>event</i> (3.21) or action and its originating entities	The ability to prevent a sender from denying later that he or she sent a message or performed an action [ITU-T J.170] but also H.235 and J.93]
	(reliability)	property of consistent intended behaviour and results	/

IETF on privacy

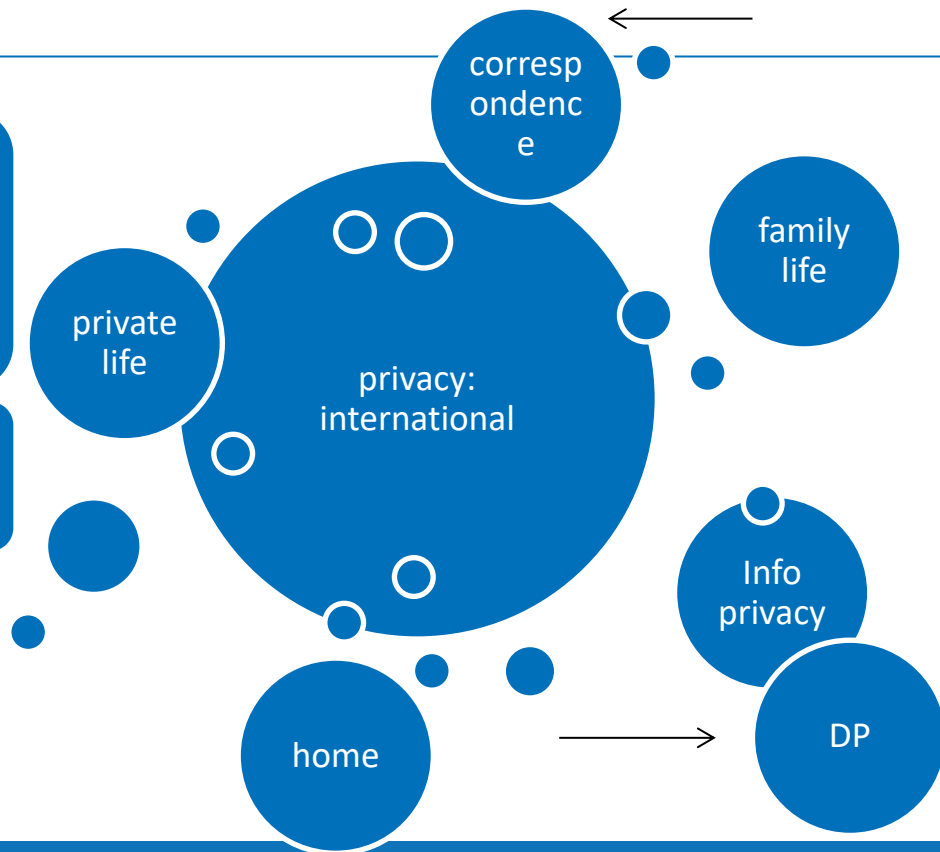
<https://tools.ietf.org/html/rfc4949>

Tutorial: "privacy" used for ...separate but related concepts, e.g. bodily privacy, territorial privacy, personal information privacy, & communication privacy...

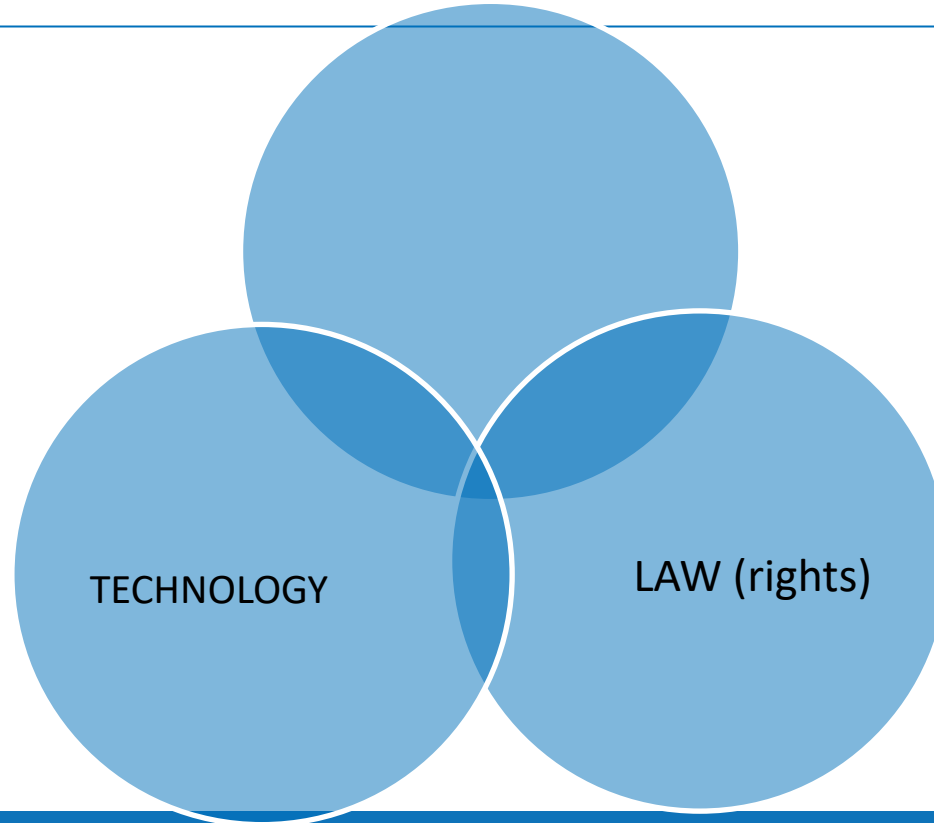
... not addressed in RFC 4949:

- **information privacy... often confused with communication privacy**
- **bodily privacy or territorial privacy [undefined because they are not easily confused with communication privacy.]**

LAW



Part 2



Applicable law

- Rights to privacy & DP
- EPD
 - Confidentiality
 - Spam
 - Data breaches
- GDPR
 - Data breaches
 - Rules on security
 - DPbD

Let's start with the right to respect for private life (privacy)

Art. 12 UDHR (1948)

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

1950. European Convention on Human Rights (ECHR)

1. Everyone has the right to *respect* for his private and family life, his home and his **correspondence**.

1966. International Covenant on Civil and Political Rights (ICCPR)

1. No one shall be subjected to *arbitrary or unlawful interference* with his privacy, family, home or **correspondence**, [nor unlawful attacks on honour & reputation].

NEAT?

rules not enough

Need interpretation

- Usually courts

Interpretation

- specific to jurisdiction
- systematic & purposive

Let's start with the right to respect for private life (privacy): UN

Art. 12 UDHR (1948)

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.



1966. International Covenant on Civil and Political Rights (ICCPR)

1. No one shall be subjected to *arbitrary or unlawful interference* with his privacy, family, home or **correspondence**, [nor unlawful attacks on honour & reputation].

E.g. Art. 17 ICCPR: Human Rights Committee General Comment 16 (4/8/88) on confidentiality

§8 «Compliance with article 17 requires that the *integrity* and *confidentiality* of correspondence should be guaranteed **de jure** and **de facto**. Correspondence should be delivered to the addressee **without interception** and without being opened or otherwise read. **Surveillance**, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations **should be prohibited**»

General comments: <https://www.ohchr.org/EN/HRBodies/Pages/TBGeneralComments.aspx>



<https://juris.ohchr.org/search/documents>

In the EU → thus Ireland



1950. European Convention on Human Rights (ECHR)



1. Everyone has the right to *respect* for his private and family life, his home and his **correspondence**.



EU Charter of Fundamental Rights*



Article 8. 1. Everyone has the right to the protection of personal data concerning him or her.



Article 7. 1. Everyone has the right to *respect* for his or her private and family life, his home and communications.

E-privacy Directive and GDPR

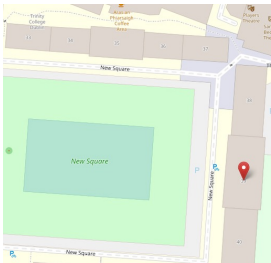
*binding primary law since Lisbon Treaty (2009); applicable when implementing Union law (Art. 51)

Back to Stephen's email : how is it protected?

If public network/providers: e-privacy Directive

What you
said

Called +353 1
896 1000
at 4 PM for
5'20''



Communication (article 2)

- any information exchanged or conveyed between a finite number of parties
- N.B.: Personal data + other information

Stephen's email
content

Traffic data (article 2)

- conveyance of a communication on an e-communications network or for billing (Rec 15)

cs.tcd.ie /
outlook.office365
.com /
DB6PR07CA0182.eur
prd07.prod.outloo
k.com/ etc.

Location data (article 2)

- geographic position of terminal equipment of user (Rec 14)

Stephen's laptop
location

When data are personal, GDPR applies

Communications, location and traffic data not automatically personal

→ Any information

→ relating to an **identified** or **identifiable**

→ natural person ('data subject');

— → Rec 27 no deceased person | Rec 14 whatever the persons' nationality or residence

Identifiable = can be identified, **directly or indirectly**, in particular **by reference to an identifier** such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity (art 4 GDPR)

Back to Stephen's email: two means of protection

Secure services/networks & principle of confidentiality

Security of processing: art 4 EPD

1. The **provider** of a publicly available electronic communications service must take appropriate **technical and organisational measures** to safeguard **security** of its services, if necessary in conjunction with the provider of the public communications network **with respect to network security**. Having regard to the **state of the art** and the **cost** of their implementation, these measures shall ensure a **level of security appropriate to the risk presented**.

Principle of confidentiality : art 5 EPD

- confidentiality of communications and related traffic data...through national law.
- **Prohibit** [all] kinds of **interception or surveillance of communications** and related traffic data ... **without the consent of the users concerned**

What do security and confidentiality mean?

No firm commitment

National case

«general right of personality (art 2.1 + art 1.1 of the Basic Law) in its particular manifestation as a fundamental right to the guarantee of the confidentiality and integrity of information technology systems.» (§ 166)

**Federal Constitutional Court,
BVerfGE 120, 274 (2008)**

CoE (ECtHR) case

confidentiality of communications by any means: emails, Internet use, data stored on computer servers, hard drives

Confidentiality = secret or private; means of protection have not been reviewed

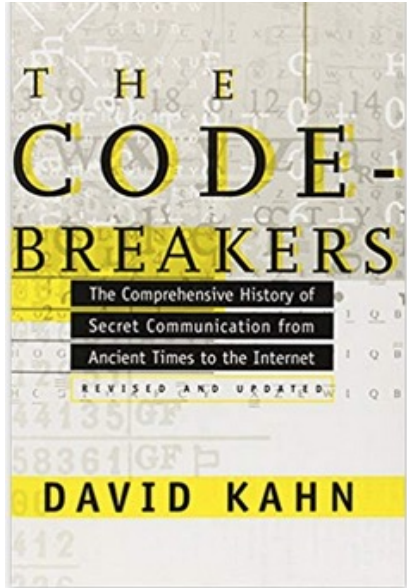
EU (CJEU)

Essence: [the acquisition of knowledge of] **the content of the electronic communications as such** (§ 39)

Digital Rights Ireland (In Joined Cases C-293/12 and C-594/12)

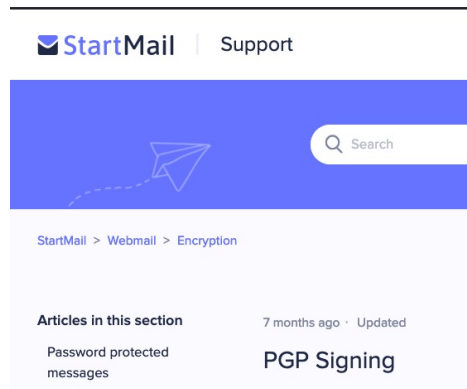
Example of a technical measure: encryption

Older than computers!



David Kahn, 'Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes and Their Effects' (1980) 23 *The Historical Journal* 617

Pretty Good Privacy (PGP)



Delegated legislation implementing EPD

measures capable to render unintelligible personal data, such as ““encryption with standardized key (letter a), or replacement of data by its hashed value calculated with a standardised cryptographic keyed hash function (letter b)”

(Commission Regulation 611/2013/EU, whose Art. 4)

Stephen's data **SHOULD** be confidential, but...(1/2)

Exceptions in article 5(2) and 15

Exception: «when legally authorised to do so in accordance with Article 15(1)»

Article 15: MSs may adopt **legislative measures to restrict the scope of the rights and obligations** ... when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard

- national security (i.e. State security)
- defence
- public security, and
- the prevention, investigation, detection and prosecution of criminal offences or **of unauthorised use of the electronic communication system (cybercrime)**

Member States may...adopt legislative measures [on] the **retention of data** for a limited period ... → Data Retention Directive

Stephen's data **SHOULD** be confidential, but... €€€ (2/2)

Exceptions in article 5

Exception: «authorised recording of communications ...in the course of lawful business practice for ... providing evidence of a commercial transaction» [Recital 21 & 23]

Conditional on informed consent, as understood in GDPR (EDPB 5/2020)

Recital 24: «Terminal equipment ...part of the private sphere of the users So-called spyware, web bugs, hidden identifiers ...can enter the user's terminal without their knowledge in order to gain access o information...and **may seriously intrude upon the privacy of these users.** **The use ...should be allowed only** for legitimate purposes, **with the knowledge of the users concerned..»**



Source:

<https://en.wikipedia.org/wiki/File:Cisforcookie.jpg>

And licensing therein

Cookies: «storing of information, or the gaining of access to information already stored, in the **terminal equipment of a subscriber or user» (Rec 25 extols virtues of cookies)**

Confidentiality & security post-Snowden

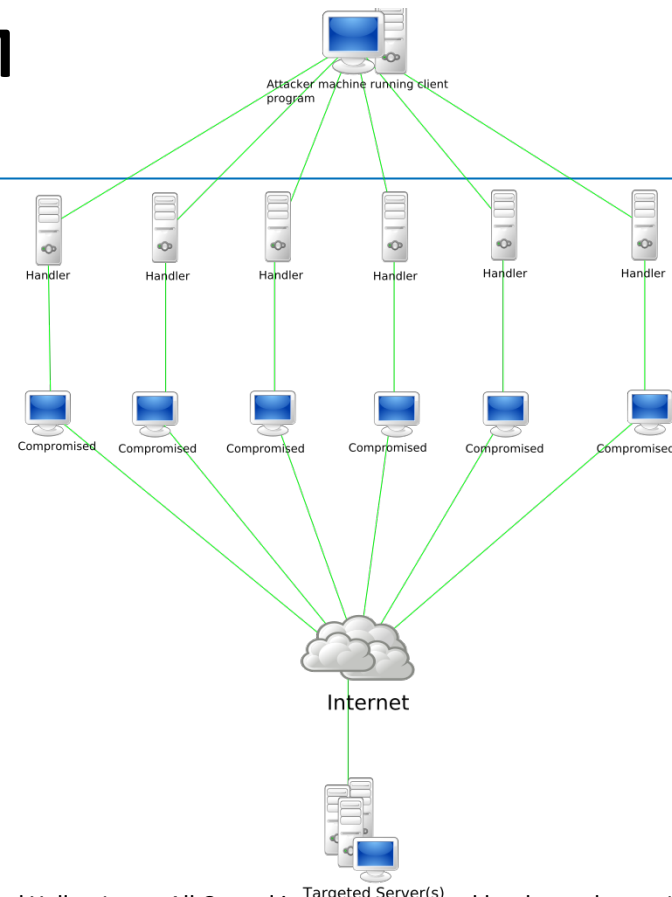


- **2013: Edward Snowden & consortium of newspapers revealed mass surveillance**
 - PRISM & Tempora
- **European Parliament:**
 - “call to promote the wide use of encryption...resist any attempts to weaken Internet safety standards, not only in the interest of privacy, but also in the interest of threats against national security posed by rogue States, terrorists, cyberterrorists and ordinary criminals.”
- **CoE court case of Big Brother Watch and others v UK (2018)**
 - “Acquiring [metadata] may not be less intrusive than acquiring content. In bulk, the degree of intrusion is magnified” (§356)
- **New legislation: e-privacy Regulation**

Stephen's unsolicited email: SPAM

Article 13, recitals 40 & 45

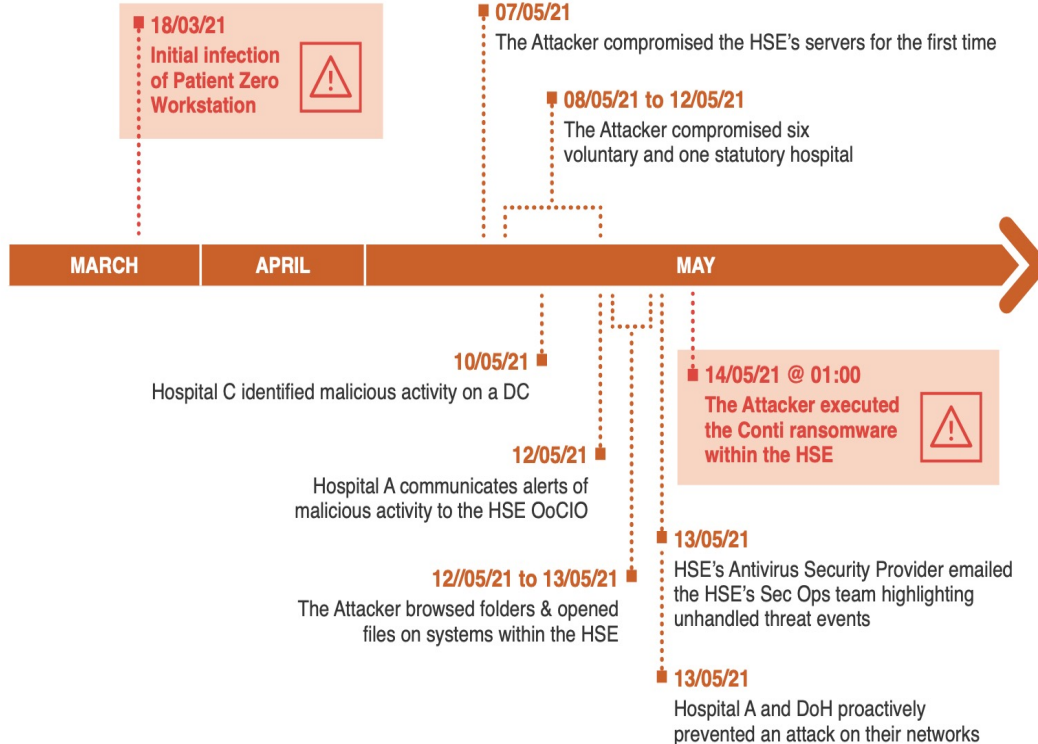
- «automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing»
- allowed only in respect of subscribers or users who have given their prior consent (BUT exceptions)
- Paragraph 4: concealed identity prohibited
- Most spam → botnets [weeks 6-8]
- **Spam and emails as vector of malware**



By Everaldo Coelho and YellowIcon - All Crystal icons were posted by the author as LGPL on kde-look, LGPL, <https://commons.wikimedia.org/w/index.php?curid=3980651>

Spam and emails as vector of malware

E.g. HSE attack: vector was email with compromised excel file



«HSE operating on frail IT estate that has lacked the investment over many years ... It does not possess the required cybersecurity capabilities to protect the operation of the health services and the data they process, from the cyber attacks that all organisations face today.» (PwC 2021, p. 10)

Data Breaches

Added in 2009, following Californian Law

Art. 2(i) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.

Art. 4 (3) Notification obligations to

Data protection
authority

Data subjects

'--have i been pwned?

Check if you have an account that has been compromised in a data breach

Source: <https://haveibeenpwned.com/>



Computer Law & Security Review

Volume 34, Issue 5, October 2018, Pages 1077-1098



Patching the patchwork: appraising the EU regulatory framework on cyber security breaches

Maria Grazia Porcedda

Show more

+ Add to Mendeley Share Cite

<https://doi.org/10.1016/j.clsr.2018.04.009>

[Get rights and content](#)

Abstract

Breaches of security, a.k.a. security and data breaches, are on the rise, one of the reasons being the well-known lack of incentives to secure services and their underlying technologies, such as cloud computing. In this article, I question

What facilitates data breaches?

(I) Big data

(II) Data hoarding

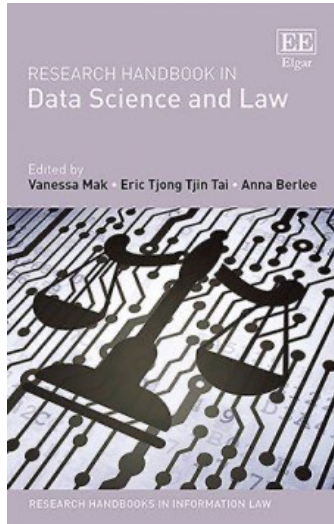
(III) Cloud computing

(IV) Market value of data

Dis-incentives not working

- **Private law liability**
- **Tortious liability**
- **Criminal liability / offences without custodial sentence**
 - Custodial sentences
- **Individual action/ Class actions/ ex officio action**
- **Data protection law**

(I) + (II) + (III)



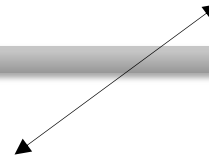
M.G. Porcedda and D. S. Wall,
Data Science, Data crime and the Law (SSRN)

'DATA CRIME' (Porcedda and Wall 2018)



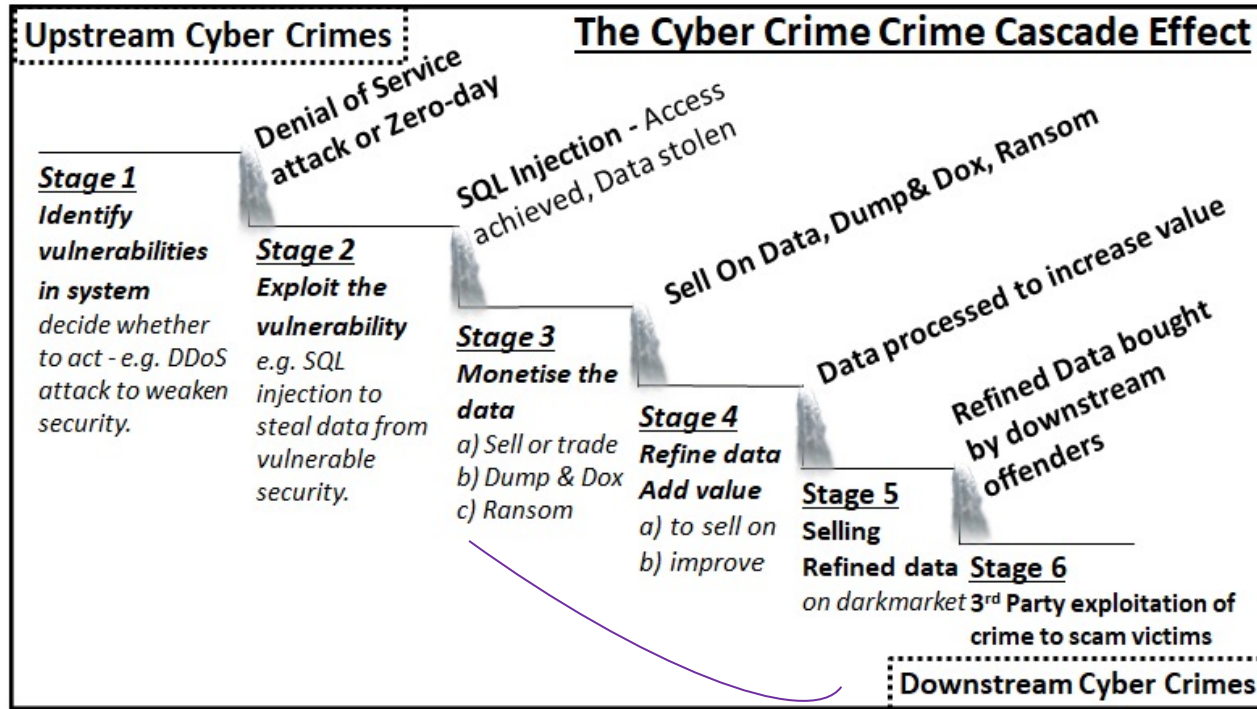
Cybercrime;
Data breaches
(hacking + exfiltration)

Internet usage;
Innovation; datafication



'CYBER LIFT' (Wall 2007, 2017, 2018)

Chain and cascade effects of data crime



Porcedda, M.G. and Wall, D. S., the cybercrime cascade effect (IEEE Europe S&P 2020 and 2021)

GDPR to the rescue: articles 2, 33 and 34

Art. 2 (12) ‘personal data breach’ means a **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Obligations:

- **Art. 33:** Notification of a personal data breach to the supervisory authority
- **Art 34:** Communication of a personal data breach to the data subject
- **Sanctions:** administrative fines up to 10 000 000 EUR/2 % of total worldwide annual turnover

ARTICLE 29 DATA PROTECTION WORKING PARTY



18/EN

WP250rev.01

Guidelines on Personal data breach notification under Regulation 2016/679

Adopted on 3 October 2017

As last Revised and Adopted on 6 February 2018

Many more measures in GDPR to implement right

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Embodies **tensions** between two origins

- Data should not be safeguarded, but if you must then adopt protection
- Data are a resource (€€€), adopt protections to enable flow

(González Fuster and Gutwirth 2013)

Protection = fair information principles
or data protection principles

GDPR: 5+ 1 principles (art 5)

Principle of data security: Art. 5 (f)

«processed in a manner that ensures appropriate **security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, **using appropriate technical or organisational measures** (**‘integrity and confidentiality’**).»

- **Fines for disrespect of principles:** administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher

(See Porcedda (2018) CLSR 34 (5))

The 'essence' of the right to data protection

Essence: Art. 52 «Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms» (very substance)

Opinion 1/15 of the Court

Essence: even if PNR data may, in some circumstances, reveal very specific information concerning the private life of a person, the nature of that information is limited to certain aspects of that private life...

BUT data protection: the agreement lays down,**rules intended to ensure**, inter alia, **the security, confidentiality and integrity of that data**, and to protect it against unlawful access and processing. (§150)

Porcedda (2018), *On Boundaries*

SSRN:

How to achieve security in practice? Art. 32 (I)

Applies to controller
/ processor

1. **Taking into account the state of the art**, the **costs** of implementation and the nature, scope, context and purposes of processing as well as the **risk of varying likelihood and severity** for the rights and freedoms of natural persons, the controller and the processor **shall implement appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, including inter alia as appropriate:
- (a) the pseudonymisation and encryption of personal data;
 - (b) the ability to ensure the **ongoing confidentiality, integrity, availability** and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to personal data in a timely manner
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Art. 32 continued (II)

2. In assessing the appropriate level of security account shall be taken in particular of the **risks that are presented** by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. **Adherence to an approved code of conduct** as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 **may be used** as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

More rules on data security:

- Art 25 DP by design and by default
- Art 35 and 36 on IA and prior assessment
- Article 36 on Prior consultation

Rules to demonstrate security:

- **Art 40** on code of conduct
- **Art 42** on certification

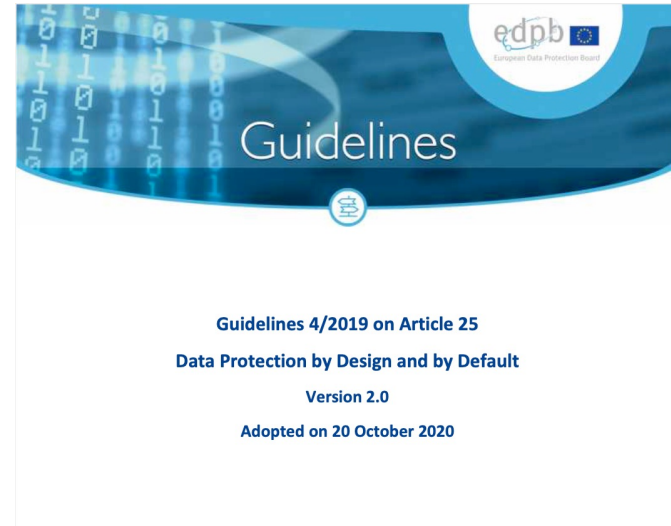
Article 25 – data protection by design and by default

1. **Data protection by design:** implement appropriate technical and organisational measures, such as pseudonymisation, designed

- to implement data protection principles...in an effective manner and
- to integrate the necessary safeguards into the processing
- in order to meet GDPR requirements + protect the rights of data subjects

2. **Data protection by default:** only personal data which are necessary for each specific purpose of the processing are processed → data minimization + purpose specification + storage limitation

3. **An approved certification mechanism (Article 42) may be used as an element to demonstrate compliance with ...paragraphs 1 and 2.**



Tearing the requirements apart

Appropriate technical measures

- «State of the art» → ??? Rec 78

Appropriate organisational measures

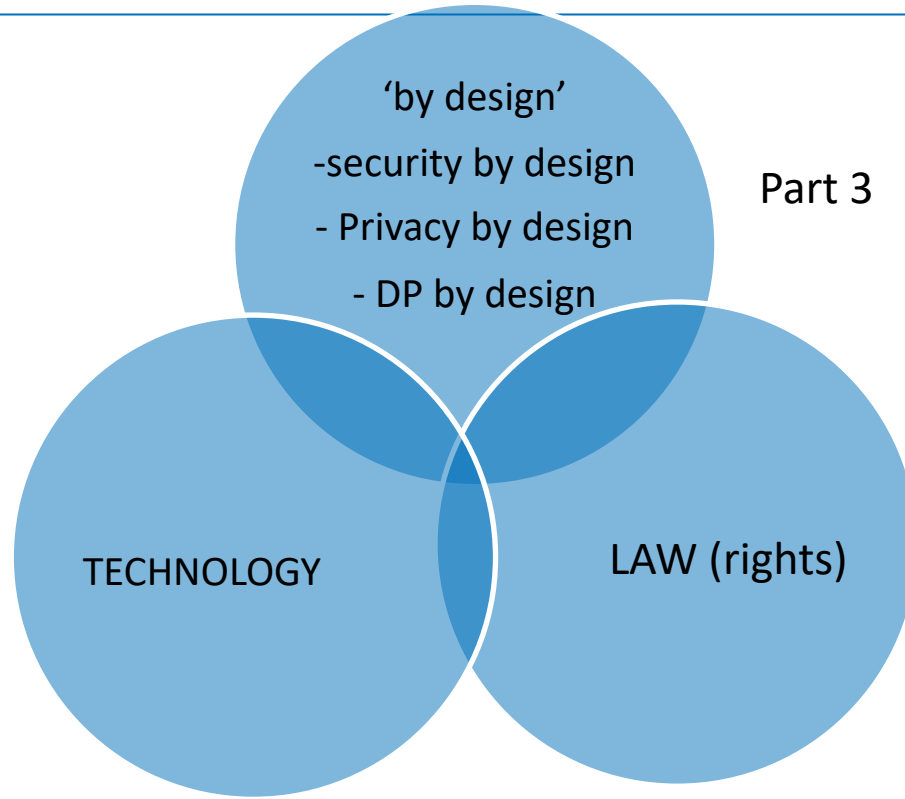
Costs → of implementation

Processing → Nature, scope, context and purposes

Risk of varying likelihood and severity → for rights & freedoms of natural persons

Shall implement → **Who?** the controller and the processor

Part 3: 'by design' as bridge between law & tech



Code as the answer?

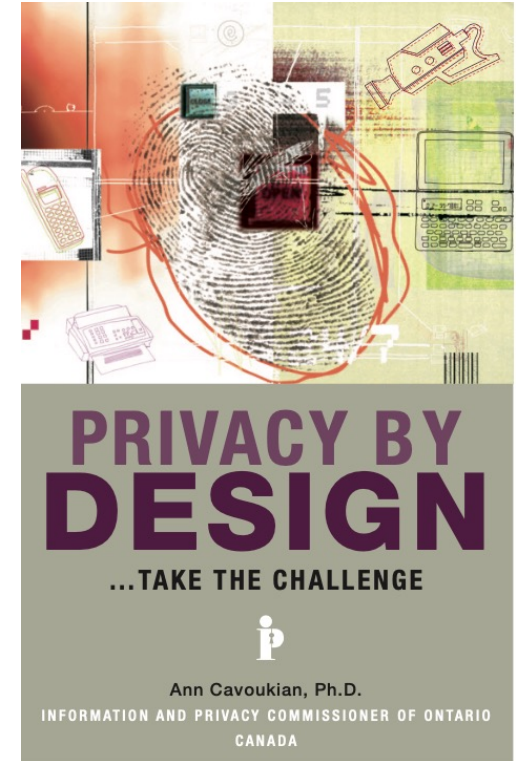
Old IT law debate

- **PETs:** privacy enhancing technologies
 - PGP
 - DoNoTrack, Sticky policies
- **Privacy by Design:** preventative inclusion of privacy considerations
- **Personal Data siloses:** decentralisation of data for control
- **Blockchain**




Foundational principles of privacy by design

1. **Proactive not Reactive; Preventative not Remedial**
2. Privacy as the default design
3. Privacy embedded into the design
4. Full functionality - Positive-Sum, not Zero-Sum
5. **End-to-end security - Full Lifecycle Protection**
6. **Visibility and Transparency — Keep it Open**
7. Respect for User privacy — Keep it User-Centric



By design and by default: but how? Standards!!!

Once adopted they are applicable in EU law



European Committee for Standardization

[CEN COMMUNITY](#) [TECHNICAL BODIES](#) [STANDARDS EVOLUTION AND FORECAST](#) [SEARCH STANDARDS](#)

[Technical Bodies](#) > **CEN/CLC/JTC 13**

CEN/CLC/JTC 13 - Cybersecurity and Data Protection

[General](#) [Structure](#) [Work programme](#) [Published Standards](#)

[EN](#) [FR](#) [DE](#)

CEN/CLC/JTC 13 Scope

Development of standards for cybersecurity and data protection covering all aspects of the evolving information society including but not limited to: - Management systems, frameworks, methodologies - Data protection and privacy - Services and products evaluation standards suitable for security assessment for large companies and small and medium enterprises (SMEs) - Competence requirements for cybersecurity and data protection - Security requirements, services, techniques and guidelines for ICT systems, services, networks and devices, including smart objects and distributed computing devices Included in the scope is the identification and possible adoption of documents already published or under development by ISO/IEC JTC 1 and other SDOs and international bodies such as ISO, IEC, ITU-T, and industrial fora. Where not being developed by other SDO's, the development of cybersecurity and data protection CEN/CENELEC publications for safeguarding information such as organizational frameworks, management systems, techniques, guidelines, and products and services, including those in support of the EU Digital Single Market.

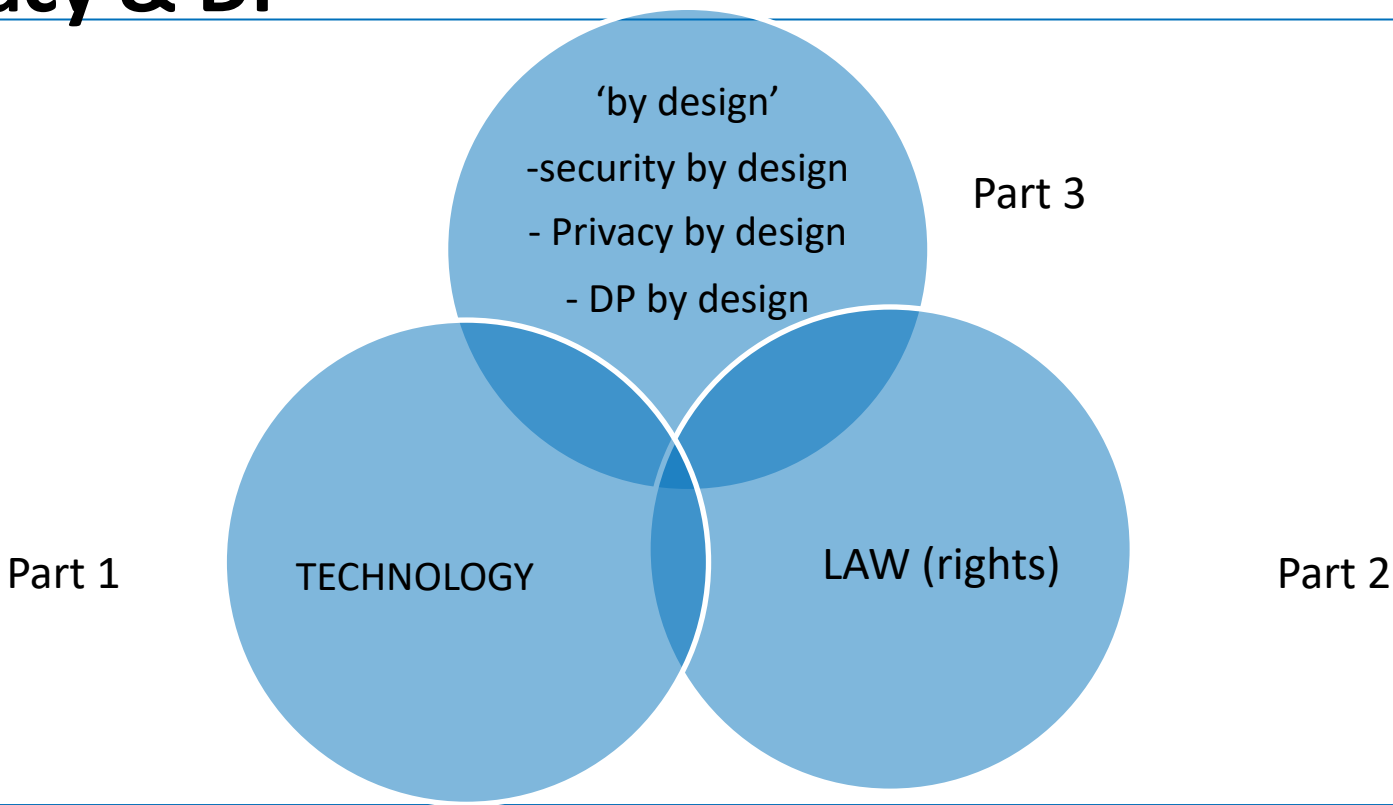
Officers

Chairperson	Mr Walter Fumy
Secretary	Mr Martin Uhlherr

Further information

CEN Technical Secretariat(s)	DIN
CCMC Programme Manager	Kohler Constant
Activity sector	Information Processing Systems

Conclusions: open-ended interplay of tech, privacy & DP





Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

Thank you and see you next Monday

Is there international agreement on confidentiality?

At home, think:

- Does the UN level gives us much indication about a right to confidentiality and integrity?
- What type of regulatory intervention would be needed?

Special Rapporteur on the right to privacy



A Special Rapporteur is an independent expert appointed by the Human Rights Council to examine and report back on a country situation or a specific human rights theme. This position is honorary and the expert is not United Nations staff nor paid for his/her work. The Special Rapporteurs are part of the [Special Procedures](#) of the Human Rights Council.

Introduction

In July 2015, the Human Rights Council appointed Prof. Joseph Cannataci of Malta as the first-ever

Special Rapporteur on the right to privacy. The appointment is for three years.