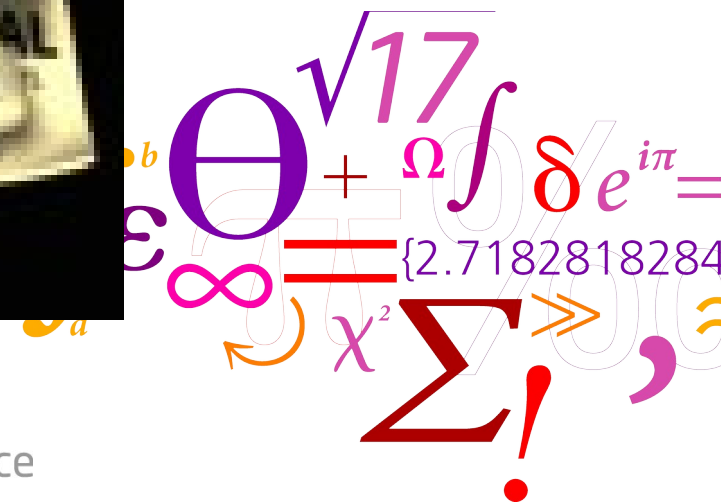


Legal Aspects of Computer Security



Why are Legal Issues Relevant?



What is GDPR, the EU's new data protection law?

—



How to prepare for the NIS2 Directive?

Basic Ideas (why is this relevant)

- Laws and Ethics are important for shaping behaviour
 - Law: Rules adopted and enforced by governments to codify expected behaviour in modern society
 - Ethics: Relatively fixed moral attitudes or customs of a societal group (based on cultural and social norms)
- Defines the rules that govern interactions
 - First the Rule of Law should protect against anarchy and the Hobbesian war of all against all
 - Second, the Rule of Law should allow people to plan their affairs with reasonable confidence that they can know in advance the legal consequences of various actions
 - Third, the Rule of Law should guarantee against at least some types of official arbitrariness

Basic Principles of Law

- The state monopolizes the use of force in the resolution of disputes
 - The use of force must be justified and proportional to the offence
- Individuals are secure in their persons and property
- The state is itself bound by law and does not act arbitrarily
- The law can be readily determined and is stable enough to allow individuals to plan their affairs
- Individuals have meaningful access to an effective and impartial legal system
- The state protects basic human rights and fundamental freedoms
- Individuals rely on the existence of justice institutions and the content of law in the conduct of their daily lives

5 Types of Legal Frameworks

- European Continental Law (Roman Law, Napoleonic Code, ...)
 - Laws are organized into systematic written codes that are recognized as authoritative, court precedents are also considered
- Common Law
 - In the common law system, court judges are bound by the rules and other doctrines developed - and supplemented over time - by the judges of earlier courts
- Customary Law
 - Laws in customary legal systems are seldom written down, they embody an organized set of rules regulating social relations, and they are agreed upon by members of the community
- Religious Law
 - A legal system which stems from the sacred texts or religious traditions
- Mixed Law
 - Law consists of elements of some or all of the other main types of legal systems
 - civil, common, customary, and religious

Laws and Regulation

- Civil Law
 - Governs relationships between individuals and organizations
- Tort law
 - A subset of civil law that allows individuals to seek redress in the event of personal, physical, or financial injury
- Criminal Law
 - Addresses violations harmful to society
 - Actively enforced and prosecuted by the state
- Regulations
 - A subset of criminal law designed to control or govern conduct

Civil Law

- In a civil law problem, 'victim' must take action to get a legal remedy (adequate compensation)
 - 'victim' must hire a private lawyer & pay expenses of pursuing the matter
 - the police does not get involved, beyond the point of restoring the order
- In Civil Law, to convict someone, the guilt must be proven on *'balance of probabilities'*
- In Civil Law, monetary remedies (damages) are most common

Criminal Law

- In a criminal law problem, 'victim' (may) report the case to the police and they have the responsibility to investigate.
 - if charge has been properly laid and there is supporting evidence, the prosecutor (not person who complains of incident) prosecutes in the courts – public funds finance these services
 - Even if a 'victim' starts a prosecution privately, the Police Attorney has the power to take over the prosecution
 - *Police is obliged to investigate crimes that come to their attention*
- In Criminal Law, to convict someone, the guilt must be proven '*beyond reasonable doubt*'
- In Criminal Law, the sentence to the offender may include one or a combination of the following:
 - imprisonment
 - community service
 - fine
 - probation
 - restitution – compensate for victim's loss or damages

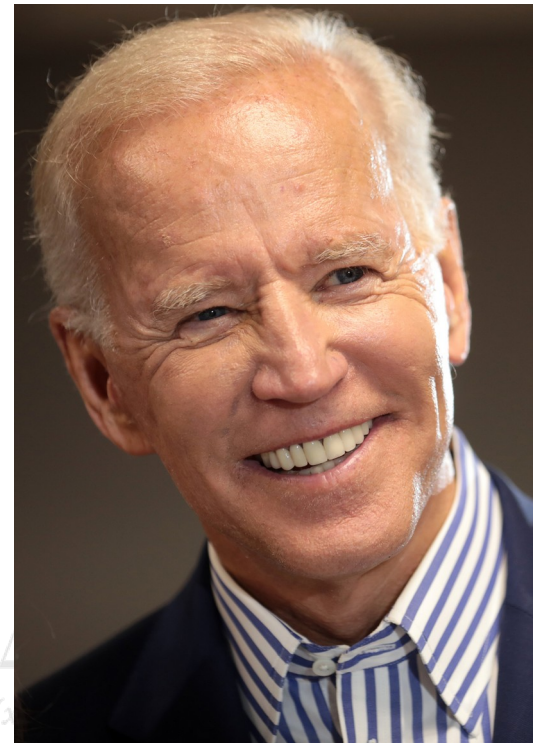
The Role of Computers in Crime

- Computer (or network) as target
 - Using computer(s) to attack a victim's computer
 - Attack on Confidentiality, Integrity or Availability of data or systems
 - Cyber Terrorism and Cyber Warfare
- Computer as tool
 - Fraud - Phishing, Nigerian 419 (after Fraud § in Nigerian Criminal Code)
 - Ransomware (WannaCry, NotPetya, ...)
 - Gambling
 - Copyright infringements (aka piracy)
 - Harassment (aka cyber bullying), stalking, etc.
- Computer as accomplice
 - Personal information (diaries, downloaded e-mails,)
 - *Other evidence unknown to suspect - web-history, cookies, ...*
 - Contraband - digital goods, copyrighted material, (child) pornography
 - Stolen information – trade secrets, credit card data
 - Monetizing proceeds of cyber crime (online marketplaces, Bitcoins, ...)

Cyber Crime

- Problem of jurisdiction
 - Laws are mostly national, cyber crime is typically transnational
 - *International treaties/conventions may codify crime in several countries*
 - *Netiquette may (self-)regulate some unwanted behaviour*
 - Where is crime committed?
 - *Who should investigate, prosecute and sentence*
 - Location of victim, criminal or beneficiary?
 - *The crime may not be a legal offence in all relevant jurisdictions*
 - How to investigate
 - *Collecting evidence requires collaboration among law enforcement agencies*
 - How to get hold of the accused person(s) / evidence?
 - *Extradition agreements between national states*
 - How to punish criminals
 - *Some criminals may be tried in absentia*

Problem of Jurisdiction



Convention on Cyber Crime

- Convention established by the Council of Europe
 - 30 states sign Convention at opening ceremony in Budapest in 2001
- First international treaty on cyber crimes, dealing particularly with:
 - Infringements of copyright
 - Computer-related fraud
 - Child pornography
 - Violations of network security
 - Hate crimes and Racism as an addendum (optional extras)
- Contains a series of powers and procedures such as search of computer networks and interception
- Main objective is to pursue a common criminal policy aimed at protection of society against cyber-crime, especially by adopting appropriate legislation and fostering international co-operation

Protecting Intellectual Property

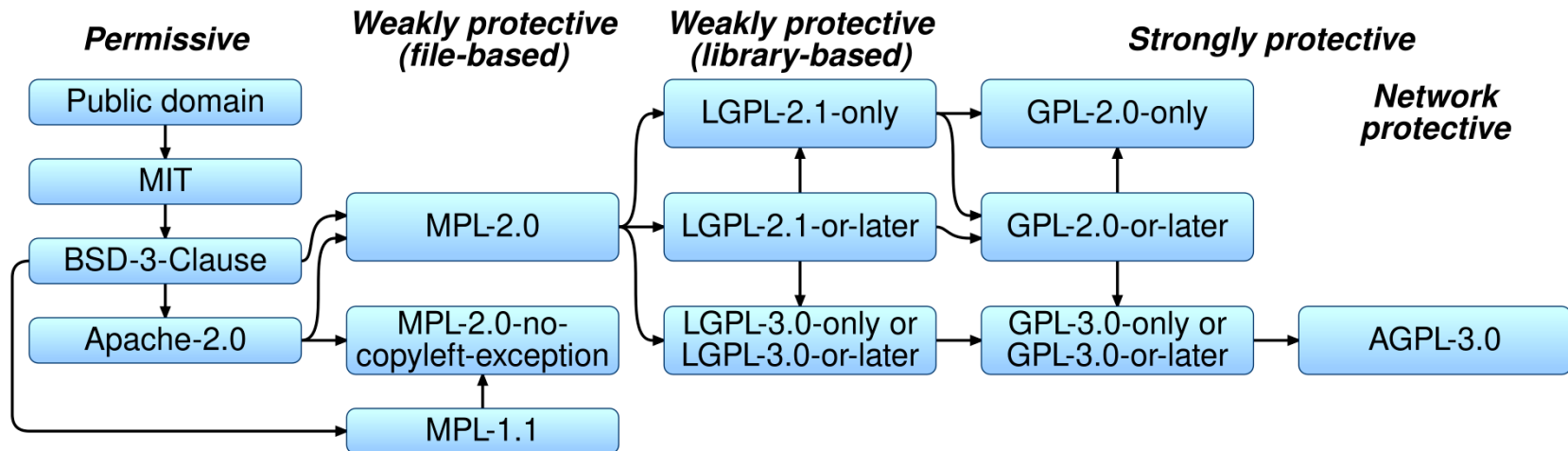
- Three legislative frameworks are applicable to programs and data:
 - Copyright law (publication of works of art)
 - *Copyright law was conceived to protect works of art, music, literature and written scholarship*
 - *Provides incentive to produce works of art*
 - Patent law (public information about inventions)
 - *Patent law was conceived to protect inventions and innovation in science, technology and engineering*
 - *Provides an incentive to inventors to disclose their inventions*
 - Trade secrets law (secret information incl. data and processes)
 - *Trade secrets identify information that must be kept secret*
 - Punish people who reveal the secret to outsiders
 - *Provides a legal framework to deal with disclosure of confidential info.*

Copyrights, Patents & Trade Secrets

	Copyright	Patent	Trade Secret
Protects	Expression of idea, not idea itself	Invention – the way something works	A secret, competitive advantage
Protected objects made public	Yes, intention is to promote publication	Design filed at Patent Office	No
Requirement to distribute	Yes	No	No
Ease of filing	Very easy, do-it-yourself	Very complicated; specialist lawyer suggested	No filing
Duration	Life of human originator plus 70 years, or total of 95 years for a company	19 years	Indefinite
Legal protection	Sue if unauthorized copy sold	Sue if invention copied	Sue if secret improperly obtained

Open-source licenses

AGPL (and often GPL) licenses are not adapted to commercial software.



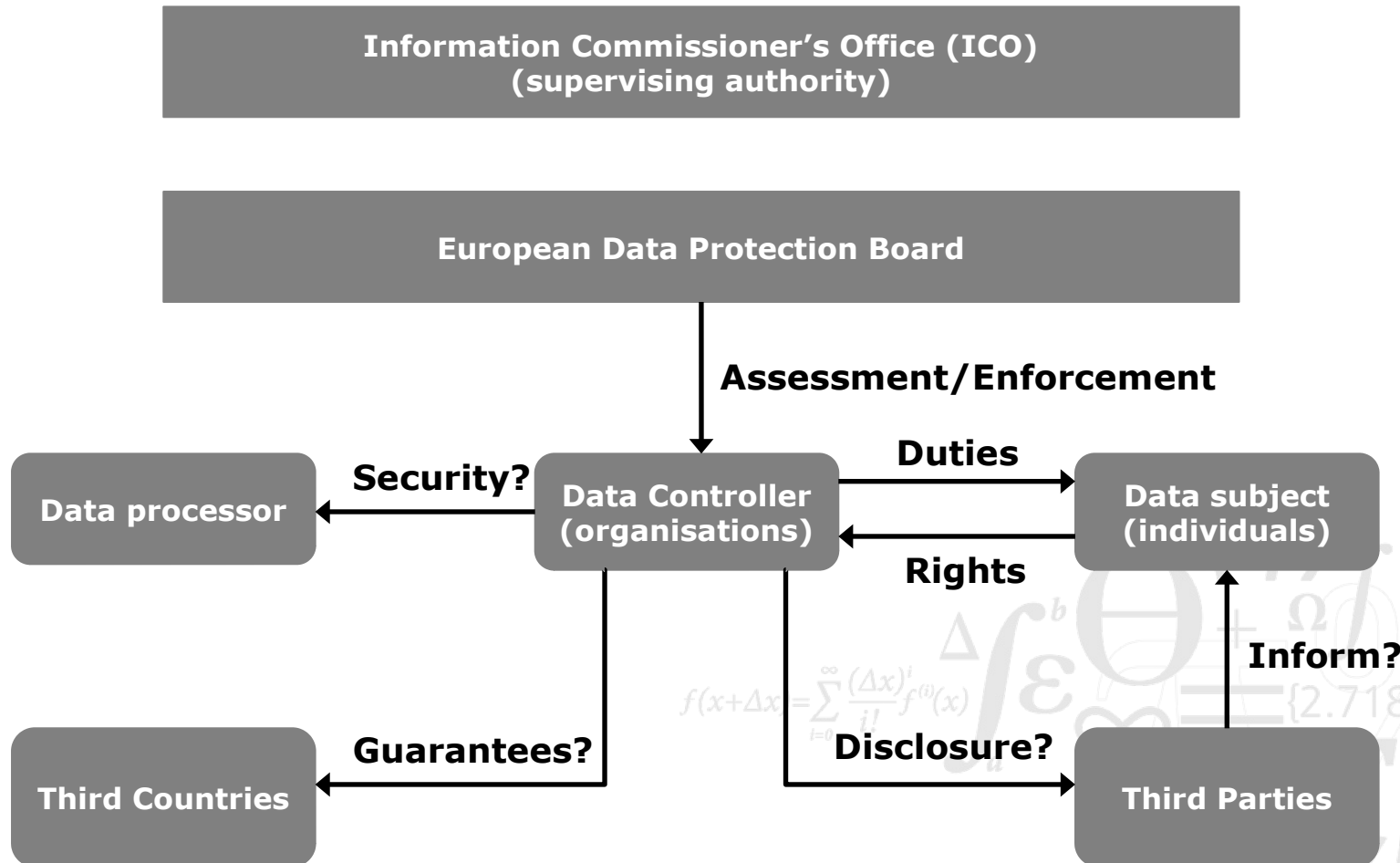


Data Protection

- Large amounts of data are being collected about all of us



GDPR - Data Protection Model



GDPR - Definitions

- Natural person = a living individual
- Natural persons have rights associated with:
 - The protection of personal data
 - The protection of the processing of personal data
 - The unrestricted movement of personal data within the EU
- In material scope:
 - Personal data that is processed wholly or partly by automated means;
 - Personal data that is part of a filing system, or intended to be
- The Regulation applies to controllers and processors in the EU irrespective of where processing takes place
- It applies to controllers not in the EU

GDPR - Remedies, liabilities and penalties

- Natural Persons have rights
 - Judicial remedy where their rights have been infringed as a result of the processing of personal data.
 - *In the courts of the Member State where the controller or processor has an establishment*
 - *In the courts of the Member State where the data subject habitually resides*
 - Any person who has suffered material, or non-material, damage shall have the right to receive compensation from the controller or processor
 - Controller involved in processing shall be liable for damage caused by processing
- Administrative fines
 - Imposition of administrative fines will in each case be effective, proportionate, and dissuasive (*No administrative fines in Denmark, fines imposed by the courts*)
 - *taking into account technical and organisational measures implemented;*
 - €10,000,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year
 - €20,000,000 or, in case of an undertaking, 4% total worldwide annual turnover in the preceding financial year

GDPR - Personal Data Breaches (Article 33)

- The definition of a Personal Data Breach in GDPR:
 - A '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.
- Obligation for data processor to notify data controller
 - Notification without undue delay after becoming aware
 - No exemptions
 - All data breaches have to be reported
- Obligation for data controller to notify the supervisory authority
 - Notification without undue delay and not later than 72 hours
 - Unnecessary in certain circumstances
 - Description of the nature of the breach
 - No requirement to notify if unlikely to result in a high risk to the rights and freedoms of natural persons
 - Failure to report within 72 hours must be explained

GDPR - Rights of Data Subjects

- The controller shall take appropriate measures to provide any information ... relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 11-1)
- The controller shall facilitate the exercise of data subject rights (Article 11-2)
 - Rights to
 - *Consent*
 - *Access*
 - *Rectification*
 - *Erasure*
 - *Objection*
 - the right to data portability;
 - the right to withdraw consent at any time;
 - the right to lodge a complaint with a supervisory authority;
 - The right to be informed of the existence of automated decision-making, including profiling, as well as the anticipated consequences for the data subject

GDPR - the Principle of Accountability

- Governance: Board accountability
 - Corporate risk register
 - Nominated responsible director
- Clear roles and responsibilities
 - Data Protection Officer
- Privacy Compliance Framework
 - PIMS/ISMS
 - Cyber incident response
 - Cyber Essentials is a minimum security standard
 - Certification and data seals (Article 42) –ISO 27001
- Data Protection by Design and by Default
 - Data Flow Audits
 - Data Protection Impact Assessments (DPIA)
 - *Mandatory for many organizations*
 - *Legal requirements around how performed and data collected*

GDPR – Lawfulness (Article 5 & 6)

- Secure against accidental loss, destruction or damage
- Processing must be lawful –which means, inter alia:
 - Data subject must give consent for specific purposes
 - Other specific circumstances where consent is not required
 - *So that controller can comply with legal obligations etc.*
- One month to respond to Subject Access Requests & no charges
- Controllers and processors clearly distinguished
 - Clearly identified obligations
 - Controllers responsible for ensuring processors comply with contractual terms for processing information
 - Processors must operate under a legally binding contract
 - *Note issues around extra-territoriality*

GDPR – Consent (Article 7-9)

- Consent must be clear and affirmative
 - Must be able to demonstrate that consent was given
 - Silence or inactivity does not constitute consent
 - Consent must be clear, intelligible, easily accessible, to be binding
 - Consent can be withdrawn at any time, and it must be as easy to withdraw consent as give it
- Special conditions apply for children (under 16) to give consent
- Explicit consent necessary for processing sensitive personal data
 - Race, ethnic origin, gender, etc.
 - Specific circumstances allow non-consensual processing,
 - *Regulatory or legal requirements*
 - *To protect vital interests of the data subject*
 - ...
- Secure against accidental loss, destruction or damage (article 5)

GDPR – Transparency (Article 12 – 18)

- Any communications with a data subject must be concise, transparent, intelligible
 - This excludes legal jargon
- Controller must be transparent in providing information about itself and the purposes of the processing
- Controller must provide data subject with information about their rights
- Specific provisions (Article 14) covering data not obtained directly from the data subject
- Rights to access, rectification, erasure ('right to be forgotten'), to restriction of processing, and data portability

GDPR - Privacy by Design (Article 25 et seq.)

- Privacy must now be designed into data processing by default
- Data controllers/processors not established in the EU must designate a representative
- Data Privacy Impact Assessments mandatory (article 35)
 - For technologies and processes that are likely to result in a high risk to rights of data subjects
- Data audits
 - GDPR applies to existing data, as well as future data
 - Privacy may have to be designed in retrospectively
 - Organizations need to identify what PII they hold, where, on what grounds, and how it is secured in a way that will meet requirements of GDPR

GDPR - Security of Personal Data (Article 32)

- Sixth Principle: Data must be 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"*
- A requirement for data controllers and data processors to implement a level of security appropriate to the risk, including:
 - pseudonymisation and encryption of personal data;
 - ensure the ongoing confidentiality, integrity and availability of systems;
 - a process for regularly testing, assessing and evaluating the effectiveness of security measures;
 - security measures taken need to comply with the concept of privacy by design;
- Certifications demonstrate intent: Cyber Essentials, ISO 27001

GDPR - Data Protection Officer (DPO)

- DPO mandatory in organizations processing substantial volumes of PII (Article 37)
- A protected position, reporting directly to senior management
 - Appropriately qualified
 - Consulted in respect of all data processing activities
- Will be a 'good practice' appointment outside the mandatory appointments
- Most staff dealing with PII (e.g. HR, marketing, etc.) will need at least basic training
- Staff awareness training also critical (accidental release of PII could have financially damaging consequences)

GDPR - International Transfers (Article 44)

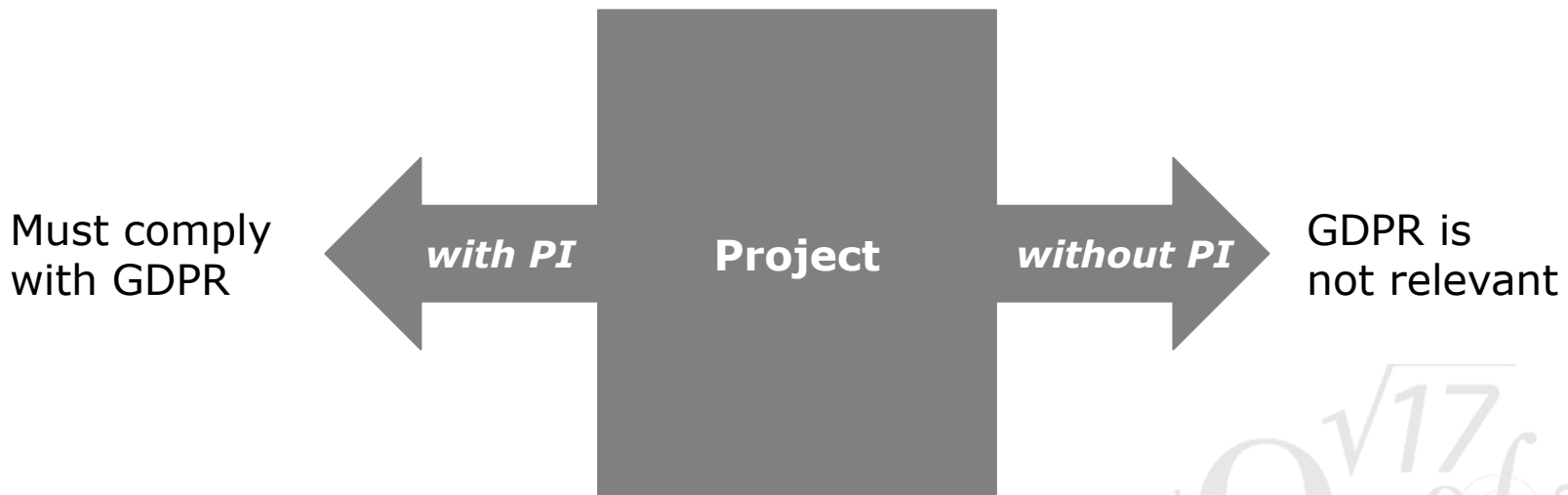
- Any transfer of personal data by controller or processor shall take place only if certain conditions are complied with:
 - Transfers on the basis of adequacy;
 - Transfers subject to the appropriate safeguards
 - Binding corporate rules apply
- All provisions shall be applied to ensure the protection of natural persons is not undermined
- To countries with similar data protection regulations
 - Cloud providers are a key risk area
 - *Schrems II decision in European Court of Justice raises questions about transfer to US and US owned companies*
 - Highest penalties apply to breaches of these provisions

Nine Steps to GDPR compliance

1. Establish governance framework – board awareness, risk register, accountability framework, review
 2. Appoint and train a DPO
 3. Data inventory – identify processors, unlawfully held data
 4. Data flow audit
 5. Compliance gap analysis
 - Ensure FPN and SAR documents and processes are robust and legal
 6. DPIA and security gap analysis
 - Penetration testing, security and privacy code analysis
 7. Remediate
 1. Privacy compliance framework
 2. Cyber Essentials/Ten Steps to Cyber Security/ISO 27001
 8. Data breach response process (NB: Test!)
 9. Monitor, audit and continually improve
- NB: steps can be tackled in parallel

GDPR in Practice

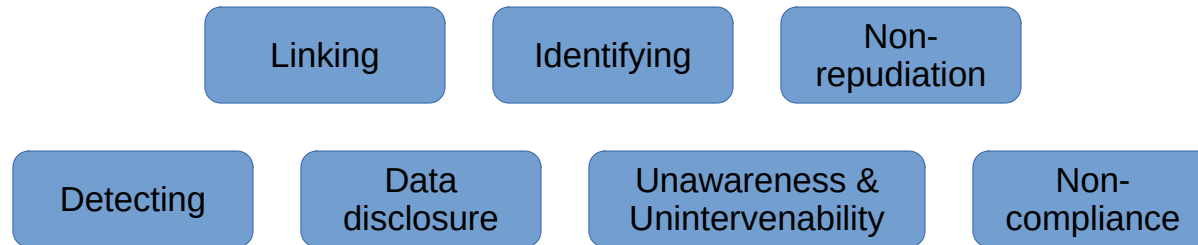
- When considering the data you collect when implanting a project



- GDPR can be ignored *if you do not collect personal data*
 - This is one reason why privacy enhancing technologies are so important

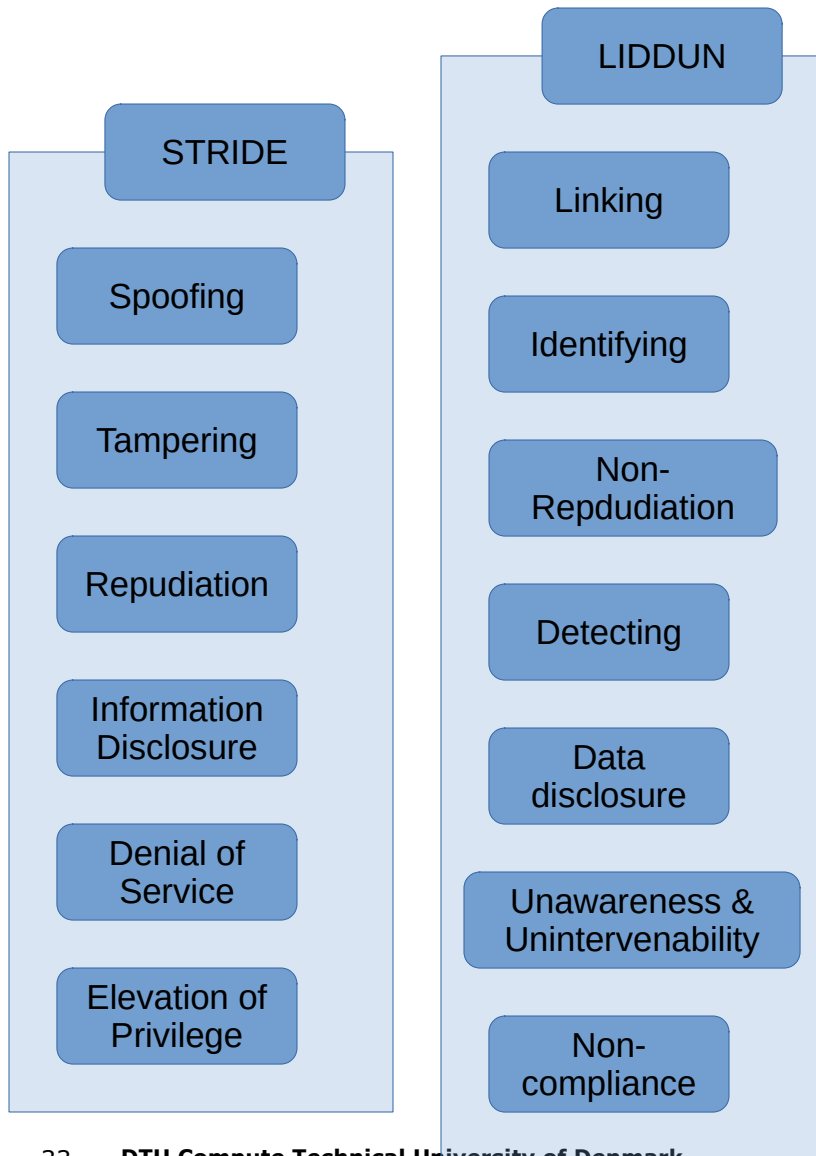
Privacy threat modelling

LIDDUN Threats



- The LIDDUN framework was first introduced by Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel and Wouter Joosen in 2011: <https://linddun.org/publications/>
- **Linking**: associating data items or user actions to learn more about an (unidentified) individual or group
- **Identifying**: learning the identity of an individual, through leaks, deduction, inference
- **Non-repudiation**: being able to attribute a claim to an individual
- **Detecting**: deducing the involvement of an individual by observing (data)
- **Data Disclosure**: excessively collecting, storing, processing or sharing personal data
- **Unawareness & Unintervenability**: insufficiently informing, involving or empowering individuals in the processing of their personal data.
- **Non-compliance**: deviating from security and data management best practices, standards and legislation.

Security vs. Privacy

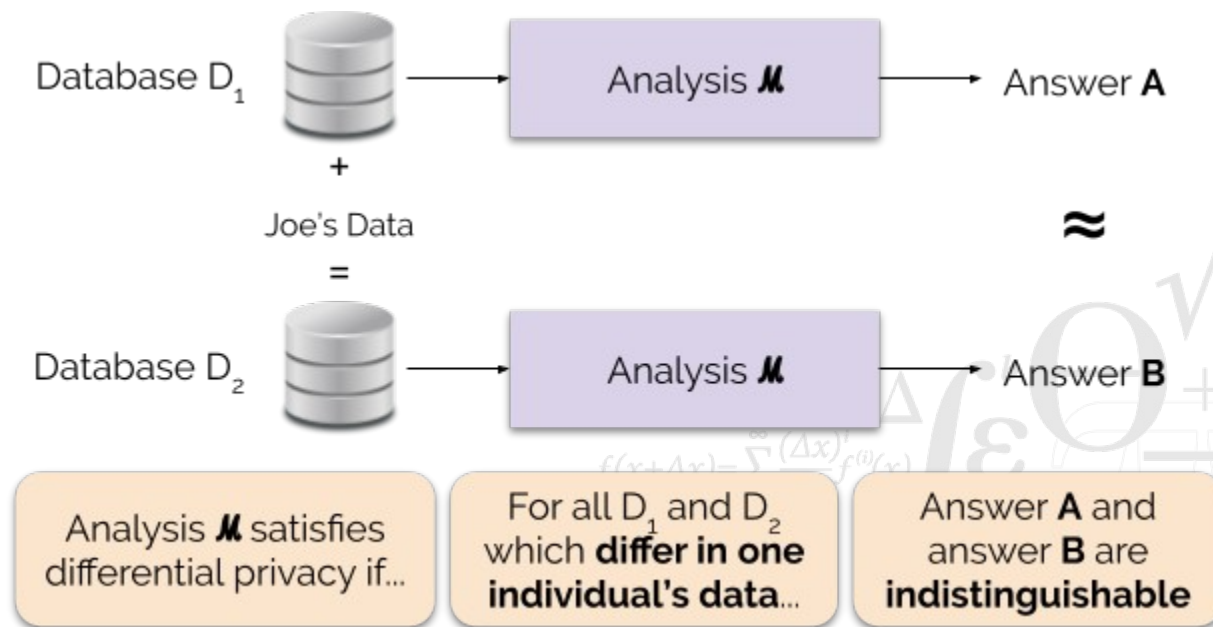


Recommendation: A taste of Privacy
Threat Modelin – Kim Wuyts:

<https://www.youtube.com/watch?v=0H MxksszzDI>

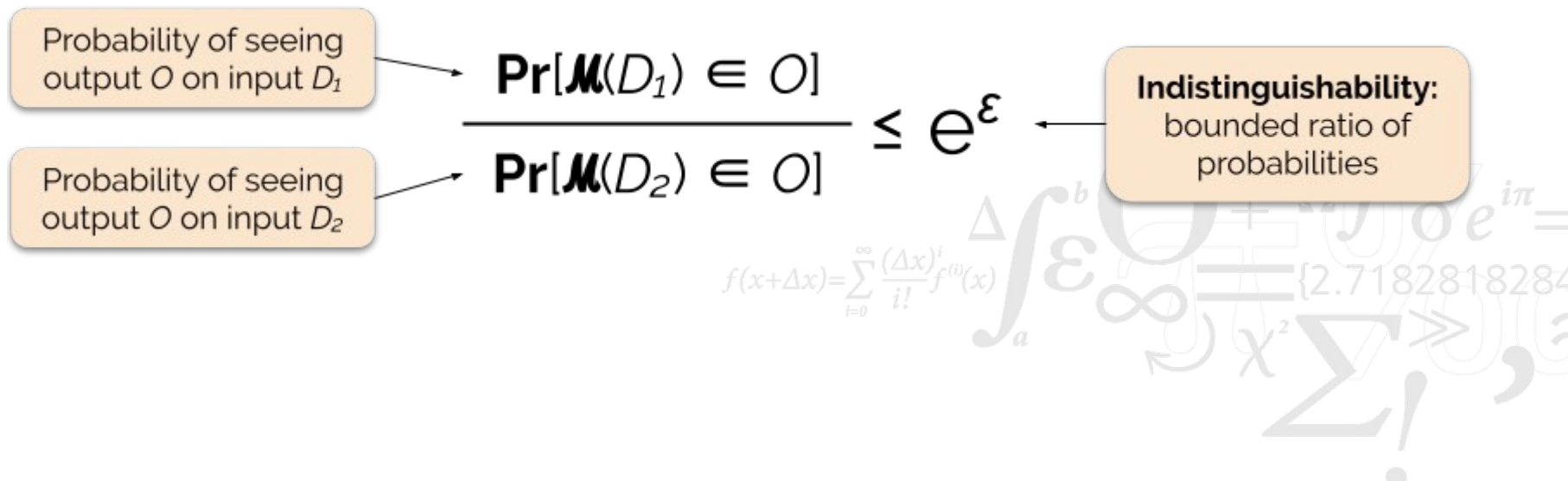
Differential Privacy (DP)

- Differential Privacy ensures that the presence or absence of any individual in a database, or changing the data of any individual, does not significantly affect the probability of obtaining any specific answer for a certain query



Differential Privacy (DP)

- Differential Privacy ensures that the presence or absence of any individual in a database, or changing the data of any individual, does not significantly affect the probability of obtaining any specific answer for a certain query



Probability of seeing output O on input D_1 → $\Pr[\mathcal{M}(D_1) \in O]$

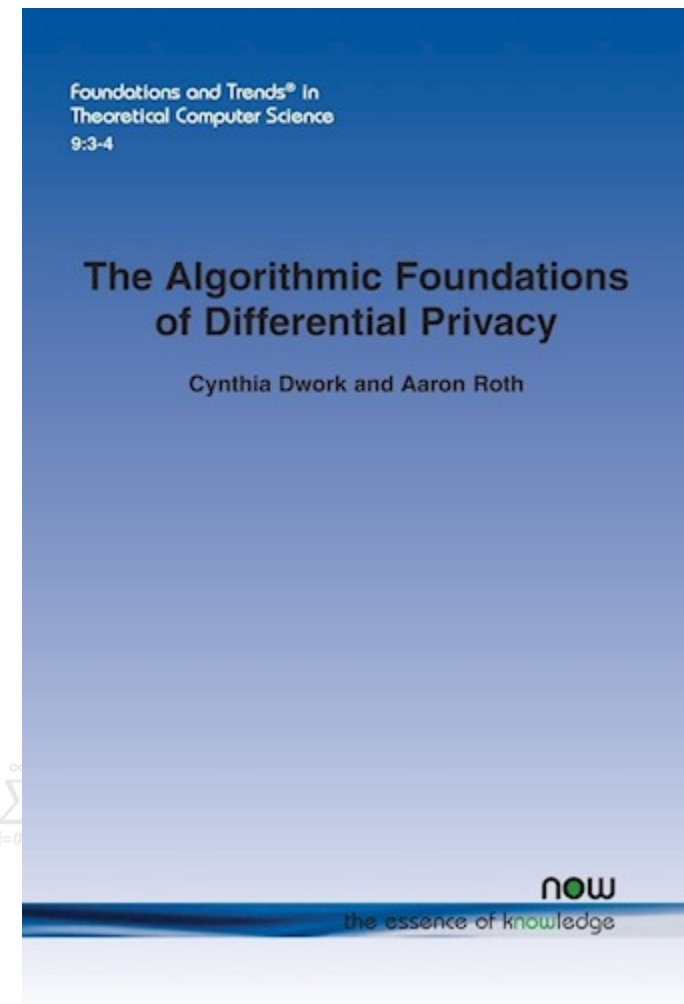
Probability of seeing output O on input D_2 → $\Pr[\mathcal{M}(D_2) \in O]$

$$\frac{\Pr[\mathcal{M}(D_1) \in O]}{\Pr[\mathcal{M}(D_2) \in O]} \leq e^\epsilon$$

Indistinguishability: bounded ratio of probabilities

Differential Privacy (DP)

- Cynthia Dwork and Aaron Roth, *The Algorithmic Foundations of Differential Privacy*:
<http://www.cis.upenn.edu/~aaroht/Papers/privacybook.pdf>
- Other data privacy methods:
 - k-anonymity
 - l-diversity
 - t-closeness



EU Regulations

- Existing Regulations
 - Electronic Identification and Trust Services (eIDAS)
 - Network and Information Systems (NIS) Regulation (critical infrastructure)
 - General Data Protection Regulation (GDPR)
 - Cybersecurity Act
 - Digital Services Act (primarily addressed towards large online platforms)
- Upcoming Regulations
 - NIS 2 (broader definition of critical infrastructure)
 - Digital Resilience Act
 - AI Act
 - Data Act
 - eIDAS 2
 - Combating Child Sexual Abuse Online (Chat Control regulation)