2019-03-04

IT Security #4

Privacy, GDPR, and PrivacyByDesign

Niels Christian Juul

Informatik
Datalogi
Roskilde Universitet

Roskilde Universitet
Niels Christian Juul
Hus 08.2-071
Universitetsvej 1
4000 Roskilde
ncjuul@ruc.dk

IT-security

Course book

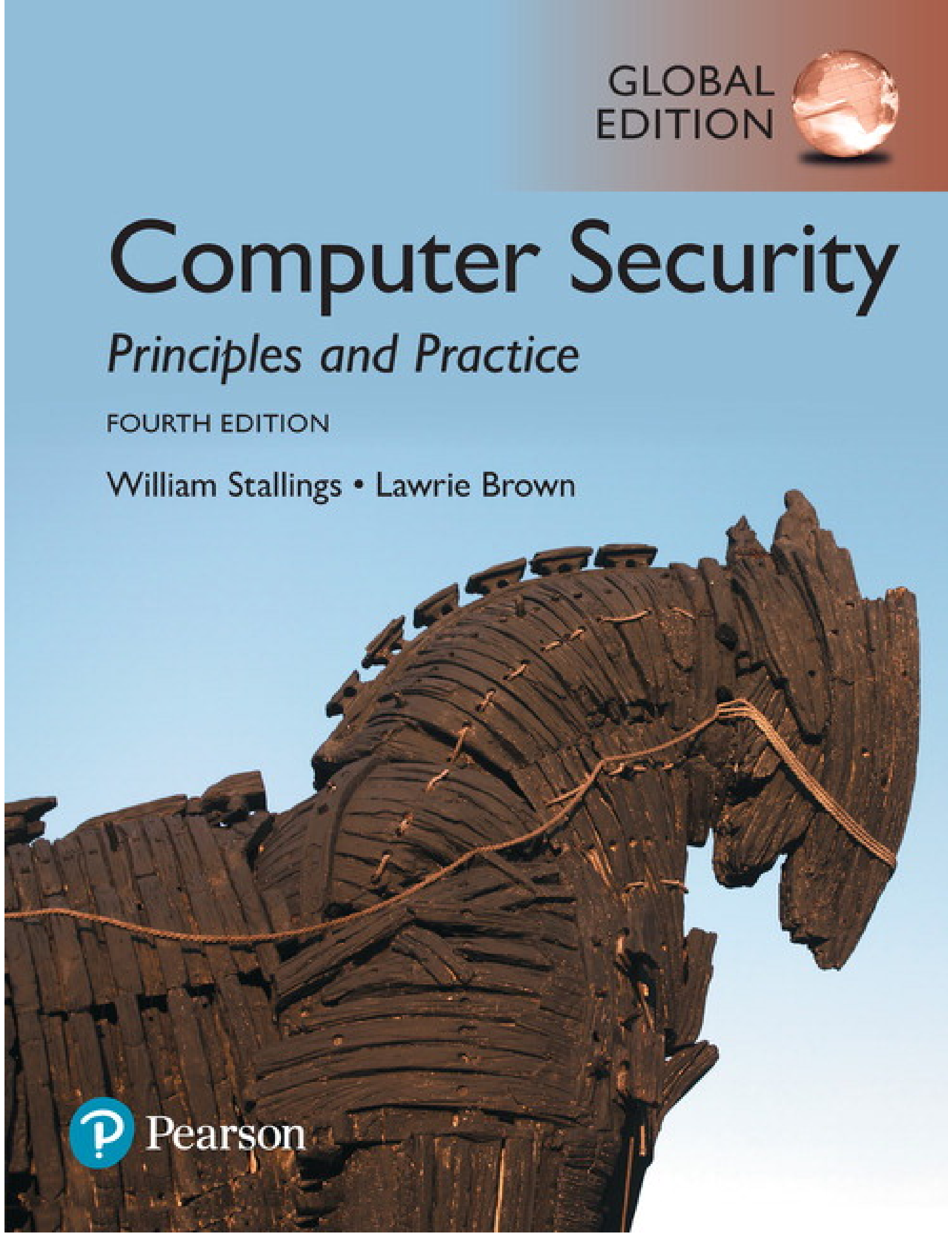
- Chapter 19 (19.1+19.3) today

Additional mandatory literature:

- Presthus, W., Sørum, H., & Andersen, L. R. (2018). GDPR compliance in Norwegian Companies. In: Proceedings from the annual NOKOBIT conference held at Svalbard the 18th-20th of September 2018, Vol 26 No 1.
- Colesky, M., Hoepman, J. H., & Hillen, C. (2016). A critical analysis of privacy design strategies. In 2016 IEEE Security and Privacy Workshops (SPW) (pp. 33-40). IEEE.

Background:

- Automatic Number Plate Recognition (Wikipedia)


GLOBAL EDITION

Computer Security

Principles and Practice

FOURTH EDITION

William Stallings • Lawrie Brown

Pearson

Learning outcome

- What is privacy?
- Why is it a requirement?
- How can we achieve it?

Exam themes/questions:

- What is GDPR and how should it be implemented in praxis?
- Show how Privacy can influence the design of an IT system

Additional knowledge not covered here, but part of the big picture:

- PrivacyByDesign (PbD), as defined by Ann Cavoukian, and Privacy Impact Assessment (PIA) is covered in BUITA class ITS1 (+ITS2)

Agenda

1. Intro (NC)
2. Cybercrime, Chapter 19.1 (Frederik).
3. Privacy, Chapter 19.3 (NC)
4. GDPR, article 1 (Natalia)
5. Privacy By Design, article 2 (Daniel)
6. ANPR (NC)
7. (Re-)design of ANPR for daily police work (NC)

Next time and next time again

- **Monday 11th March 13.15-17.00 (NJ)**
  Buffer overflows, cloud computing, and IoT
  Theme B: Software and system security.
- Student presentations:
  - Presentation of the article about "Code Red".
  - Presentation of the article about the webcam hack.
- **Monday 18th March 13.15-17.00 (NC)**
  Organizational IT Security Policy & Analysis & Implementation
  Theme C: Management issues (ii).
- Student presentations:
  - Security risk assessment (ch. 14.3)
  - Security controls, (ch. 15.2)

Agenda

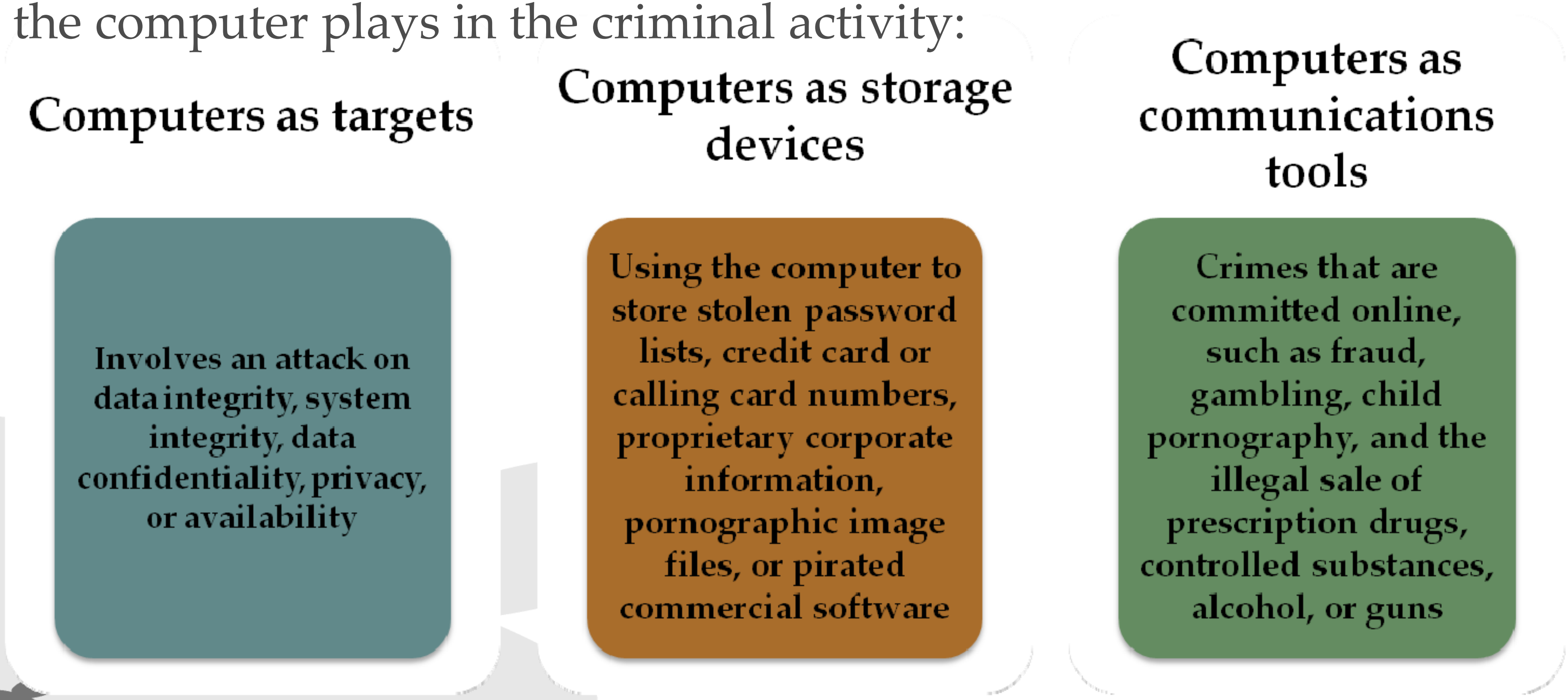
1. Intro (NC)
2. **Cybercrime, Chapter 19.1 (Frederik).**
3. Privacy, Chapter 19.3 (NC)
4. GDPR, article 1 (Natalia)
5. Privacy By Design, article 2 (Daniel)
6. ANPR (NC)
7. (Re-)design of ANPR for daily police work (NC)

“Computer crime, or cybercrime, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity.”

--From the New York Law School Course on Cybercrime, Cyberterrorism, and Digital Law Enforcement

Types of Computer Crime

- The U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity:



Computers as targets

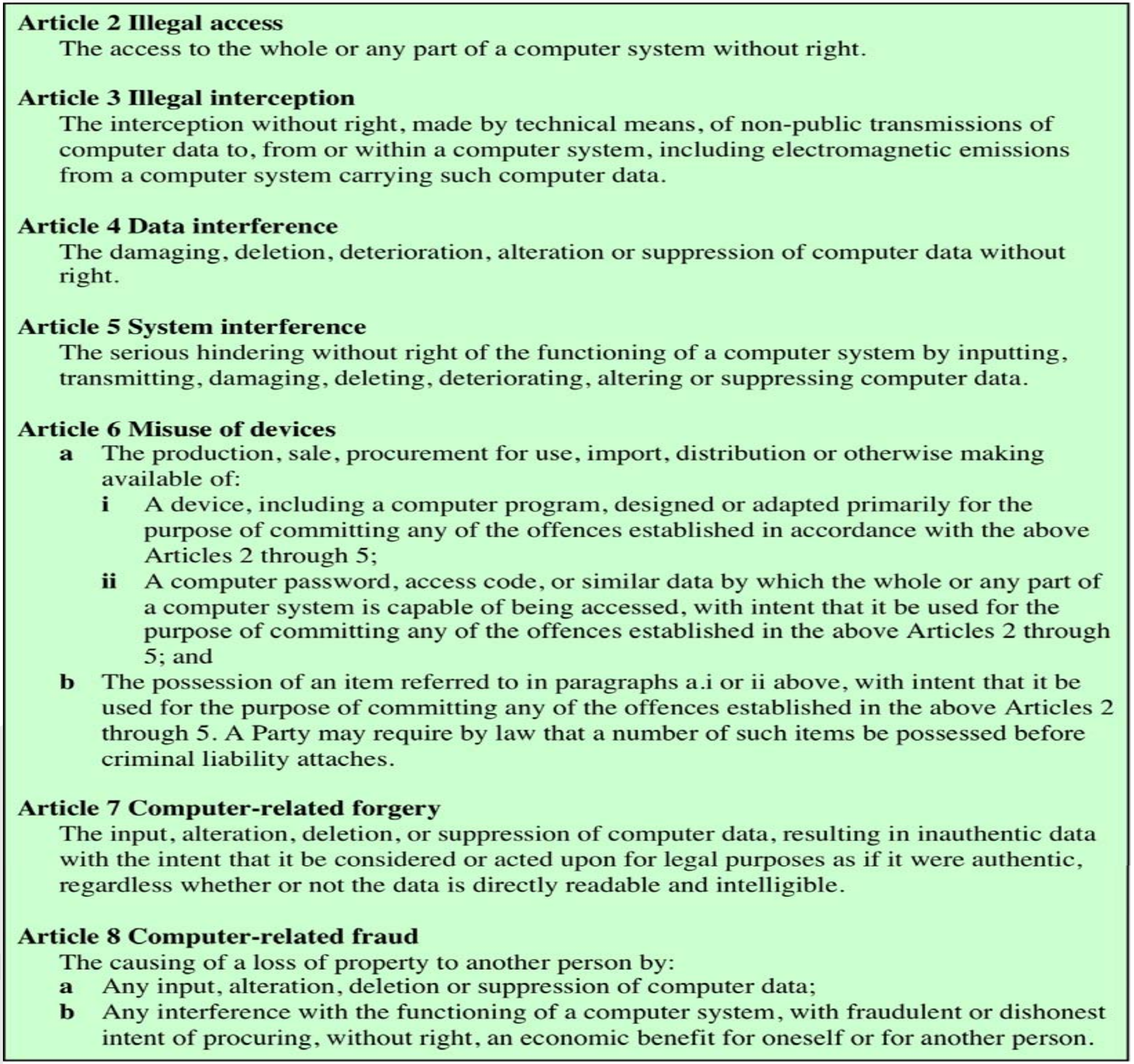
Involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability

Computers as storage devices

Using the computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or pirated commercial software

Computers as communications tools

Crimes that are committed online, such as fraud, gambling, child pornography, and the illegal sale of prescription drugs, controlled substances, alcohol, or guns



Article 2 Illegal access

The access to the whole or any part of a computer system without right.

Article 3 Illegal interception

The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Article 4 Data interference

The damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 System interference

The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 Misuse of devices

a The production, sale, procurement for use, import, distribution or otherwise making available of:

i A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; and

b The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Article 7 Computer-related forgery

The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Article 8 Computer-related fraud

The causing of a loss of property to another person by:

a Any input, alteration, deletion or suppression of computer data;

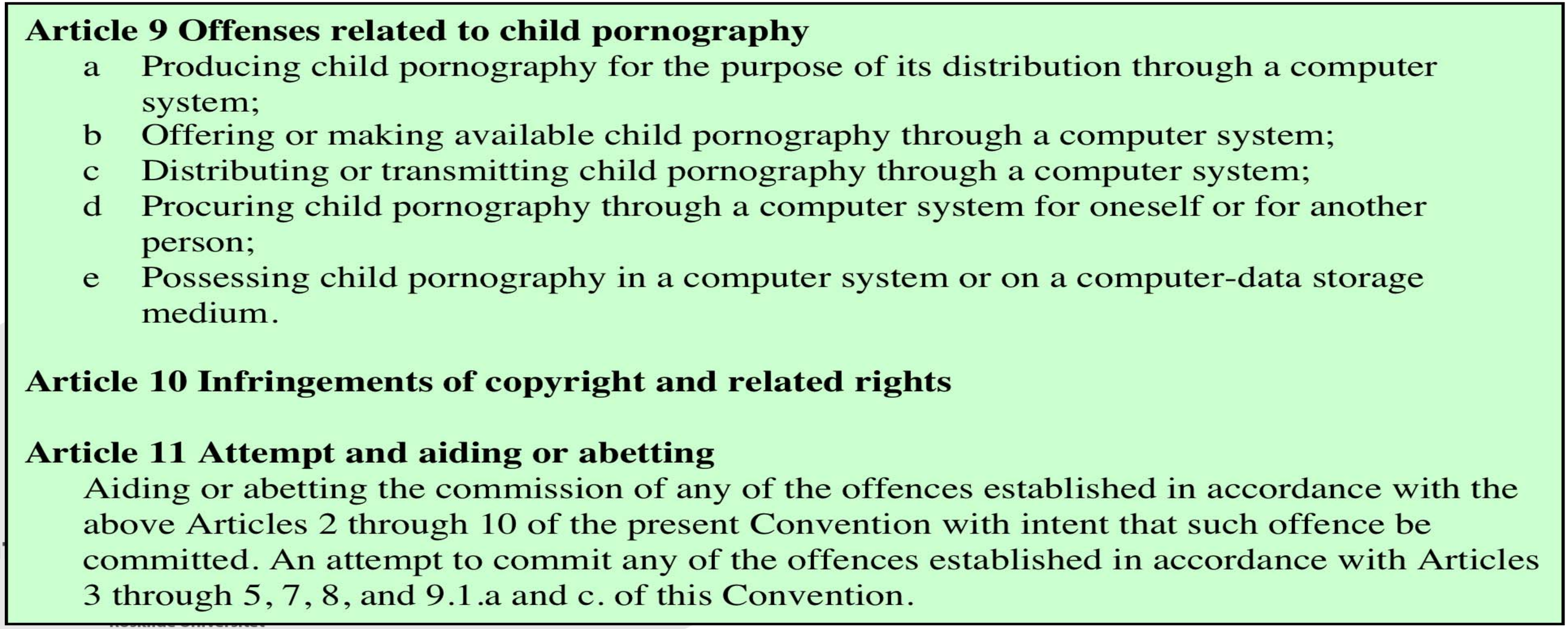
b Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Table 19.1

Cybercrimes Cited in the Convention on Cybercrime

(page 1 of 2)

Table 19.1
Cybercrimes Cited in the Convention on Cybercrime (page 2 of 2)



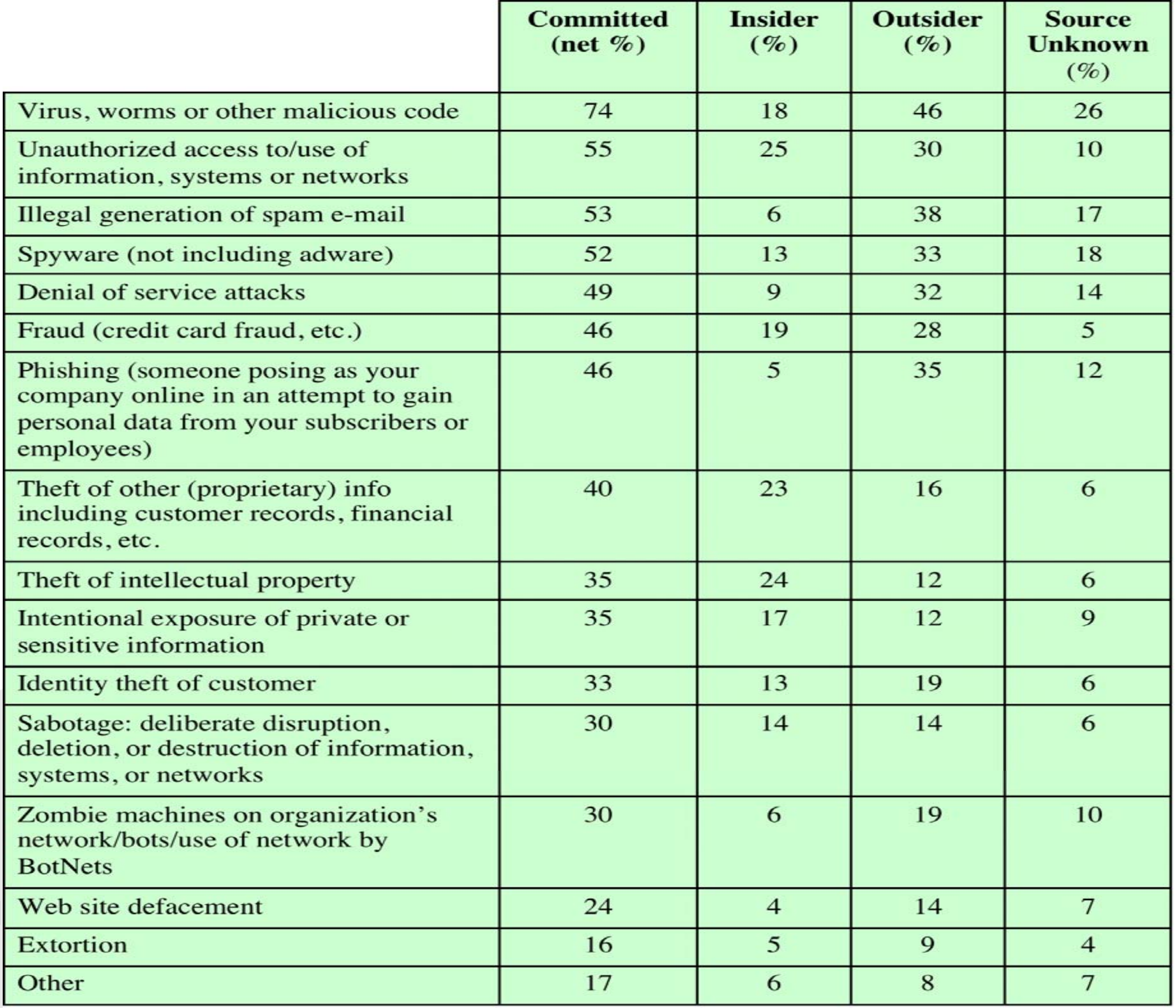
Article 9 Offenses related to child pornography

- a Producing child pornography for the purpose of its distribution through a computer system;
- b Offering or making available child pornography through a computer system;
- c Distributing or transmitting child pornography through a computer system;
- d Procuring child pornography through a computer system for oneself or for another person;
- e Possessing child pornography in a computer system or on a computer-data storage medium.

Article 10 Infringements of copyright and related rights

Article 11 Attempt and aiding or abetting

Aiding or abetting the commission of any of the offences established in accordance with the above Articles 2 through 10 of the present Convention with intent that such offence be committed. An attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.



	Committed (net %)	Insider (%)	Outsider (%)	Source Unknown (%)
Virus, worms or other malicious code	74	18	46	26
Unauthorized access to/use of information, systems or networks	55	25	30	10
Illegal generation of spam e-mail	53	6	38	17
Spyware (not including adware)	52	13	33	18
Denial of service attacks	49	9	32	14
Fraud (credit card fraud, etc.)	46	19	28	5
Phishing (someone posing as your company online in an attempt to gain personal data from your subscribers or employees)	46	5	35	12
Theft of other (proprietary) info including customer records, financial records, etc.	40	23	16	6
Theft of intellectual property	35	24	12	6
Intentional exposure of private or sensitive information	35	17	12	9
Identity theft of customer	33	13	19	6
Sabotage: deliberate disruption, deletion, or destruction of information, systems, or networks	30	14	14	6
Zombie machines on organization's network/bots/use of network by BotNets	30	6	19	10
Web site defacement	24	4	14	7
Extortion	16	5	9	4
Other	17	6	8	7

Table 19.2

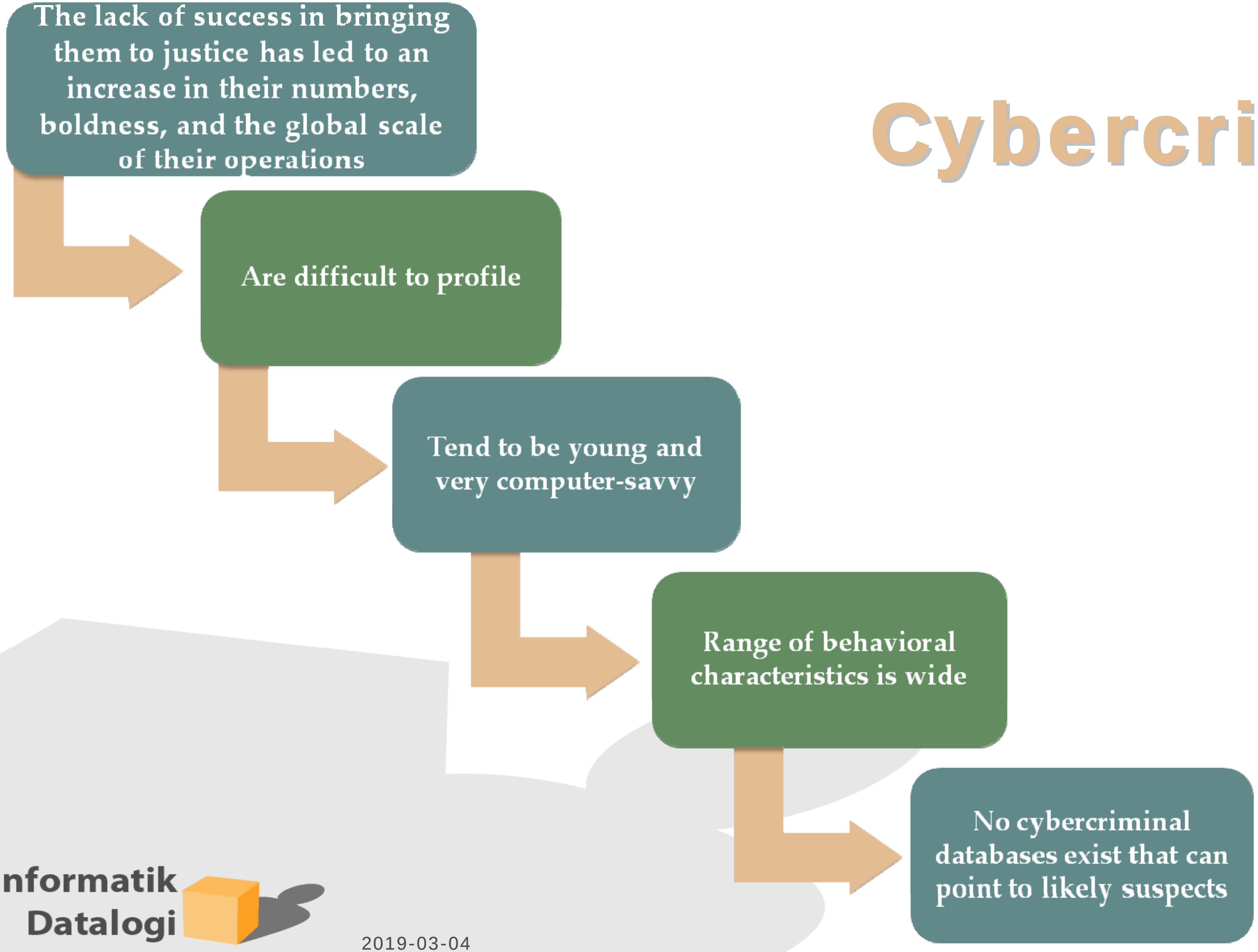
CERT 2007
E-Crime
Watch Survey Results

(Table can be found on page 582 in the textbook)

Law Enforcement Challenges

- The deterrent effect of law enforcement on computer and network attacks correlates with the success rate of criminal arrest and prosecution
- Law enforcement agency difficulties:
  - Lack of investigators knowledgeable and experienced in dealing with this kind of crime
  - Required technology may be beyond their budget
  - The global nature of cybercrime
  - Lack of collaboration and cooperation with remote law enforcement agencies
  - Convention on Cybercrime introduces a common terminology for crimes and a framework for harmonizing laws globally

Cybercriminals



The lack of success in bringing them to justice has led to an increase in their numbers, boldness, and the global scale of their operations

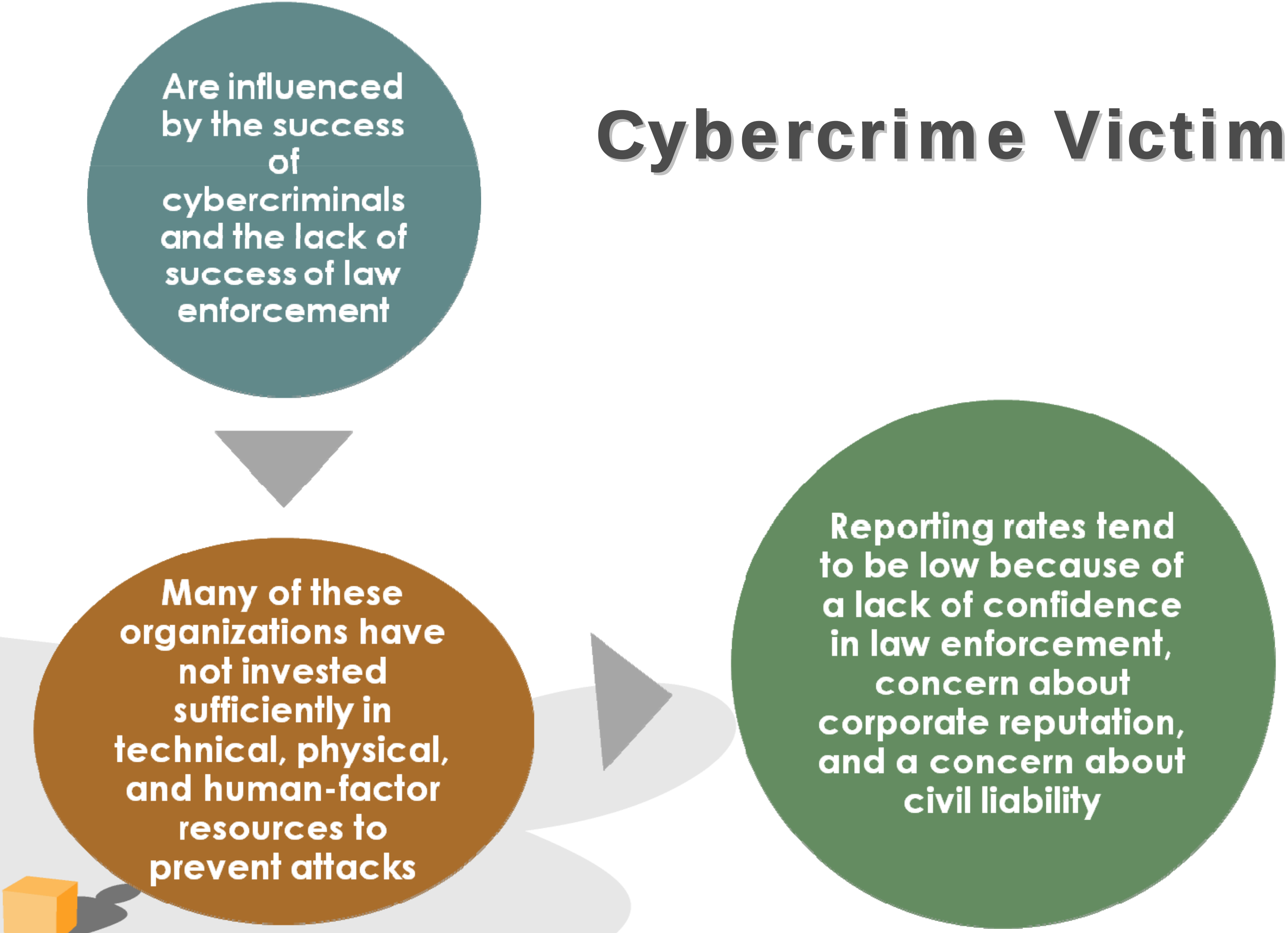
Are difficult to profile

Tend to be young and very computer-savvy

Range of behavioral characteristics is wide

No cybercriminal databases exist that can point to likely suspects

Cybercrime Victims



Are influenced by the success of cybercriminals and the lack of success of law enforcement

Many of these organizations have not invested sufficiently in technical, physical, and human-factor resources to prevent attacks

Reporting rates tend to be low because of a lack of confidence in law enforcement, concern about corporate reputation, and a concern about civil liability

Working with Law Enforcement

- Executive management and security administrators need to look upon law enforcement as a resource and tool
- Management needs to:
  - Understand the criminal investigation process
  - Understand the inputs that investigators need
  - Understand the ways in which the victim can contribute positively to the investigation

Agenda

1. Intro (NC)
2. Cybercrime, Chapter 19.1 (Frederik).
3. **Privacy, Chapter 19.3 (NC)**
4. GDPR, article 1 (Natalia)
5. Privacy By Design, article 2 (Daniel)
6. ANPR (NC)
7. (Re-)design of ANPR for daily police work (NC)

Privacy

- Overlaps with computer security
- Dramatic increase in scale of information collected and stored
    - Motivated by law enforcement, national security, economic incentives
- Individuals have become increasingly aware of access and use of personal information and private details about their lives
- Concerns about extent of privacy compromise have led to a variety of legal and technical approaches to reinforcing privacy rights

A Privacy Definition

- Privacy: *The right of people to choose freely under what circumstances and to what extent they will reveal themselves, their attitude, and their behavior to others*
- Threats to Privacy: Government and business
  - Regime spying on citizens
  - Employee surveillance
  - Customer surveillance (trading private information for business)
  - Use/abuse of transaction information (or citizen records)

Privacy and Data Surveillance

The demands of big business, government and law enforcement have created new threats to personal privacy

Ex.

- Scientific and medical research data collection for analysis
- Law enforcement data surveillance
- Private organizations profiling

This creates tension between enabling beneficial outcomes in areas including scientific research, public health, national security, law enforcement and efficient use of resources, while still respecting an individual's right to privacy

Privacy and Data Surveillance

Another areas of particular concern is the rapid rise in the use of public social media sites:

- These sites gather, analyze, and share large amounts of data on individuals and their interactions with other individuals and organizations
- Many people willingly upload large amounts of personal information, including photos and status updates
- This data could potentially be used by current and future employers, insurance companies, private investigators, and others, in their interactions with the individual

Exercise

Your privacy has many violators.

2 by 2 – 7 minutes with your neighbor student

1. Make a list of classes of violators
2. Assess the likelihood (0%..100%) that your privacy is threatened by each
3. Assess the harm between 0(no)..10(catastrophic)) due to each violation

Which violator should you care most about (and which less) ?

Privacy Protection

- Both policy and technical approaches are needed to protect privacy
- In terms of technical approaches, the requirements for privacy protection for data stored on information systems can be addresses in part using the technical mechanisms developed for database security
- In terms of policy approaches, overall regulations like OECD Guidelines, GDPR, etc must be implemented in each organization

How to protect privacy

System designers shall use:

- **PIA**
  Privacy Impact Assesement
- **PET**
  Privacy Enhancing Technology
- **PbD**
  Privacy by Design

PET – Privacy Enhancing Technology

- Data minimization
- Unlinkability
- Informed consent
- Virtual identities
- Anonymous credentials
- Transaction logs

Data mining challenge: big data

- Privacy leakage problem

1. solution:

- Remove all identification data

2. Solution

- Anonymize (e.g. use pseudonyms)

But:

- Can de-identified data be re-identified?

PRIVACY

Credit card study blows holes in anonymity

Attack suggests need for new data safeguards

By John Bohannon

For social scientists, the age of big data carries big promises: a chance to mine demographic, financial, medical, and other vast data sets in fine detail to learn how we lead our lives. For privacy advocates, however, the prospect is alarming. They worry that the people represented in such data may not stay anonymous for long. A study of credit card data in this week's issue of *Science* (p. 536) bears out those fears, showing that it takes only a tiny amount of personal information to de-anonymize people.

The result, coming on top of earlier demonstrations that personal identities are easy to pry from anonymized data sets, indicates that such troves need new safeguards. "In light of the results, data custodians should carefully limit access to data," says Arvind Narayanan, a computer scientist at Princeton

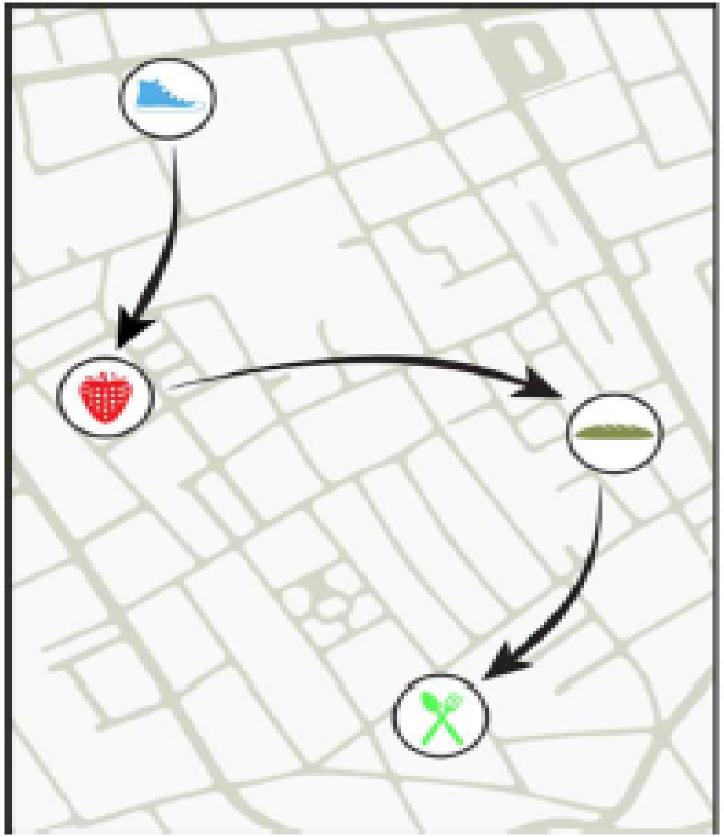
One correlation attack became famous last year when the New York City Taxi and Limousine Commission released a data set of the times, routes, and cab fares for 173 million rides. Passenger names were not included. But armed with time-stamped photos of celebrities getting in and out of taxis—there are websites devoted to celebrity spotting—bloggers, after deciphering taxi driver medallion numbers, easily figured out

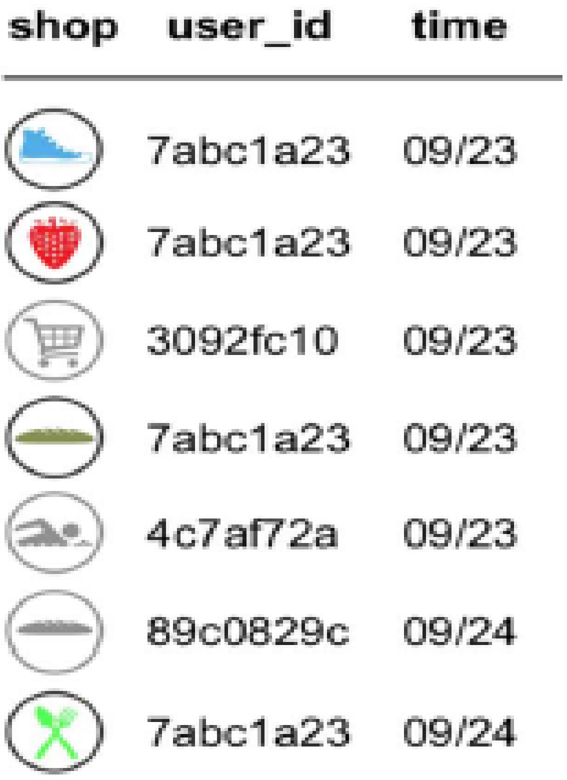
the amount spent on those occasions—the equivalent of a few receipts from someone's trash—made it possible to de-anonymize nearly everyone and trace their entire transaction history with just three pieces of information per person. The findings echo the results of a 2013 *Scientific Reports* study in which de Montjoye and colleagues started with a trove of mobile phone metadata on subscribers' movements and showed that knowing a person's location on four occasions was enough to identify them.

One way to protect against correlation attacks is to blur the data by binning certain variables. For example, rather than revealing the exact day or price of a transaction, the public version of the data set might reveal only the week in which it occurred or a price range within which it fell. Binning did not thwart de Montjoye's correlation attack; instead, it only increased the amount of information needed to de-anonymize each person to the equivalent of a dozen receipts.

These studies needn't be the death knell for social science research using big data. "We need to bring the computation to the data, not the other way around," de Montjoye says. Big data with sensitive information could live "in the cloud," protected by gatekeeper software, he says. The gatekeeper would not allow access to individual people, thwarting correlation

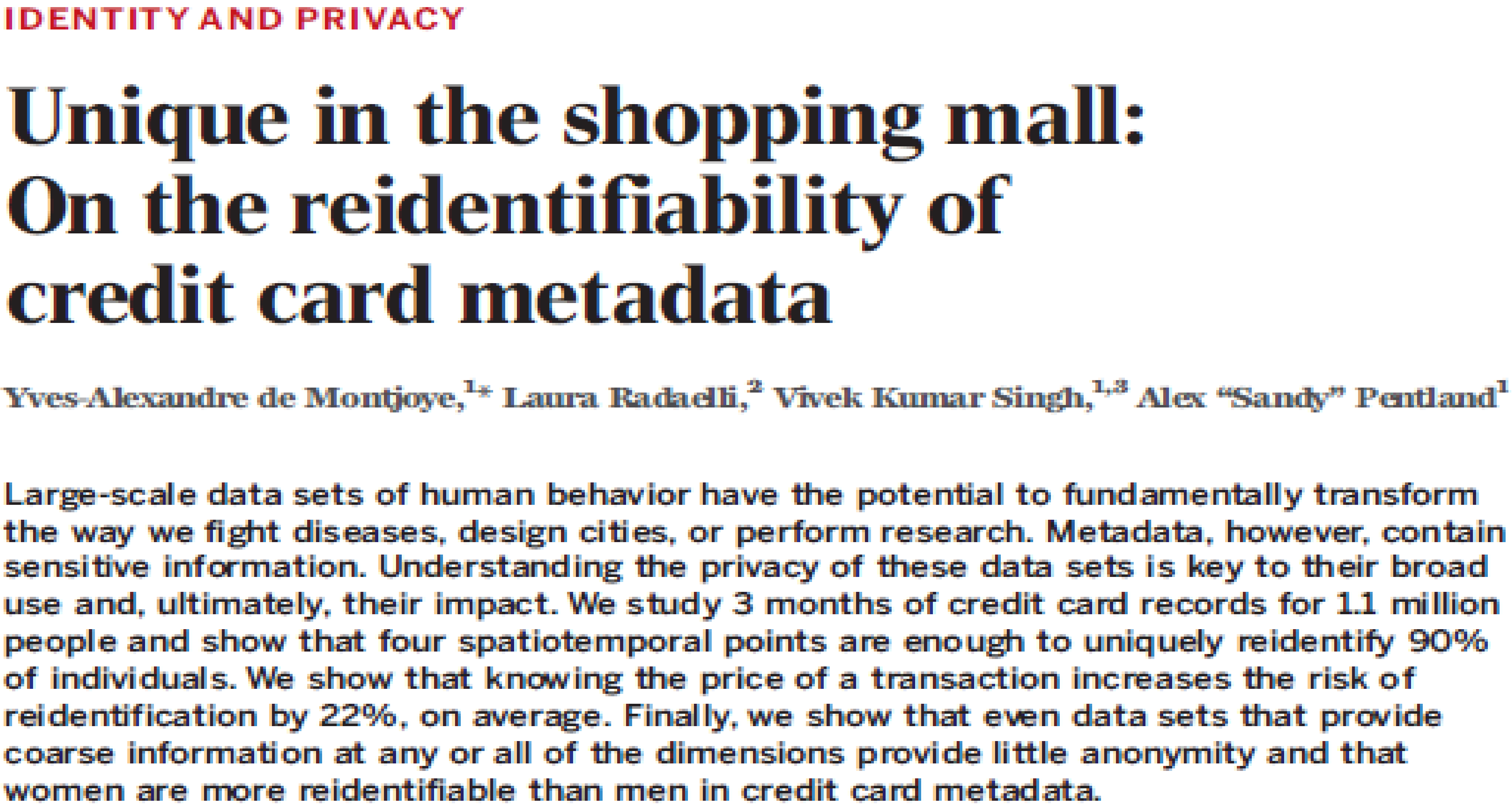
Anonymous data about 1.1 mill people shopping in 10.000 shops during 3 month





shop	user_id	time
👟	7abc1a23	09/23
🍓	7abc1a23	09/23
🛒	3092fc10	09/23
🥖	7abc1a23	09/23
🏊	4c7af72a	09/23
🥖	89c0829c	09/24
🍴	7abc1a23	09/24

- Add the equivalent of a photo with timestamp, eg. name and data
- In 9 out of 10 cases we can link to the right user_id, if the person did four purchases
- Add prices to the purchases in our dataset, and we have 95% hits.



IDENTITY AND PRIVACY

Unique in the shopping mall: On the reidentifiability of credit card metadata

Yves-Alexandre de Montjoye,[1*] Laura Radaelli,[2] Vivek Kumar Singh,[1,3] Alex "Sandy" Pentland[1]

Large-scale data sets of human behavior have the potential to fundamentally transform the way we fight diseases, design cities, or perform research. Metadata, however, contain sensitive information. Understanding the privacy of these data sets is key to their broad use and, ultimately, their impact. We study 3 months of credit card records for 1.1 million people and show that four spatiotemporal points are enough to uniquely reidentify 90% of individuals. We show that knowing the price of a transaction increases the risk of reidentification by 22%, on average. Finally, we show that even data sets that provide coarse information at any or all of the dimensions provide little anonymity and that women are more reidentifiable than men in credit card metadata.

Additional exercises with your class mate

- Two by two
- 5 minutes

Find at least one additional case / study that prove privacy risks in big data?

Try to identify:

- What system
- Origin of data
- Risk including both positive and negative outcome of studies system

Privacy Protection

With regard to social media sites, technical controls include:

- The provision of suitable privacy settings to manage who can view data on individuals
- Notification when one individual is referenced or tagged in another's content
- Although social media sites include some form of these controls, they are constantly changing, causing frustration for users who are trying to keep up with these mechanisms
- Another approach for managing privacy concerns in big data analysis is to anonymize the data, removing any personally identifying information before release to researchers or other organizations for analysis

Data Privacy

- In terms of policy, guidelines are needed to manage the use and reuse of big data, ensuring suitable constraints are imposed in order to preserve privacy
    - **Consent**
      Ensuring participants can make informed decisions about their participation in the research
    - **Privacy and confidentiality**
      Privacy is the control that individuals have over who can access their personal information
      Confidentiality is the principle that only authorized persons should have access to information
    - **Ownership and authorship**
      Addresses who has responsibility for the data, and at what point does an individual give up their right to control their personal data
    - **Data sharing – assessing the social benefits of research**
      The social benefits that result from data matching and reuse of data from one source or research project in another
    - **Governance and custodianship**
      Oversight and implementation of the management, organization, access, and preservation of digital data

Fair Information Practices

- OECD (Organization of Economic Cooperation and Development) in 1980 developed the standard eight-point list of privacy principles:

- Limited Collection Principle
- Quality Principle
- Purpose Principle
- Use Limitation Principle

- Security Principle
- Openness Principle
- Participation Principle
- Accountability Principle

Same 8 principles in 2013 OECD Guidelines. Table 19.3, p.625

OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA © OECD 2013

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA © OECD 2013

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the preceding principle except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA © OECD 2013

Individual Participation Principle

Individuals should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

b) to have communicated to them, data relating to them

i. within a reasonable time;

ii. at a charge, if any, that is not excessive;

iii. in a reasonable manner; and

iv. in a form that is readily intelligible to them;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA © OECD 2013

Accountability Principle

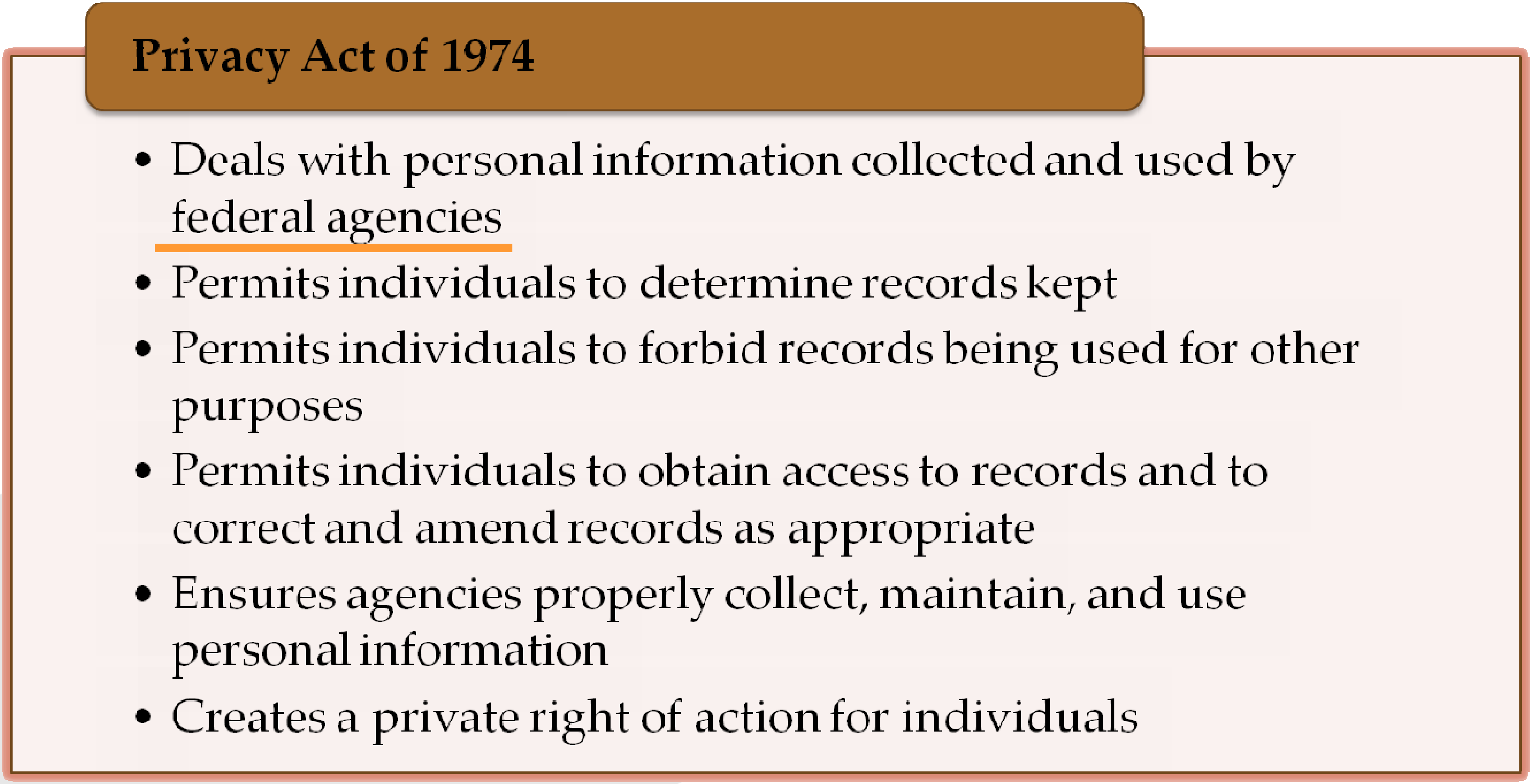
A data controller should be accountable for complying with measures which give effect to the principles stated above.

Following OECD Guidelines….

- European Union had European Data Protection Directive (OECD principles) since 1995
- EU Directive requires data on EU citizens to be protected at same standard even when it leaves their country (Directive 95/46/EC)
- EU General Data Protection Regulation (GDPR) in force May 2018
- China does not protect privacy
- U.S. has not adopted OECD principles

BUT

United States Privacy Initiatives: citizen vs government



Privacy Act of 1974

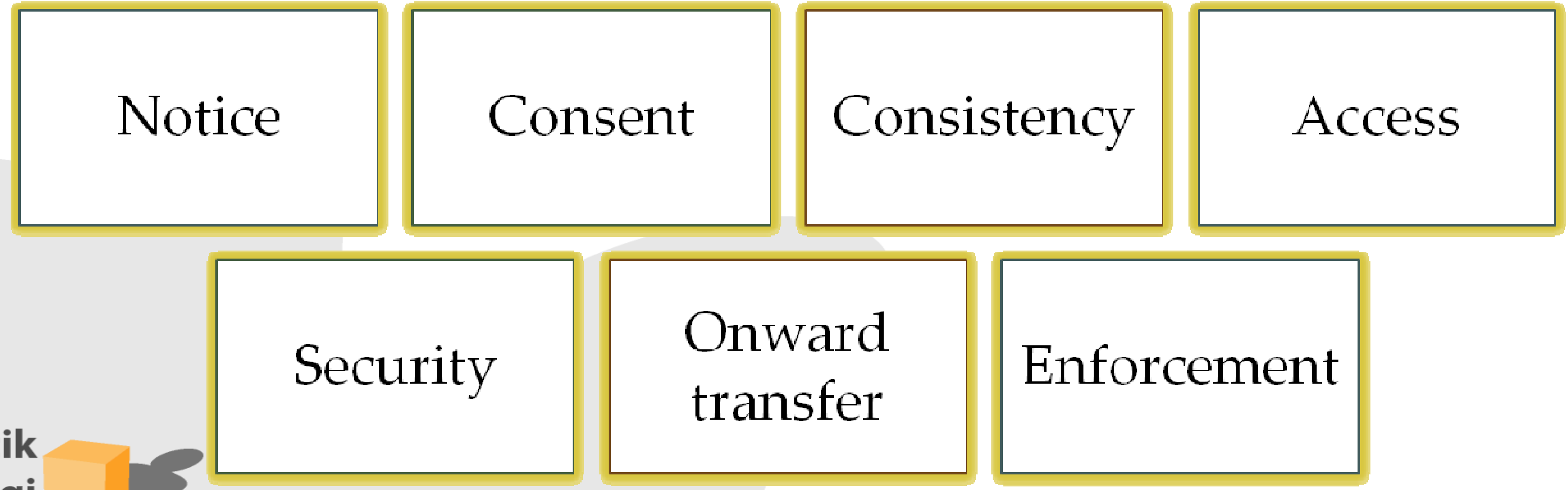
- Deals with personal information collected and used by federal agencies
- Permits individuals to determine records kept
- Permits individuals to forbid records being used for other purposes
- Permits individuals to obtain access to records and to correct and amend records as appropriate
- Ensures agencies properly collect, maintain, and use personal information
- Creates a private right of action for individuals

US Laws Protecting Privacy: single sector, single state

- Federal Trade Commission Act, 1914 (FTCA)
- Fair Credit Reporting Act, 1970 (FCRA)
- Electronic Communication Privacy Act, 1986 (ECPA)
- Video Privacy Protection Act, 1988 (VPPA)
- Telephone Consumer Protection Act, 1991 (TCPA)
- Driver's Privacy Protection Act, 1994 (DPPA)
- Health Insurance Privacy and Accountability Act, 1996 (HIPAA)
- Financial Services Modernization Act, 1999 (Gramm-Leach-Bliley Act (GLBA))
- Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003 (CAN-SPAM)
- Data Security and Breach Notification Act *Proposal 2017* (DSBN)
- California Consumer Privacy Act of 2018 (CCPA), eff. 2020

European Union (EU) Directive on Data Protection

- Adopted in 1995 to:
  - Ensure member states protect fundamental privacy rights when processing personal information
  - Prevent member states from restricting the free flow of personal information within EU
- Organized around principles of:



Notice

Consent

Consistency

Access

Security

Onward transfer

Enforcement

The right to be forgotten

- Proposal for the new EU Data Regulation to supersede the Data Protection Directive
- Started out with "the net never forget" challenge:
- Vivian Reading, former commissioner, responded:

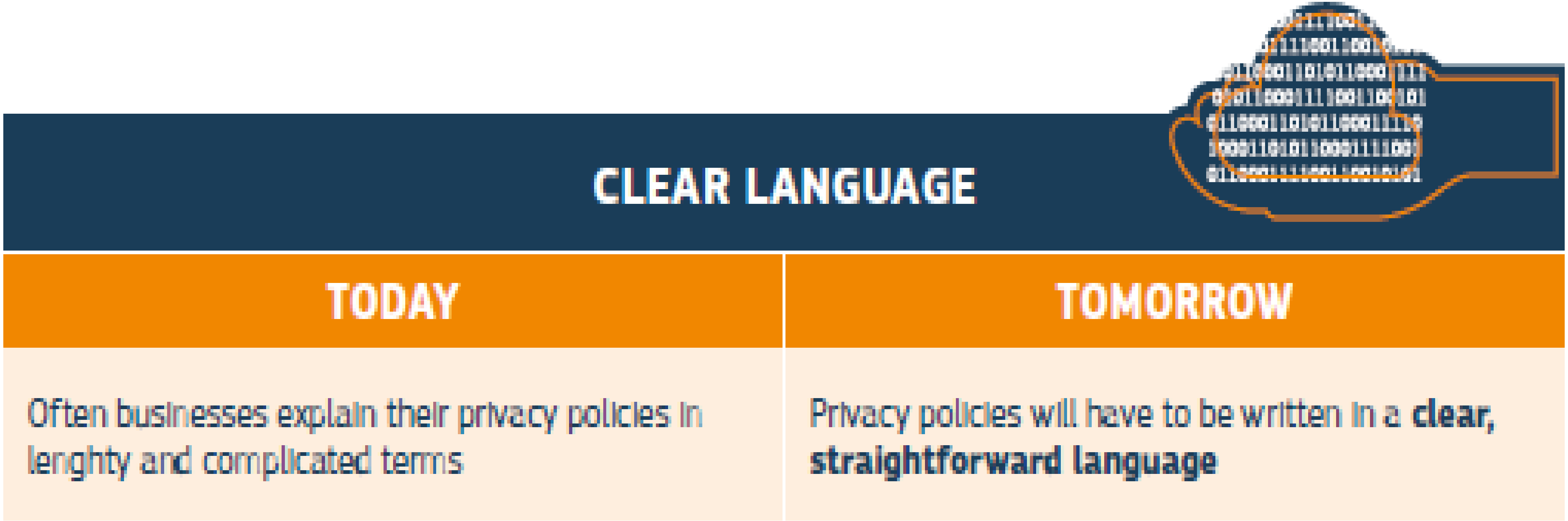
  "The right to be forgotten"
- and finally became

ISO 27002 states . . .

"An organization's data policy for privacy and protection of personally identifiable information should be developed and implemented. This policy should be communicated to all persons involved in the processing of personally identifiable information. Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personally identifiable information should be implemented."

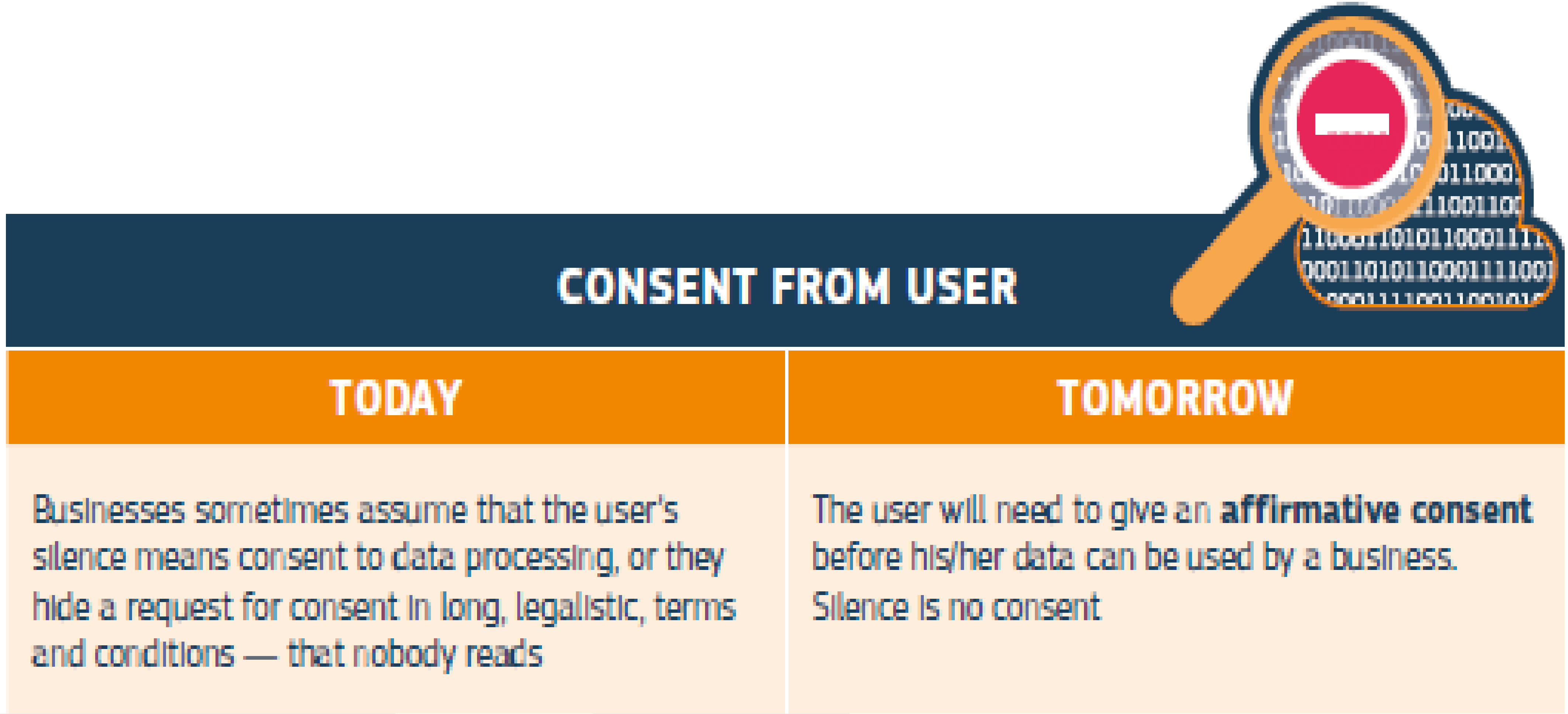
Agenda

1. Intro (NC)
2. Cybercrime, Chapter 19.1 (Frederik).
3. Privacy, Chapter 19.3 (NC)
4. **GDPR, article 1 (Natalia)**
5. Privacy By Design, article 2 (Daniel)
6. ANPR (NC)
7. (Re-)design of ANPR for daily police work (NC)



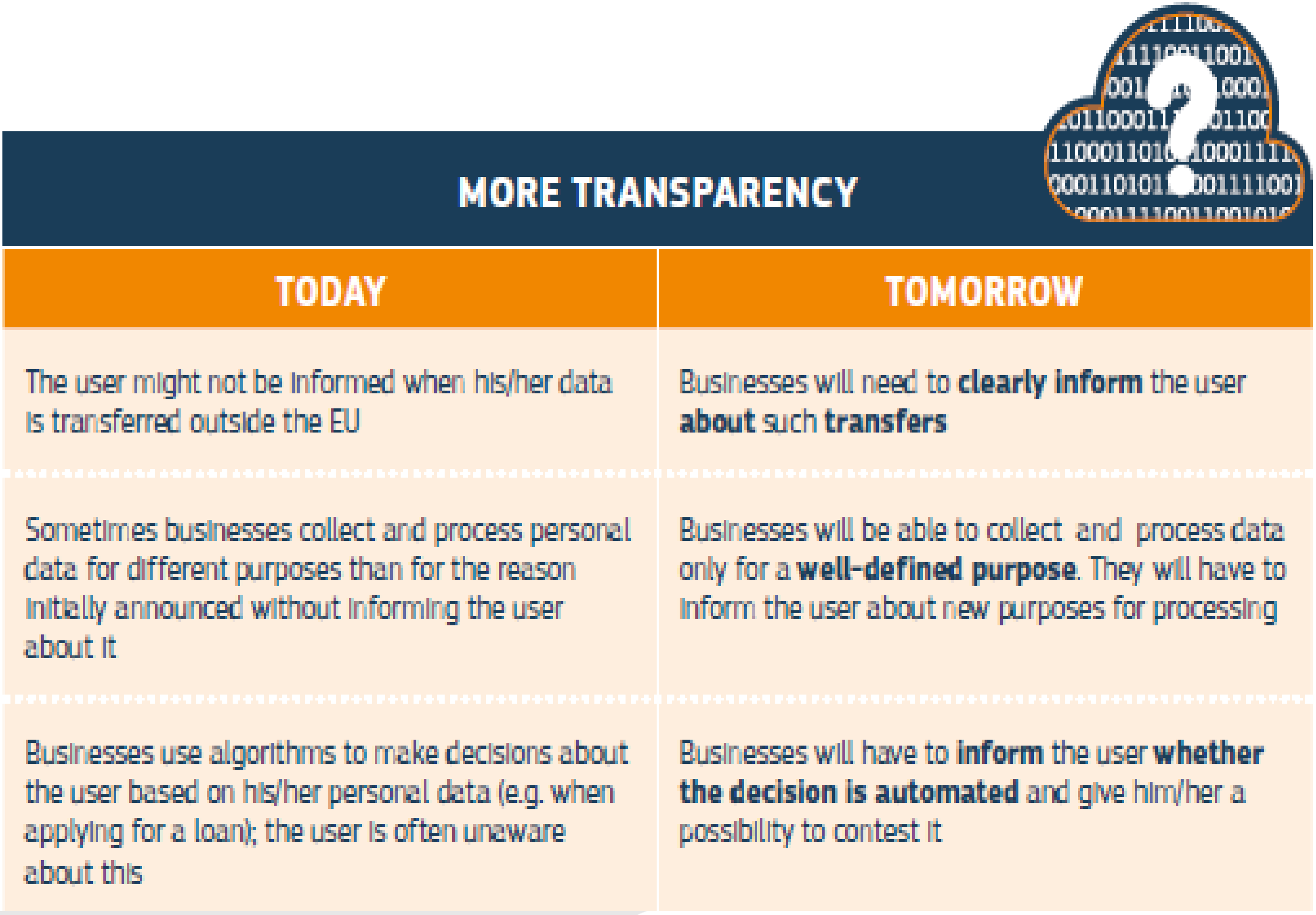
CLEAR LANGUAGE

TODAY	TOMORROW
Often businesses explain their privacy policies in lenghty and complicated terms	Privacy policies will have to be written in a **clear, straightforward language**



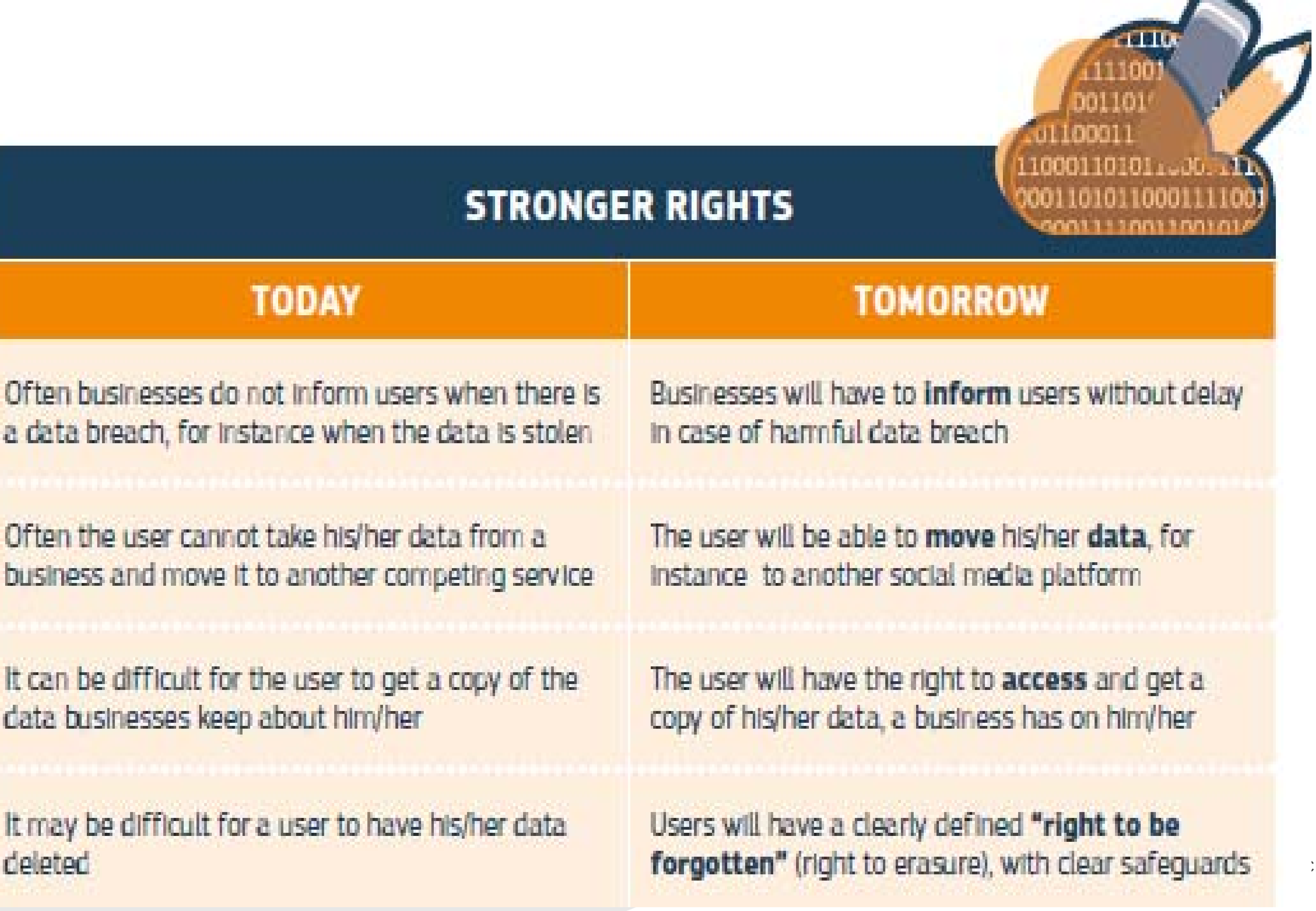
CONSENT FROM USER

TODAY	TOMORROW
Businesses sometimes assume that the user's silence means consent to data processing, or they hide a request for consent in long, legalistic, terms and conditions — that nobody reads	The user will need to give an **affirmative consent** before his/her data can be used by a business. Silence is no consent



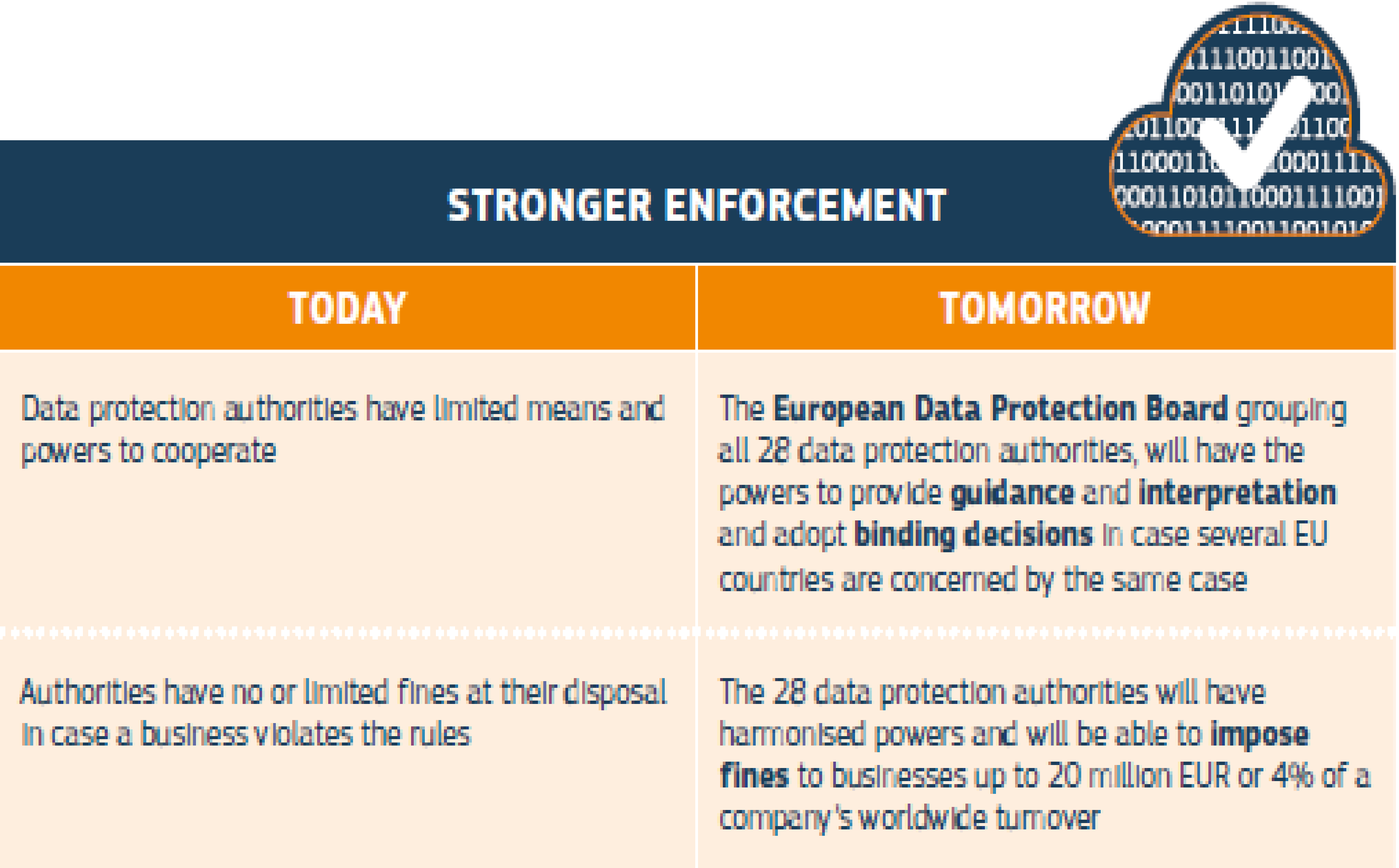
MORE TRANSPARENCY

TODAY	TOMORROW
The user might not be informed when his/her data is transferred outside the EU	Businesses will need to **clearly inform** the user **about** such **transfers**
Sometimes businesses collect and process personal data for different purposes than for the reason initially announced without informing the user about it	Businesses will be able to collect and process data only for a **well-defined purpose**. They will have to inform the user about new purposes for processing
Businesses use algorithms to make decisions about the user based on his/her personal data (e.g. when applying for a loan); the user is often unaware about this	Businesses will have to **inform** the user **whether the decision is automated** and give him/her a possibility to contest it



STRONGER RIGHTS

TODAY	TOMORROW
Often businesses do not inform users when there is a data breach, for instance when the data is stolen	Businesses will have to **inform** users without delay in case of harmful data breach
Often the user cannot take his/her data from a business and move it to another competing service	The user will be able to **move** his/her **data**, for instance to another social media platform
It can be difficult for the user to get a copy of the data businesses keep about him/her	The user will have the right to **access** and get a copy of his/her data, a business has on him/her
It may be difficult for a user to have his/her data deleted	Users will have a clearly defined **"right to be forgotten"** (right to erasure), with clear safeguards



STRONGER ENFORCEMENT

TODAY	TOMORROW
Data protection authorities have limited means and powers to cooperate	The **European Data Protection Board** grouping all 28 data protection authorities, will have the powers to provide **guidance** and **interpretation** and adopt **binding decisions** in case several EU countries are concerned by the same case
Authorities have no or limited fines at their disposal in case a business violates the rules	The 28 data protection authorities will have harmonised powers and will be able to **impose fines** to businesses up to 20 million EUR or 4% of a company's worldwide turnover

Agenda

1. Intro (NC)
2. Cybercrime, Chapter 19.1 (Frederik).
3. Privacy, Chapter 19.3 (NC)
4. GDPR, article 1 (Natalia)
5. **Privacy By Design, article 2 (Daniel)**
6. ANPR (NC)
7. (Re-)design of ANPR for daily police work (NC)

Privacy by Design

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner
Ontario, Canada

Ir

PbD – Privacy by Design

1. *Proactive* not Reactive; *Preventative* not Remedial
2. Privacy as the *Default Setting*
3. Privacy *Embedded* into 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*

PbD – Privacy by Design

7 Foundational Principles

1. *Proactive* not Reactive; *Preventative* not Remedial

- The *Privacy by Design* (*PbD*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

PbD – Privacy by Design

2. Privacy as the *Default Setting*

- We can all be certain of one thing – the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

3. Privacy *Embedded* into Design

- Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

PbD – Privacy by Design

4. Full Functionality – *Positive-Sum*, not Zero-Sum

- *Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Security – *Full Lifecycle Protection*

- *Privacy by Design*, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

PbD – Privacy by Design

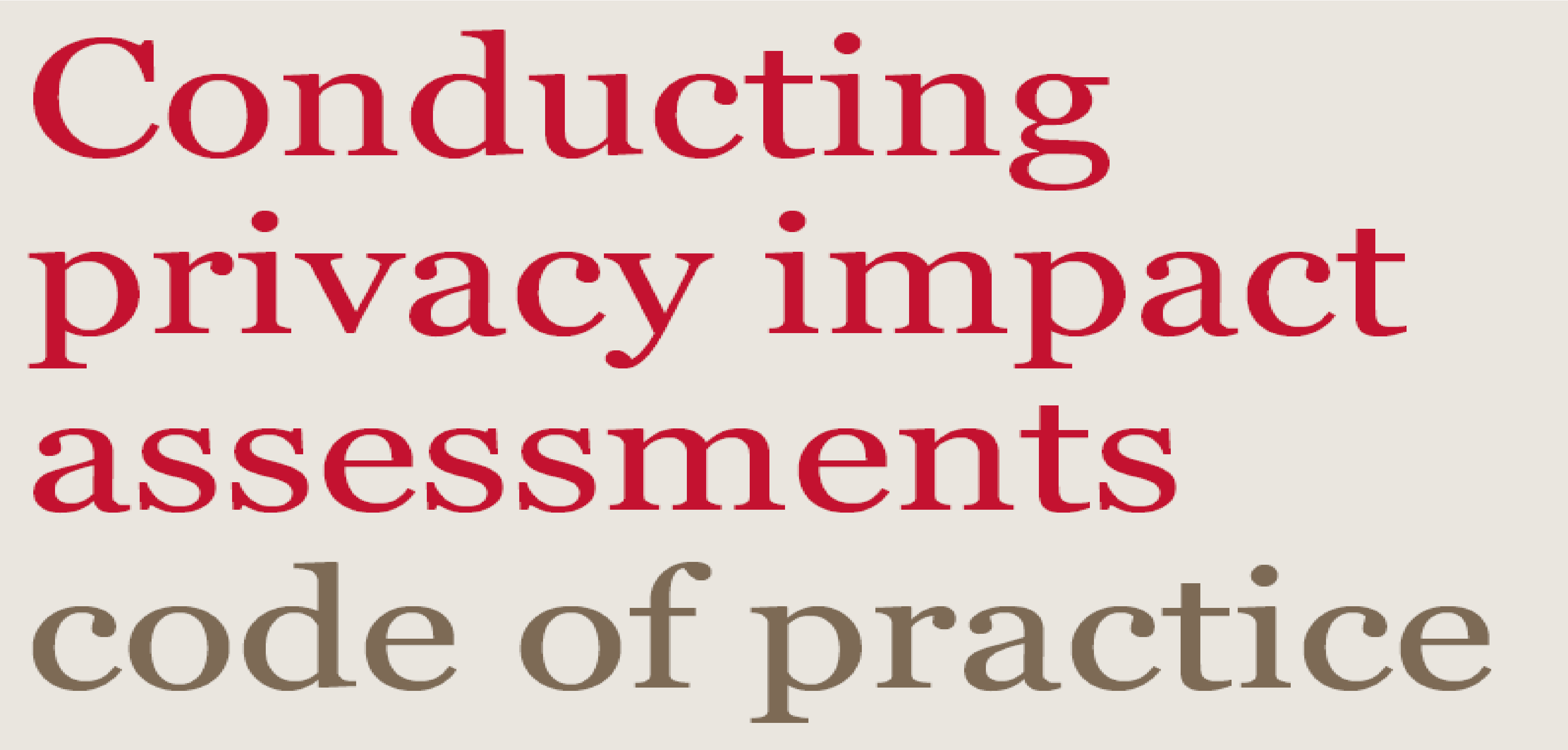
6. *Visibility* and *Transparency* – Keep it *Open*

- *Privacy by Design* seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. *Respect* for User Privacy – Keep it *User-Centric*

- Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

PIA – Privacy Impact Assesment



Conducting privacy impact assessments code of practice

A PIA should incorporate the following steps:

1. Identify the need for a PIA
2. Describe the information flows
3. Identify the privacy and related risks
4. Identify and evaluate the privacy solutions
5. Sign off and record the PIA outcomes
6. Integrate the outcomes into the project plan
7. Consult with internal and external

Overview of the PIA process

1. Identifying the need for a PIA.

- The need for a PIA can be identified as part of an organisation’s usual project management process or by using the screening questions in annex two of this Code.

2. Describing the information flows.

- Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information

Overview of the PIA process

3. Identifying the privacy and related risks.

- Some will be risks to individuals – for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy.
- Some risks will be to the organisation - for example damage to reputation, or the financial costs or a data breach.
- Legal compliance risks include the DPA, PECR, and the Human Rights Act.

Overview of the PIA process

4. Identifying and evaluating privacy solutions.

- Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.
- Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.

Overview of the PIA process

5. Signing off and recording the PIA outcomes.

- Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval.
- A PIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.
- Publishing a PIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.

Overview of the PIA process

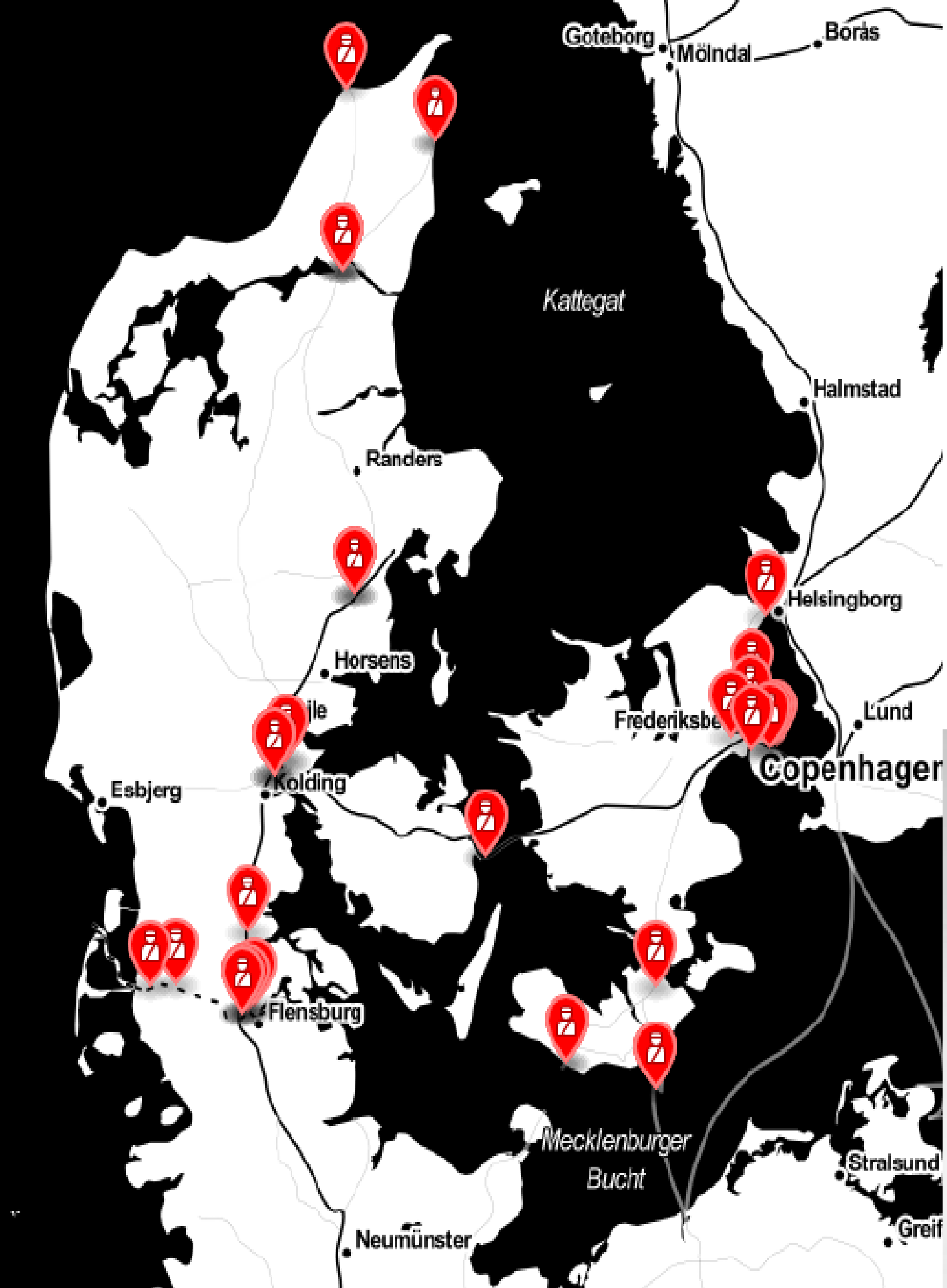
6. **Integrating the PIA outcomes back into the project plan.**

- The PIA findings and actions should be integrated with the project plan. It might be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.
- A PIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored.
- Record what you can learn from the PIA for future projects.

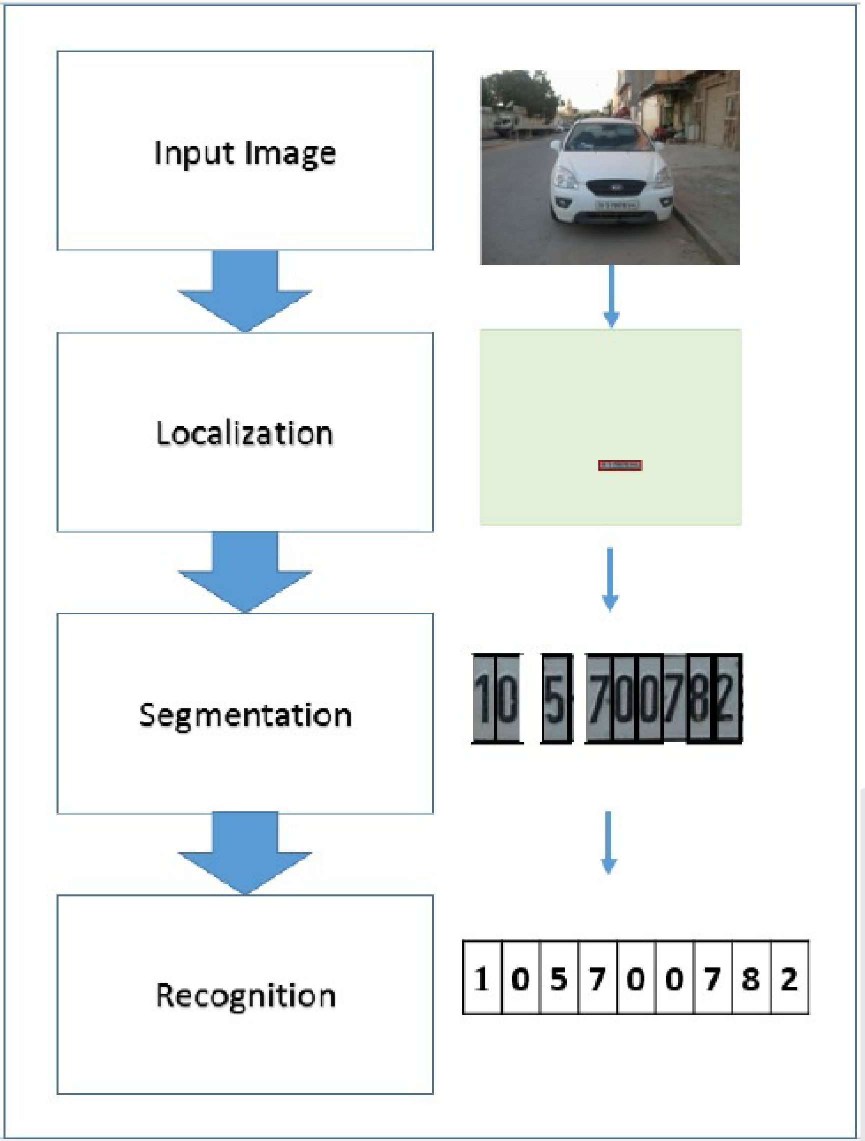
Agenda

1. Intro (NC)
2. Cybercrime, Chapter 19.1 (Frederik).
3. Privacy, Chapter 19.3 (NC)
4. GDPR, article 1 (Natalia)
5. Privacy By Design, article 2 (Daniel)
6. **ANPR (NC)**
7. (Re-)design of ANPR for daily police work (NC)

ANPG stationary positions



Automated Number Plate Recognition



- System installed in Police cars and stationary on road sides.
- ANPR generates plate numbers and other data about cars seen by the cameras (infrared view, no blitz)
- Works with a dynamic and updated **hotlist** of "wanted" plate numbers managed by the police, i.e. cars worth looking for.
- Classifies each view as **hit** or **no-hit** according to hotlist.

Agenda

1. Intro (NC)
2. Cybercrime, Chapter 19.1 (Frederik).
3. Privacy, Chapter 19.3 (NC)
4. GDPR, article 1 (Natalia)
5. Privacy By Design, article 2 (Daniel)
6. ANPR (NC)
7. **(Re-)design of ANPR for daily police work (NC)**

Exercise on ANPR system

With PbD principles in mind, design a system using these ANPR installations (stationary and/or on police cars) to achieve either both or one of the two official goals

1. Hits
   Catch stolen and other wanted cars from the hotlist
2. No-Hits
   Catch all plate numbers (not on the hotlist) during targeted police investigations limited in space and time for later search operations within 30 days maximum

Evaluate pros and cons for your proposed solutions wrt legal outcome and privacy protection.

Learning outcome

- What is privacy?
- Why is it a requirement?
- How can we achieve it?

Exam themes/questions:

- What is GDPR and how should it be implemented in praxis?
- Show how Privacy can influence the design of an IT system

Additional knowledge not covered here, but part of the big picture:

- PrivacyByDesign (PbD), as defined by Ann Cavoukian, and Privacy Impact Assessment (PIA) is covered in BUITA class ITS1 (+ITS2)