Legal Definitions of Privacy

Doaa ABU ELYOUNES

Technicalities

The raising hand functionality will be handled through a dedicated website

1) Go to: iraisemyhand.com

2) Enter channel name: **RML2023**

3) Enter your name, and join

Keep the website running in the background and simply press on the raise hand icon any time you have a question/reaction.

Different aspects of privacy

What does privacy protect us from and what is it exactly that we want to keep private?

Additional aspects of privacy

- Privacy of the person/ the body
- Privacy of behavior and action/ thoughts
- Privacy of communication
- Informational privacy/ data
- Privacy of identity/ anonymity
- Privacy in location/ the right not to be tracked
- Privacy in territory/ home and personal belonging

The difference between privacy and data protection

- Two separate rights
- Privacy is internationally recognized as a human right while data protection is not.
- Privacy: dignity, autonomy, right to private life, right to be left alone, right to be free from intrusion by the state.
- Data protection: protecting the information related to an identifiable living person, such as name, photo, date of birth, etc.
- Data protection aims to ensure faire processing, collection, use and storage of data.

The right to privacy in international documents

Article 12 to the Universal Declaration of Human Rights:

“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.”

Key differences between perceptions of privacy in the EU and the US

- In Europe, the notion of privacy can be linked to the second world war, where the Nazi regime used highly sensitive personal data from the population registers
- This led to the development of very strong and protective privacy laws and data protection laws
- In the U.S. the believe is that data tracking can lead to more good than harm, benefits in the form of personalized recommendations and discounted products
- In the U.S. the perception is that collecting and analyzing personal data gives American companies competitive commercial advantage in developing new and innovative products
- In Europe privacy is a human right, in the US it is a liberty
- In the US the approach to consent is opt out, while in Europe it is opt in

The evolution of privacy rights in the U.S.

- The Fourth Amendment to the U.S. Constitution, protection against unreasonable searches and seizures, balance between the right of individuals from intrusion, and the public interest
- No search without a warrant, and warrant requires a probable cause
- Article from 1890 by Samuel Warren and Judge Louis Brandeis
- Right to Privacy, mainly the right to be left alone
- The protected acts are as follows: intrusion into private affairs, public disclosure of embarrassing facts, false publicity; and appropriation of name.
- Third party doctrine, no reasonable expectation of privacy information was given voluntarily to third party

The evolution of privacy law in the U.S.- U.S. v. Jones

- The government obtained a search warrant to be installed on Jones's car
- Based on the tracking data collected from the device, Jones was indited for drug trafficking offenses
- The claim of the government was that Jones could not have had expectation of privacy when he was on public streets, therefore the evidence are admissible
- The question before the supreme court: Does the attachment of a GPS tracking device to a vehicle and subsequent use of that device to monitor the vehicle's movements on public streets constitute a search or seizure within the meaning of the Fourth Amendment?
- Until Jones, the president was taken from Katz v. U.S.
- Whether the investigated person had an expectation of privacy and whether society would view that expectation as reasonable.
- Whether the actions were exposed to the public or if the individual did something to shield himself
- In Jones, the supreme court ruled that this constitute a search because the government entered private property to install the device

The evolution of privacy rights in the US- Carpenter v. United States

- The government obtained more than 5 month of historical cell phone records, and used it for criminal investigations
- Obtaining the data was pursuant to the Stored Communications Act ("SCA"), which requires reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation"
- The question before the court: whether the seizure of historical cell phone data, obtained from a cell phone provider pursuant to a court order violates the fourth amendment
- What do you think the court decided?

The evolution of privacy law in the U.S. continued

- Sectorial approach to privacy law, industry specific laws enforced by different agencies, these include HIPAA (personally identifiable health information), GLBA (financial information), the Telephone Consumer Protection Act (TCPA) (tele- marketing), the CAN-SPAM Act (spam email), the Computer Fraud and Abuse Act (CFAA) (hacking), and ECPA (electronic communications).
- State privacy laws, particularly California
- Self regulatory guidelines
- Consumer protection laws

Privacy rights in Europe

- **Article 8 to the European Convention on Human Rights ECHR: right to respect for private and family life**

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

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

- **Article 7 to the European Charter of Fundamental Rights ECFR: Respect for private and family life**

"Everyone has the right to respect for his or her private and family life, home and communications."

- **Article 8 ECFR: Protection of personal data**

"(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."

The difference between privacy and data protection

- The information protected according to data protection laws, is the information of any identifiable individual.
- Data protection laws unpack the general privacy expectation, and detail how the identifiable data should be treated.
- Data protection laws are broader and they go beyond the anonymity of individuals, realizing that in some instances data must be collected, but the limitation should be about how it is processed.

The General Data Protection Regulation GDPR- purpose and scope

- To protect individuals' rights and freedoms, particularly the right to the protection of personal data
- Applied to all instances of the automated data processing of individuals, and even some manual processing
- Personal data is any information that which is related to an identified or identifiable natural person directly or indirectly, or by linking pieces of information together

The Principles for data processing- article 5 GDPR

"(1) personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

(d) Accurate and, where necessary, kept up to date

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

(f) Processed in a manner that ensures appropriate security of the personal data

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1"

Lawfulness fairness and transparency 5(a)

"personal data must be 'processed lawfully, fairly and in a transparent manner in relation to the data subject"

- Lawfulness is anchored in article 6, which provides six grounds for lawful processing: The consent of the data subject (6(1)(a))
- Consent is a corner stone, but it is not very easy to achieve
- It has to be freely given, genuine choice
- Positive opt in
- It has to be specific, granular and concise

Planet49 case

- Planet49 is a lottery sight, and in order to participate users were presented with two pre-ticked check boxes, one for third party advertising, and the second allowed Planet49 to set cookies for tracking users behavior online
- The German Federation of Consumer Organizations sued the sight
- The court ruled that pre-ticked check boxes do not comply with consent requirements
- Even if the cookies were not collecting personal data it is not allowed without consent
- Lack of information about the duration of the cookies and whether third party will have access to them constitute unfair processing

Who is responsible for data processing under the GDPR? Facebook v. Fashion ID

- Fashion ID is a German online retailer
- The site embodied the like button of Facebook, so customers can like articles and post them on social network
- The plugin meant that all individuals who visited Fashion ID had their IP address and browser string transmitted to Facebook, even if they do not have an account
- The plaintiffs claim that the transmission of personal data occurred without consent
- What would be the responsibility of each party?

Lawfulness continued

- *The necessity of the performance of a contract (6(1)(b)),*
- *The necessity to comply with a legal obligation on the controller (6(1)(c)),*
- *The necessity to protect the vital interests of the data subject (6(1)(d)),*
- *The necessity to perform a task carried out in the public interest or the exercise of official authority (6(1)(e)),*
- *Necessity in the legitimate interest of the controller or another third party (6(1)(f))*

- Necessity is a key concept, meaning that the question should be asked if the controller can reasonably achieve the same purpose with less intrusive means
- Legitimate interest, 6(f) is commonly used, example prevention of fraud

Fairness

- The data should be handled in a away that people would reasonably expect it
- No adverse impact how the data collection effect the interest of the people
- Fair treatment in accessing data rights
- Ethical processing of data, value sensible design

Transparency

- Specific requirements in articles 13-14 GDPR
- The right to be informed: the purpose for the collection and processing, length of retention, and who it will be shared with
- The information should be given in plane language
- Information should be given about the data controller and data protection officer
- Information about the right to access the data, to erase it, to object to the collection, and the right to data portability

Purpose limitation 5(b)

“Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”

- Specified, explicit and legitimate purpose
- The purpose has to be consistent and cannot be changed without proper notice
- For example, using “safety” as a general purpose is not sufficient for the instalment of surveillance camera, every instalment requires a clearer purpose

Data minimization 5(c)

“Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”

- Closely related to the purpose and to the way processing is done to achieve this purpose
- Excessive access to data is not allowed
- The CJEU clarified that video surveillance for example could comply with this principle if the camera blocks or obscure images taken in areas where surveillance is unnecessary

Accuracy 5(d)

"personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay"

- Correct representation of the person at the most diverse levels and in diverse contexts
- Accuracy should also be applied to forecasts, correlations and predictions
- A person has the right to ask for correcting incomplete data

Storage limitation 5(e

“personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”

- The storage period must be defined internally before processing begin
- Anchors the principle of temporariness
- The data controller must proactively delete the data once the purpose is fulfilled, without waiting a request from the data subject
- There should be also a time stamp for a periodic review if the retention is still necessary
- Data can be kept if it is anonymized

Integrity and confidentiality 5(f)

“Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures”

- Technical and organizational measures that ensure security such as encryption
- Requirement to notify the data subject about any data bridg
- Requirement to conduct risk assessment
- Impact assessment

Accountability article 5(2)

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1”

- Keeping record of processing activities
- Adequate documentation on what personal data is processed
- Data protection impact assessment DPI particularly for high risk data processing activities such as tracking people’s location or behavior, or monitoring a publicly accessible place on a large scale

Prohibition on fully automated decision making- article 22

"(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) Paragraph 1 shall not apply if the decision is necessary for entering into, or performance of, a contract between the data subject and a data controller;

is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

is based on the data subject's explicit consent."

Profiling article 4(4) *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."*

Automated decision making continued

- Profiling is defined as applying to a particular individual the profile of the group they can belong to through data collected on them
- Individual profiling- targeting specific person
- Group profiling- a set of people who share similar characteristics
- Distributed and non distributed profiling
- Possible clash between art 22 and transparency requirements in arts 13-14

Automated decision making continued

- What does “solely automated” mean?
- Debate in the literature if it is a full prohibition on ADM or the right to object to it
- What kind of human intervention makes a reasoning not solely automated?
- Legal effects or similarly significant effects
- A German court asked the ECJ to rule whether the activity of credit agencies to create credit score and transmit them to third parties like banks is legal
- How do you think this provision should be interpreted?

https://digi-con.org/is-credit-scoring-an-automated-decision-the-opinion-of-the-ag-pikamae-in-the-case-c-634-21/

Privacy by design

- “appropriate technical and organisational measures, such as pseudonymization”- article 25 GDPR
- Data protection certification mechanisms and data protection seals and marks
- Technical measures ensuring that by default, only personal data which are necessary is processed
- Technical tools allowing data subjects to monitor the data
- User authentication
- A lot of uncertainty as for what does privacy by design mean from a technical perspective

Case study: Data Protection Laws and Facial Recognition

Article 9 GDPR- processing of special categories of personal data

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric ***data*** *for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation* ***shall be prohibited****."*

There are ten exceptions to this rule, including consent, and "substantial public interest".

Article 4(14) GDPR

“biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the ***unique identification of that natural person****, such as* ***facial images*** *or dactyloscopy data”*

What is facial recognition?

- “probabilistic software application that can automatically recognize a person based on its facial attributes in order to authenticate or identify them” (CNIL, 2019)
- Not every technology that uses image processing is facial recognition
- Facial recognition is used for many tasks
- Two main ways to use facial recognition: authentication and remote identification
- What are the pros and cons of the technology?

The benefits of the technology

- Enhanced security
- Faster processing
- Reducing fraud
- Improving computer vision recognition

The risks associated with the technology

- A person cannot be dissociated from the data
- The information is contactless, thus it can be processed without ones knowledge
- Unprecedented surveillance potential
- The technology is fallible

The view of the European Commission

- The European Commission considered a moratorium on facial recognition.
- The EC white paper on AI distinguish between remote biometric identification and biometric authentication.
- The European Data Protection Supervisor (EDPS) released a position saying that automated recognition technologies in public spaces should be temporarily banned.
- It remains an open question whether facial recognition will be band under the EU AI Act

The situation in the United States

- There is no single, comprehensive federal law regulating the collection and use of biometric data.
- Public/ private distinction in privacy law.
- Microsoft, Amazon, and IBM put a one year moratorium on selling facial recognition technology to law enforcement.
- Proposed federal law that seeks to limit the use of facial recognition and other biometric surveillance technology by federal law enforcement agencies.

State laws

- California, New Hampshire, and Oregon prohibit law enforcement from using facial recognition and other biometric tracking technology in body cameras.
- Washington, Illinois, and Texas have biometric privacy laws
- The Illinois law permits individuals to sue over the collection and use of biometric data.
- In a settlement over a big class action lawsuit, Facebook was required to pay 650 million dollars.

City level laws

- San-Francisco, Oakland, California, and Somerville, Massachusetts, already have banned the use of facial recognition technology by city agencies.
- In Detroit facial recognition can be used only in connection with investigation of violent crimes and home invasions (and not in real time).
- In Portland Oregon, the use of facial recognition is prohibited not just in city agencies but also in private entities and places of public accommodation.

Is the use of facial recognition legal in the following example?

An app that compares a photo or video taken in real time to a photograph stored in the id card of a person for the purpose of authentication before using online administrative services or accessing certain public places.

According to the French data protection authority CNIL, yes

- Alicem system
- Experimental mode given three conditions:
  - Draw some redlines
  - Put respect for people at the heart of the approach
  - Adopt a genuinely experimental approach

Is the use of facial recognition legal in the following example?

- A public school tracked the attendance of students by identifying each student's face when they entered the classroom.
- The school compared the captured image with a previously uploaded photo of the student and linked the image with the student's full name.
- The school got explicit consent from the parents

According to the Swedish Data Protection Authority, no

- The school got fined with €20,000
- Personal data was processed more extensively than needed for the purpose,
- Less intrusive means were available
- Consent did not matter because of power imbalance
- Data protection impact assessment was not conducted

Thank you