Recent CJEU case law related to privacy of electronic communications data

Laura Drechsler, PhD researcher at Brussels Privacy Hub and LSTS (FWO aspirant) at the VUB, Brussels
Confidentiality of communication (data) is an old legal principle
What are communication data?

Content data: the content of communication (e.g. content of a letter, an e-mail, a phone conversation, a text message...)

Meta-data:
- Traffic data: ‘traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof’ (Art. 2(b) EPD)
- Location data: ‘location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service’ (Art. 2(c) EPD)

Traditionally content data were considered more revealing than meta-data. This might have changed with new technologies.

Content data and meta-data are often personal data but not always.
What is the legal framework for communication data in the EU?

**EU primary law**
- Privacy (Article 7 CFR)
- Personal data protection (Article 8 CFR)

**EU secondary law**
- General Data Protection Regulation (Regulation 2016/679)

**National law**
- National (communication) data retention laws
- National laws regulating access by public authorities to communication data
Overview

• Theme 1: Data retention obligations and access to retained data by public authorities

  • Joined Cases C-293/12 and C-592/12, Digital Rights Ireland (2014) (Grand Chamber)
  • Joined Cases C-203/15 and C-698/15, Tele2 (2016) (Grand Chamber)
  • Case C-207/16, Ministerio Fiscal (2018) (Grand Chamber)
  • Joined Cases C-511/18 and C-512/18, La Quadrature du Net and Others (2020) (Opinion of Advocate General); Case C-520/18, Ordre des barreaux francophones et germanophone and Others (2020) (Opinion of Advocate General); Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs (2020) (Opinion of Advocate General)
  • Case C-746/18, H.K. v Prokuratuur (2020) (Opinion of Advocate General)

• Theme 2: Access to communication data by Non-EU public authorities

  • Case C-362/14, Schrems (2015) (Grand Chamber)
  • Case C-311/18, Schrems II (2020) (Grand Chamber)
  • ECtHR, Big Brother Watch v UK (2018)
Theme 1: Data retention obligations and access to retained data by public authorities
Joined Cases C-293/12 and C-592/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others and Kärntner Landesregierung, Michael Seitlinger and others, judgment of 8 April 2014 (Grand Chamber) (ECLI:EU:C:2014:238)
Joined Cases C-293/12 and C-592/12, Digital Rights Ireland – Facts and Question

**Facts:** Legal challenges based on EU fundamental rights (privacy and data protection) against the Data Retention Directive in Ireland and in Austria.

**Question:** Is the EU Data Retention Directive compatible with EU fundamental rights (privacy, personal data protection and freedom of expression)?
Joined Cases C-293/12 and C-592/12, *Digital Rights Ireland* – Key findings

The type and amount of meta-data collected allowed for ‘very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained’ (para. 27).

Such precise conclusions pose an interference with the fundamental rights of privacy and personal data protection.

The act of retaining data and the act of accessing that data are two different interferences (paras. 34-36).

Interferences with EU fundamental rights can be justified if they are based on law, serve an objective of general interest, do not breach the essence of a fundamental right and are necessary and proportionate (Article 52(1) Charter).

Crucial aspect was whether the retention was strictly proportional considering its wide scope, lack of link between data and concrete crimes, lack of limits related to crime, lack of safeguards for access by public authorities.
For data retention there needs to be a link between data retained and serious crime and it cannot be general retention (paras. 56-58).

For access by public authorities, three safeguards need to be included: access can only be for serious crime, there needs to be prior review of any access by a court or independent body after a reasoned request, data needs to be stored in Europe for effective control of the data protection authorities (paras. 60-68).
Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, judgment of 21 December 2016 (Grand Chamber) (ECLI:EU:C:2016:970)
 Joined Cases C-203/15 and C-698/15, *Tele2 – Facts and Question*

**Facts:** Legal challenges based on EU fundamental rights (privacy and data protection) against the national data retention rules for telecommunication providers and law enforcement authorities in Sweden and the UK.

**Question:** How does *Digital Rights Ireland* apply to national rules requiring retention of data by telecommunication providers and/or access to telecommunication data by law enforcement?
Joined Cases C-203/15 and C-698/15, Tele2 – Key findings

National laws on retention of communication data and/or its access by public authorities are an exception to the principles of the e-Privacy Directive.

Exceptions are regulated in Article 15(1) e-Privacy Directive.

The retention and access to communication data as an exception to the e-Privacy Directive are an interference with the fundamental rights of privacy, personal data protection and freedom of expression (para. 92).

The assessment of Article 52(1) Charter has to be applied for these interferences.

Article 15(1) e-Privacy Directive lists exhaustively the objectives of general interest capable of justifying the interference.
Joined Cases C-203/15 and C-698/15, Tele2 – Proportionality

National retention laws:

• Profiling of individuals is a serious interference with the fundamental rights of privacy and personal data protection which can only be justified for the fight against serious crime (paras. 101-102).

• Retention of communication data needs to be targeted towards the crime (link to crime, limited to certain persons/areas, based on objective evidence) (paras. 106-112).

National access laws:

• Access to data can only be authorised for fighting serious crime (para. 119).

• Required safeguards are prior review after reasoned request, retention of data in the EU with high standards of data security and (new) the concerned data subject needs to be notified as soon as this does not endanger investigation (paras. 120-123).
Case C-207/16, Ministerio Fiscal, judgment of 2 October 2018 (Grand Chamber) (ECLI:EU:C:2018:788)
Case C-207/16, Ministerio Fiscal – Facts and Question

**Facts:** Spanish court denied access for law enforcement to limited cell phone data in a case concerning a stolen mobile phone as it did not consider mobile phone theft a serious crime.

**Question:** How serious does a crime need to be to justify access by law enforcement authorities to communication data?
Case C-207/16, *Ministerio Fiscal* – Key findings

Case concerns only the national law governing access by law enforcement to which the e-Privacy Directive is applicable via Article 15(1) EPD.

Access by a law enforcement authority to communication data is always an interference with the fundamental rights of privacy and personal data protection (para. 51).

The objectives for justifying such interferences are exhaustively listed in Article 15(1) e-Privacy Directive and include the fighting of crime.

Fighting of crime is not limited to serious crime in the e-Privacy Directive (para. 53).
Case C-207/16, *Ministerio Fiscal* – Serious interference needs serious crime

Seriousness of interference must be *proportionate* to seriousness of crime (para. 55).

Seriousness of crime is determined by *amount* of data requested and *period* involved (para. 59).

Key question is whether or not it is possible to draw *precise conclusions* about an individual (para. 60).
Joined Cases C-511/18 and C-512/18, *La Quadrature du Net and Others* (pending) (ECLI:EU:C:2020:6)
Case C-520/18, *Ordre des barreaux francophones et germanophone and Others* (pending) (ECLI:EU:C:2020:7)
Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (pending) (ECLI:EU:C:2020:5)
Joined Cases C-511/18 and C-512/18, La Quadrature du Net; Case C-520/18, Ordre des barreaux francophones et Germanophone; Case C-623/17, Privacy International – Facts and Questions

**Facts:** Cases brought in France, Belgium and the UK against national laws for retention and access to communication data.

**Questions:**

- Are the national retention and access laws in line with the CJEU case law (Digital Rights Ireland, Tele2 and Ministerio Fiscal)? (all)
- Can problems in the law for data retention be outbalanced by remedies against access by law enforcement? (France)
- Can national retention laws be temporary in force even if against EU law? (Belgium)
- Does the EPD also apply to laws regulating access by intelligence agencies? (UK)
Joined Cases C-511/18 and C-512/18, La Quadrature du Net; Case C-520/18, Ordre des barreaux francophones et Germanophone; Case C-623/17, Privacy International – Opinion of Advocate General Campos Sánchez-Bordona (15 January 2020)

All three data retention laws are not targeted enough and thus disproportionate.

As the interference of retention is different than that of access, each has to be judged separately and they cannot outbalance each other.

National laws not in line with EU law could in this case potentially be temporary valid until new rules are adopted for interests of national security.

The e-Privacy Directive applies via Article 15(1) also to laws regulating access to communication data for intelligence services.
Case C-746/18, *H.K. v Prokuratuur* (pending) (ECLI:EU:C:2020:18)
Case C-746/18, H.K. v Prokuratuur – Facts and Questions

Facts: Estonian police used access to communication data to convict a man to two year of prison for low-value crimes. Authorisation for access was given by the Estonian public prosecutor (Prokuratuur).

Questions:
• How to assess seriousness of an interference into fundamental rights?
• Is a public prosecutor independent enough to provide prior review of access to communication data?
Case C-746/18, H.K. v Prokuratuur – Opinion of Advocate General Pitruzzella (21 January 2020)

Criteria for assessing the seriousness of an interference created by access to communication data are: amount of data, type of data, duration of access and overall preciseness of the conclusions about the private lives of individuals concerned.

Prior review of access by public authorities by a court or independent authority is a minimum safeguard that needs to be included in any regulation.

An independent authority has to be functionally independent and impartial.
Theme 2: Access to communication data by Non-EU public authorities
Case C-362/14, Maximillian Schrems v Data Protection Commissioner, judgment of 6 October 2015 (Grand Chamber) (ECLI:EU:C:2015:650)
Case C-362/14, Schrems – Facts and Question

Facts: Austrian activist Maxmillian Schrems questions the validity of the Safe Harbour Agreement used by Facebook to transfer his data to the US in light of EU fundamental rights, because of access by US public authorities to communication data in the US as revealed by Edward Snowdon.

Question: Does the adequacy decision for the US (Safe Harbour Agreement) adequately protect EU communication data?
Case C-362/14, Schrems – Key findings

To obtain an adequacy decision, a third country must have an ‘essentially equivalent level’ of protection of fundamental rights than the EU achieves with its secondary data protection law and the Charter (para. 73).

For its assessment, the Commission must consider domestic law, international commitments and practice (para. 75).

The Commission has limited discretion in its assessment due to the fundamental rights involved (para. 78).
Case C-362/14, Schrems – Proportionality

Safe Harbour Agreement:
• Safe Harbour Agreement enables an interference into EU fundamental rights (para. 87).
• Due to wide exceptions from its obligation, the Safe Harbour Agreement does not limit this interference to what is strictly necessary (para. 88).
• Commission is required to reason in an adequacy decision on the basis of what findings it finds a foreign legal system adequate (paras. 96-97).

Access by US public authorities:
• Rules for access by US public authorities to EU communication data need to be proportionate and there needs to be a link between access and a recognised objective (paras. 91-93).
• Rules allowing generalised access to EU communication data without limits violate the essence of privacy (para. 94).
• Rules not giving an effective judicial remedy in case of access by public authorities to achieve access, rectification or erasure of data violate the essence of effective judicial protection (para. 95).
Case C-311/18, Data Protection Commissioner v Facebook Ireland, Maximilian Schrems (‘Schrems II’), judgment of 16 July 2020 (Grand Chamber) (ECLI:EU:C:2020:559)
Case C-311/18, Schrems II – Facts and Questions

**Facts:** Austrian activist Maxmillian Schrems questions the validity of the Standard Contractual Clauses used by Facebook in light of EU fundamental rights, because of access by US public authorities to communication data in the US as revealed by Edward Snowdon. He also questions the adequacy finding by the Commission made in the Privacy Shield.

**Questions:**
- Do Standard Contractual clauses adequately protect EU communication data?
- Does the Privacy Shield (new US adequacy decision) adequately protect EU communication data?
Case C-311/18, Schrems II – Key Findings

All transfer instruments (adequacy decisions, standard contractual clauses, binding corporate rules...) have to ensure that the protection of fundamental rights in a third country is essentially equivalent to that of the EU achieved via GDPR and Charter (para. 92).

A controller using standard contractual clauses has to assess whether they offer sufficient protection from access by third country public authorities (para. 104) before any transfer (para. 142).

In some cases, standard contractual clauses might need to be supplemented to achieve essentially equivalent protection (paras. 127-132).

If controllers cannot guarantee essentially equivalent level of protection, they must not transfer data (para. 135).
Case C-311/18, Schrems II – Proportionality

**Privacy Shield:**
• A broad possibilities for exemption from the Privacy Shield obligation leads to the Privacy Shield enabling interferences with EU fundamental rights (para. 165).
• Assessment of Article 52(1) CFR applicable (paras. 175-176).

**Access by US public authorities:**
• Scope of law regulating access needs to be clear and precise with minimum safeguards for data subjects (para. 178).
• Data subjects need to have an effective remedy enabling them to gain access, rectification or erasure of their personal data with US public authorities (para. 181).
• US Ombudsperson not sufficiently independent for counting towards an effective remedy (para. 195).
Big Brother Watch and Others v the United Kingdom, Appl. Nos. 58170/13, 62322/14 and 24960/15, judgment of 13 September 2018 (currently being appealed)
Big Brother Watch and Others (ECtHR) – Facts and Question

Facts: UK human rights organisations complain about UK intelligence laws, that allow UK intelligence agencies wide-spread access to communication data and permit its sharing with foreign intelligence agencies of the Five Eyes Arrangement.

Question:
• Are the UK surveillance laws compatible with the right to private life, freedom of expression and fair trial of the ECHR?
Big Brother Watch and Others (ECtHR) – Key findings

Laws authorising surveillance measures needs to be of a certain quality and foreseeable.

Surveillance measures need to be targeted.

The protection of Article 8 ECHR also applies to the sharing of data with foreign intelligence agencies.
Common themes, differences and open questions
Common themes and differences

**Common themes:**

- Both strings of case law separate different interferences (retention/access or transfer/access) into EU fundamental rights.
- The assessment of Article 52(1) CFR is key for both strings of case law (especially proportionality considerations).

**Differences:**

- CJEU careful to always separate the different interferences in the Theme 1 case law, whereas they are very intertwined in Theme 2.
- Individual remedies seem to play a role for Theme 2 case law only *ex post*, whereas Theme 1 introduces also *ex ante* options (notification).
Open questions

How far can EU law regulate national intelligence operations?

How can national legislators target their retention laws?

How can controllers assess access to transferred data in a third country by public authorities? How can they supplement protection?

How do these safeguards apply in the context of voluntary data sharing between law enforcement and telecommunication providers?
Thank you for your attention!

Contact: laura.drechsler@vub.be