Mass collection of data: failing typologies

van Eijk, N.A.N.M.

Published in:
Human Rights Challenges in the Digital Age: Judicial Perspectives

Citation for published version (APA):
The digital space is a powerful enabler for more inclusive democratic discourse, participation and policy-making. At the same time, digitisation comes with new challenges. The abundance of data in the online space and powerful algorithm-based technologies pose serious risks to privacy, as well as to other interrelated human rights. The trans-border nature of the Internet itself presents significant legislative and judicial challenges for existing legal and institutional frameworks.

This book follows on from the June 2019 seminar paying tribute to the outstanding contribution of Lawrence Early, Juricconsult of the European Court of Human Rights, as he was about to retire. The seminar brought together members of the judiciary and prominent legal practitioners and academics, as well as representatives of European institutions and non-governmental organisations. Speakers from different legal systems and jurisdictions exchanged views on the ways to address the complexity that protection of human rights online presents for the judiciary. The seminar focused on three major subjects: judicial protection of freedom of expression and the right to privacy in the digital environment; the concept of jurisdiction in the World Wide Web; and the implications of Big Data.

Given the breadth and significance of the issues arising in this complex, technical and fast-evolving area, the publication of these keynote contributions will undoubtedly inform further reflection on these matters by judges, legislators, experts and, perhaps most importantly, the general public.
HUMAN RIGHTS
CHALLENGES IN
THE DIGITAL AGE:
JUDICIAL
PERSPECTIVES

In honour of Lawrence Early

Sir Nicolas Bratza
Christos Giakoumopoulos
Dirk Voorhoof
Christopher Docksey
John F Larkin
Síofra O’Leary
Bertrand de la Chapelle
Faiza Patel
Nico van Eijk
Tim Eicke
Lorna McGregor
Robert Spano
Arto Kosonen
Mia Spolander
This book follows on from a seminar which took place on 28 June 2019 in Strasbourg to honour the outstanding achievements of Lawrence Early, Jurisconsult of the European Court of Human Rights, on the occasion of his retirement. Most of the contributions are expanded versions of panel interventions made during the event. The seminar was organised by the European Court of Human Rights in conjunction with the Directorate General Human Rights and Rule of Law (Council of Europe).

Editor-in-Chief
Michael O’Boyle

Former Deputy Registrar of the European Court of Human Rights

The Editor-in-Chief would like to thank all of the contributors for the sterling efforts that they made to enable this book to be published so soon after the seminar. He would also like to thank the sponsors for their enthusiastic support.

Finally, he would like to thank the Directorate of the Jurisconsult and in particular Leif Berg, Head of its Case-Law Information and Publications Division, his assistant Mireille Moegling and editors Rebecca Bastier, Ioulia Iankova and Jane Swift for their invaluable assistance.

Organising Committee for the seminar
Anna Austin
Leif Berg
Elena Brodeala
Olga Chernishova
Gail Fitzpatrick
Rodica Gonta
Carmen Morte-Gomez
Stefano Piedimonte Bodini

Sponsors
Ministry for Foreign Affairs of Finland
Directorate General Human Rights and Rule of Law (Council of Europe)
Lawrence Early, former Jurisconsult of the European Court of Human Rights
# Table of Contents

Preface  
SIR NICOLAS BRATZA QC, former President of the European Court of Human Rights  

PART 1 — JUDICIAL PROTECTION OF FREEDOM OF EXPRESSION AND THE RIGHT TO PRIVACY IN THE DIGITAL ENVIRONMENT

Opening remarks  
CHRISTOS GIAKOUMOPOULOS, Director General, Directorate General Human Rights and Rule of Law, Council of Europe

Same standards, different tools? The ECtHR and the protection and limitations of freedom of expression in the digital environment  
DIRK VOORHOOF, Human Rights Centre, Ghent University and Legal Human Academy

The EU approach to the protection of rights in the digital environment: today and tomorrow – State obligations and responsibilities of private parties – GDPR rules on data protection, and what to expect from the upcoming ePrivacy regulation  
CHRISTOPHER DOCKSEY, Honorary Director-General, European Data Protection Supervisor

Strasbourg or Luxembourg: a right to truth or suppressio veri?  
JOHN F LARKIN QC, Attorney General for Northern Ireland

PART 2 — ISSUES OF JURISDICTION

Data protection and privacy questions in the digital age: whither jurisdiction and the ECHR?  
SÍOFRA O’LEARY, Judge, European Court of Human Rights
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Author(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Territoriality and the cross-border Internet: three exemplary challenges</strong></td>
<td>BERTRAND DE LA CHAPELLE, Executive Director, Internet &amp; Jurisdiction Policy Network</td>
<td>123</td>
</tr>
<tr>
<td></td>
<td><strong>Judicial safeguards against transnational surveillance and jurisdiction issues: the US point of view</strong></td>
<td>FAIZA PATEL, Co-Director of the Liberty and National Security Program at the Brennan Center, New York University Law School</td>
<td>139</td>
</tr>
<tr>
<td><strong>PART 3 — BIG DATA, BIG LEGAL QUESTIONS</strong></td>
<td><strong>Mass collection of data: failing typologies</strong></td>
<td>NICO VAN EIJK, Director of the Institute for Information Law (IViR), University of Amsterdam</td>
<td>167</td>
</tr>
<tr>
<td></td>
<td><strong>Big Data and the ECtHR: the acquisition, use and disposal of data by private Internet intermediaries and the case law of the Strasbourg Court</strong></td>
<td>TIM EICKE, Judge, European Court of Human Rights</td>
<td>173</td>
</tr>
<tr>
<td></td>
<td><strong>The role of courts in addressing the human rights implications of new and emerging technologies</strong></td>
<td>LORNA MCGREGOR, Professor, University of Essex Law School</td>
<td>183</td>
</tr>
<tr>
<td><strong>PART 4 — CONCLUDING WORDS</strong></td>
<td><strong>Summary of the issues discussed during the seminar: an aerial view</strong></td>
<td>JUDGE ROBERT SPANO, Vice-President of the European Court of Human Rights</td>
<td>201</td>
</tr>
<tr>
<td></td>
<td><strong>Postface</strong></td>
<td>ARTO KOSONEN, Agent of the government of Finland before the ECtHR 2001-16, co-Agent 1992-2000</td>
<td>211</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MIA SPOLANDER, Deputy to the Permanent Representative of Finland to the Council of Europe</td>
<td>211</td>
</tr>
<tr>
<td></td>
<td><strong>Finding and understanding the case law of the European Court of Human Rights</strong></td>
<td></td>
<td>213</td>
</tr>
</tbody>
</table>
Chapter 8

Mass collection of data: failing typologies

Nico van Eijk, Director of the Institute for Information Law (IViR), University of Amsterdam

The legitimation of mass collection of data is an issue inherent to today’s information society. In this short essay I question the validity of existing typologies, while promoting a more functional approach when dealing with Big Data topics.

“BIG DATA”

Often “Big Data” is used to address a phenomenon that both includes the large-scale collection of data and the processing thereof. Technology, in particular the unlimited storage availability and dramatically increased processing power, has made it possible for data to become “big”. However, technology is not the only factor. As often, the assumed innovative aspects of Big Data have contributed to a societal shift towards accepting large scale collection and processing of data. Not so long ago “Big Data” was presented as a way to solve important societal issues, creating a hype. Benefits were outweighing disadvantages and criticism was largely silenced or ridiculed by statements such as: “If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.”

We have now entered a more realistic phase in time. Undoubtedly the Snowden revelations created a turning point on the use of Big Data in the context of national security. The use of data by (other) governmental institutions has shown to have embedded risks for democratic societies. Last but not least, more and more questions are raised about the private sector’s use of data. In particular, the behaviour of social media has become a matter of growing concern.

---

1 This contribution presents some initial ideas as a basis for further reflection and exploration. All websites referred to in this paper were accessed on 5 November 2019.
2 Google CEO Eric Schmidt on CNBC. See <www.youtube.com/watch?v=A6e7wFHzew>.
TYPOLOGY OF DATA

In the traditional approach to Big Data we see two dominating typologies. These typologies are visible in regulation and often used in the public debate. On the one hand a distinction is made between “personal” and “non-personal” data. According to the General Data Protection Regulation (“the GDPR”) of the European Union – but other definitions are quite similar – personal data means “any information relating to an identified or identifiable natural person”. Within the category of personal data the GDPR is stricter about so-called sensitive data. These data include 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 person’s sex life or sexual orientation”.

All the other data – although it represents the vast majority of data – are called “non-personal” data. The European Union has even made this the official definition in a recent Regulation on a framework for the free flow of non-personal data in the European Union: “data means data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679.” The category of non-personal data therefore includes everything from business secrets and market data to newspapers, audiovisual media and games.

A second traditional data-typology seeks to distinguish between “meta data” and “content”. Here the definitions more or less work the other way around. Everything which is not content, is meta data. The new European Electronic Communications Code regulating telecommunications frames the dilemma as follows: “It is necessary to separate the regulation of electronic communications networks and services from the regulation of content. Therefore, this Directive does not cover the content of services delivered over electronic communications networks using electronic communications services,

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119. In this position paper we will use references to EU-regulation while recognising that similar kind of regulation exists within the framework of the Council of Europe.

2 Article 4 § 1 GDPR.

3 Article 9 § 1 GDPR.


such as broadcasting content, financial services and certain information society services, and is without prejudice to measures taken at Union or national level in respect of such services, in accordance with Union law, in order to promote cultural and linguistic diversity and to ensure the defense of media pluralism.\textsuperscript{8} A clear definition of meta-data is difficult to find. In a telecommunications context, it at least includes data such as location data.\textsuperscript{9}

The assumption behind the two typologies is that they can help policy makers and regulators to decide what kind of safeguards have to be put into place. Using “ordinary” personal data is considered to be less harmful/infringing than using sensitive data, and “non-personal data” are assumed to have less relevance from a privacy perspective. The same applies to the difference between content and meta data. Meta data are “just data” where content seems to require more protection because of freedom of expression or other fundamental rights-related considerations.

**TYPOLOGY OF ACTORS**

In many regulatory ecosystems the type of actor is relevant, and often a distinction is made between public and private actors. Special rules exist on the transparency of data held and collected by public stakeholders, such as legislation on access to public documents. On the other hand, general privacy and data protection rules contain exemptions for law enforcement and national security, notwithstanding the fact that neither the European Convention on Human Rights nor the EU Charter of Fundamental Rights contains such an exemption. For example, the GDPR does not apply to law enforcement, and according to the Consolidated Version of the Treaty on European Union national security is outside the competences of the Union.\textsuperscript{10} Only recently, in parallel with the GDPR, a special Directive on data protection and law enforcement came into force.\textsuperscript{11}


\textsuperscript{9} See Directive 2018/1972 (cited above – footnote 17), “caller location information” means, in a public mobile network, the data processed, derived from network infrastructure or handsets, indicating the geographic position of an end-user’s mobile terminal equipment, and, in a public fixed network, the data about the physical address of the network termination point. On this topic: H Fischer, ‘Communications Network Traffic Data: Technical and Legal Aspects’ (2010) <https://pure.tue.nl/ws/files/3125126/689860.pdf>.

\textsuperscript{10} See, for example, Article 4 § 2, Consolidated Version of the Treaty on European Union [2008] OJ C115/18 (“In particular, national security remains the sole responsibility of each Member State”).

\textsuperscript{11} Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent
For private actors general data protection rules, such as the GDPR, are applicable and determine under which conditions data can be processed. For good reasons, governments have no direct role to play when it comes to enforcing these rules, which is emphasised by the fact that independent regulators oversee the use of data processing by private companies.

The difference between public and private is based on several arguments. Governments are in a role where they can suppress individual freedom and therefore have to meet high standards when limiting the rights of their citizens. The same applies to companies collecting and processing data.

**TYPOLOGIES ARE FAILING**

To a large extent, these data- and actor-typologies are failing as criteria for policy making and regulation. The main reason is rapid developments in technology causing a shift in application and impact. Some examples and observations in this regard:

- data that might be of an “innocent” nature – such as the age of a person and the brand of the car this person drives – become less “innocent” if there is a high correlation with the possible political preferences of a person (such as the preference for a particular car brand by a certain age group).\(^\text{12}\) Although – this should be emphasised – there is no causation, it still can be observed as support for a particular political opinion.

- the combination of “non-identifiable” data can result in the identification of a particular person. This seems to be the case when age can be linked to a six-figure postal code.\(^\text{13}\) Other researchers claim 90% of people can be identified from just four datapoints.\(^\text{14}\)

- in law enforcement, meta data have become a central element in criminal investigations, often outweighing content-related information. Mobile networks provide huge amounts of information about the when and where of a mobile phone in terms of its carrier/owner. Being at the place and time of a murder can be more convincing than the content of a phone call.


• private companies collect such vast amounts of data that they know more about you and your behaviour than yourself. And even if this is not the case, via profiling, social media and their advertisers are nudging you and try to influence your behavior. While often aimed at commercial transactions, we should not forget that profiling is also used for other purposes such as political influencing (the “Cambridge Analytica scandal”\textsuperscript{15}).

• the question arises if mass surveillance by private companies is not of a higher impact on the daily lives of citizens when compared by – regulated – mass surveillance via State institutions such as national-security agencies.\textsuperscript{16}

• more importantly, the assumed distinction between private and public collection and use of data has always been blurred and is getting even more blurred due to the fact that public authorities can have access to all private data. This is most obvious in a criminal and national-security context where – if provided with the right warrants – access can be gained to private data. But concerns can also be raised about public-private partnership resulting in the sharing of data.\textsuperscript{17} Again, this public/private sharing of data is nothing new and has always been regulated. It is the awareness of it and the changed context that creates additional questions.

**BACK TO THE FUTURE: FUNCTIONAL APPROACH**

Regulation is in many cases a good way to deal with these examples and dilemmas. However, providing clarity and guidance by narrow and precise definitions that are supposed to reflect the underlying normative framework is not the best option. Big data and its technological challenges are difficult to match with such a traditional approach. Norms need to be embedded in a different system of checks and balances. Emphasis will have to shift towards keeping a normative perspective as a central part of implementation and enforcement. It will allow dealing with technological developments and actor shifts. Technology and actors do not decide on safeguarding norms; it is the norms that direct developments in technology and the behaviour of actors. Such

\textsuperscript{15} [www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-in-to-votes-christopher-wylie].


\textsuperscript{17} Example: [www.wired.com/story/cops-offering-ring-doorbell-cameras-for-information/].
a rebalancing of the system of check and balances with more focus on implementation and enforcement will increase the legitimisation of the legislator. Sharing responsibilities with independent regulators and the judiciary will help to prevent a democratic deficit. Such a deficit occurs when other stakeholders take control over the collection and processing of data in a way that fundamental rights effectively become “privatised”.

A functional approach is not new. It is at the core of the jurisprudence of the European Court of Human Rights. Just a recent “Big Data” example that demonstrates how to deal with the aforementioned distinction between meta data and content: In the Big Brother Watch case, the Court (re)confirmed the importance of focusing on the normative aspects of the case. Judging the relevance of the difference between meta data and content, the Court states it “is not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content” and “In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of commercial patterns, and insight into who a person interacted with”. It is the impact on the freedom of citizens that counts, not the technical nature of the data. This is basically the same reasoning as in the – almost 30-year-old – Autronic case, where it was not the technical classification of a satellite (telecommunications), but its actual use (broadcasting) that was essential. The Grand Chamber will have the final word in the Big Brother Watch case, but it seems not very likely that its decision will be different on the relevance of the distinction between meta data and content. It will be up to the nation States to see such a decision as another argument to further optimise their systems of checks and balances, abandoning static approaches and replacing them with a dynamic and function-driven one. And – although the focus of this contribution was mainly on technology – the same approach is needed concerning the role of the actors. The protection of fundamental rights cannot be altered because of the mere fact that an actor is public or private.

---

18 And other courts, including the Court of Justice of the European Union and national (constitutional) courts.
19 Big Brother Watch and Others v. the United Kingdom, nos. 58170/13 and 2 others, 13 September 2018.