EdpL
EUROPEAN DATA PROTECTION LAW REVIEW

FEATURING:
YOUNG SCHOLARS AWARD 2016

FOREWORDS by Lee A Bygrave and Paul De Hert

ARTICLES

REPORTS

CASE NOTES

THE LEGAL PUBLISHER
lexxion
BERLIN
BRUSSELS

4 2016

EDPL EUROPEAN DATA PROTECTION LAW REVIEW

Call for Papers

The editors of the **European Data Protection Law Review (EDPL)**, a new pan-European publication designed to explore the legal and policy challenges of the EU data protection framework, invite you to contribute to the upcoming issues of our journal.

Content and Form

The **EDPL** provides a practical and intellectual forum to discuss, comment, and review all issues raised by the development and implementation of data protection law and policy in the EU Member States. The journal reports on key legislative developments and addresses relevant legal, regulatory, and administrative challenges in EU Member States and institutions. The **EDPL** will identify and analyse important case law that shapes the interpretation and application of EU law in this field, including decisions by the European Courts, international courts, and higher national courts.

All contributions will be subject to double blind peer-review before acceptance for publication. To guarantee **EDPL**'s high-quality standards, all submissions are required to conform to the author guidelines available at:
www.lexxion.eu/edpl/author-guidelines

Deadlines for Submission

- Issue 1/2017: 1 February 2017 – Special Issue on Big Data
- Issue 2/2017: 1 May 2017 – Special Issue on Smart Applications
- Issue 3/2017: 1 August 2017 – Special Issue on Law Enforcement
- Issue 4/2017: 15 October 2017 - featuring Young Scholars Award

Articles may be submitted after the published deadlines, by arrangement with the editor.

Contact

The editorial team looks forward to discussing your proposals and receiving your submissions. For further enquiries, please contact the

Executive Editor:

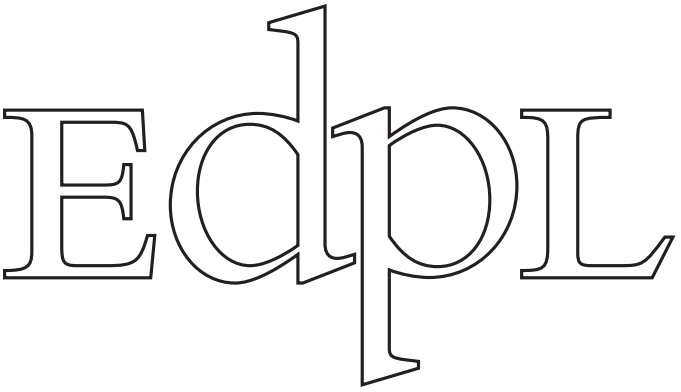
Nelly Stratieva
stratieva@lexxion.de
+49-30-81 45 06-17

4 issues/year · approx. 70 pages/ issue · ISSN 23 64-28 31 · www.lexxion.eu/edpl

THE LEGAL PUBLISHER lexxion BERLIN BRUSSELS

Lexxion Verlagsgesellschaft mbH · Güntzelstraße 63 · 10717 Berlin · Phone +49-30-81 45 06-0
Fax: +49-30-81 45 06-22 · Mail: info@lexxion.de · www.lexxion.eu

Contents



EUROPEAN DATA PROTECTION LAW REVIEW

Publisher
Lexxion Verlagsgesellschaft mbH
Güntzelstraße 63 · 10717 Berlin · Germany
Phone: +49 30/81 45 06-0 · Fax: +49 30/81 45 06-22
www.lexxion.de

Typeset
Automatic typesetting by metiTEC-software
me-ti GmbH, Berlin

EDPL annual subscription rates 2017 (4 issues)*

printed edition only	410,00 €
printed edition + online edition (incl. archive)**	471,00 €
online edition only (incl. archive)**	410,00 €

* Prices include postage and handling. EU Member States: VAT will be added if applicable.
** Single user online access via user name and password.

EDPL is supplied under our terms of sale and supply.
Copies of our terms and conditions are available upon request.
Lexxion Verlagsgesellschaft mbH. VAT Reg.No. DE 209981990.

For further information please contact
info@lexxion.de
Tel.: +49 30/81 45 06-0 · Fax: +49 30/81 45 06-22

Contributions
are welcome and should be submitted according to the EDPL author guidelines. Any such contribution is accepted on the understanding that the author is responsible for the opinions expressed in it. More informations available at www.lexxion.eu/edpl.

Ownership and shareholdings pursuant to Section § 7a I No. 2 and II No. 6 of the Berlin Press Act: Shareholder of Lexxion Verlagsgesellschaft mbH is Dr. Wolfgang Andreae, Publisher, Berlin.

This journal may be cited as [2016] EDPL.

ISSN (Print) 2364-2831 · ISSN (Online) 2364-284X

Reports

This part of the EDPL hosts reports in which our correspondents keep readers abreast of various national data protection developments in Europe, as well as on the most recent questions in different privacy policy areas. The Reports are organised in cooperation with the Institute of European Media Law (EMR) in Saarbrücken (www.emr-sb.de) of which the Reports Editor Mark D. Cole is Director for Academic Affairs. If you are interested in contributing or would like to comment, please contact him at mark.cole@uni.lu.

Introduction

Recent Developments and Overview of the Country and Practitioners' Reports

2016 has been a year with lots of significant developments in the area of data protection law. Foremost, with the entry into force of the General Data Protection Regulation (GDPR), we now have a clear target date for its applicability and obviously this new forthcoming era is creating a lot of activity: on the side of legislators in the Member States, trying to find the right way to fill the gaps or spaces left by the GDPR; on the side of Data Protection Authorities (DPAs), getting ready to implement the new procedures; on the side of consumers and users, understanding the impact some of the novelties will bring; and last but not least, on the side of businesses, and alongside with them, the legal profession, having to amplify their efforts to meet compliance requirements with the GDPR. Unsurprisingly therefore in many of the reports we were able to share with you, the country experts already put the developments into the perspective of the forthcoming Regulation and we will continue to do so increasingly in the coming year when the preparatory activities will unfold even more.

In accordance with the above, in this issue's Reports Section we have an overview in the 'Practitioner's Corner' that deals exactly with the consequences and the need for adaptation the new General Data Protection Regulation will bring for businesses. As regular readers will know, we have introduced the 'Practitioner's Corner' recently in order to give lawyers, DPA members, company legal counsels and others the opportunity to highlight in a condensed manner specific privacy and data protection questions which do not relate to a Member State but are of overarching interest. We are very pleased to have a long-standing practitioner and expert in the field that has already contributed regularly in the past to the academic and practice-oriented debates with numerous publications, to take responsibility for gathering contributions in this section: I would like to welcome *Axel Freiherr von dem Bussche* in this new role! As the author of this edition's Practitioner report he describes together with *Anja Zeiter* the modifications that will be required in data protection management, how the relationship between controllers and processors will change, as well as the new scope of data subjects' rights. The report also explains how informed consent as the central basis for data processing will need to be obtained from the data subject in the future, and how the framework of sanctions will look like. The authors identify transparency as one of the key principles that is enshrined in a series of information and notification obligations throughout the GDPR and conclude that with around 180 opening clauses it will remain to be seen whether this new legislative act can keep the promise of establishing a more uniform data protection regime in the EU.

Before the concluding Practitioner's report this time we have a number of contributions that also go beyond the scope of a national development and present very relevant general aspects of data protection. The focus this time is on a selected topic, which has been analysed in-depth and in a comparative manner by a research group around *Indra Spiecker gen. Döhmann* and *Olivia Tambou*. The report, com-

prehensively covering the situation regarding the regulation of commercial profiling in Germany, France, UK, US, Brazil and Australia, and therefore longer than our usual single-country reports, presents a major part of the outcome of a seminar held at the University of Paris Dauphine in June of this year. The authors note considerable differences in the regulatory approaches to this subject that lawmakers in the countries included in the survey have taken. They highlight what might be perceived as a striking fact: that the United States, up to now not believed to be at the forefront of limiting the use of personal data across the board, have begun to establish rather clear-cut rules governing the use of this kind of information for profiling purposes. On the other hand, the comparative view on legislation in Germany, France and the UK has demonstrated, once again, that harmonisation of national data protection laws by the Directive 95/46/EC has remained limited. Chances are that the future applicability of the GDPR will bring an important change in this regard as it addresses profiling specifically. However the upcoming Brexit might rather have a scattering effect. The report concludes that also other legal fields, such as consumer protection and telecommunications law, which provide rules applicable to profiling, too, will need to be considered when trying to strike a balance between the commercial interests of those applying this still new business practice and the personality rights of data subjects.

The ethical questions of personal data processing are in the centre of a report by *Charles Raab* and *Roger Clarke* shedding some light on the content and practicality of a UK government draft entitled 'Data Science Ethical Framework'. While the authors welcome the idea of introducing a new framework in this field that goes beyond mere compliance with the laws on data protection, their analysis comes to the conclusion that the draft presented to the public does not achieve this goal as it has severe shortcomings. The authors suggest that the framework had been developed not to solve the ethical issue of what kinds of data processing were to be regarded as having a positive or negative impact, but to serve as a fig leaf at the disposal of public administration to refer to when in need of an authority signing off any type of controversial data processing activity. The report concludes with an appeal to the Cabinet Office to correct these deficiencies swiftly and to come up with a new and more compelling version that is made available to the wider public so as to ensure a broad participation in the further development of the document. Certainly, the topic of Data Ethics will continue to be on the agenda in the UK as well as across the European Union as it is regarded to give an additional layer beyond the purely legal approach to applying data protection rules.

From the perspective of a German data protection authority, *Kristin Benedikt* reports about an interesting investigation into the data protection compliance of 13 smart TV sets that German DPAs have presented to the public in 2015. The author first lays out the outcome of a technical functions survey and identifies the different providers involved in the processing of personal data emanating from the smart TV device as it is operated by the end-user. This setting forms the basis for a legal analysis reviewing the adherence of the actors with the applicable data protection legislative framework. The report concludes by explaining the specific obligations applying to smart TV service providers, including the device manufacturers, HbbTV and app providers, operators of personalised recommendation services and processors acting on behalf of the data controller. This overview shows that even for a specific issue such as the provision and use of smart TV sets a whole range of responsible actors are on the scene and it is necessary to very clearly distinguish the different activities and derived from that responsibilities. In view of the widespread use of smart TVs this report adds an important facet to a previous report in our section on obligations of providers of such services[1].

The final country report by *Jan Tomíšek* provides us with an insight into the way the Czech legislator has dealt with data protection issues in the sector of electronic healthcare (also known as 'eHealth'). Given that health data are among the most sensitive categories of information about an individual, the author stresses the need for strong safeguards and criticises, in particular, the current lack of those in the regulation governing the National Health Information System. The database processing health data on a wide scale for statistical purposes has recently seen some amendments allowing for more data collection and merging, but does not provide for elevated security measures. The author also points to current le-

1 See Sebastian Schweda, 'German Data Protection Authorities Issue Privacy Guidelines for Smart TV Services' (2016) 1 EDPL 108-111.

gal uncertainties with regard to the maintenance of health records, which made it impossible to switch to a system keeping these data in an electronic-only form. A reform of the regime in force, he suggests, is therefore urgently needed, but the recently presented National Strategy for Electronic Healthcare, envisaged to cope with the identified problems, includes some contentious issues that still needs some more debate in his view.

We hope that readers will enjoy the present selection of reports covering a diverse range of country-specific and thematic developments which, as the extensive piece on profiling shows in a particularly telling way, in many cases outreaches European borders and sheds light on developments elsewhere that are relevant for us in Europe. As always, the editors together with the Institute of European Media Law (EMR) welcome any comments you may have or suggestions for future reports at <mark.cole@uni.lu>.

Mark D Cole
Director for Academic Affairs, EMR

Multi-Country

The Regulation of Commercial Profiling – A Comparative Analysis

*Indra Spiecker genannt Döhmann and Olivia Tambou, Paul Bernal, Margaret Hu, Carlos Alberto Molinaro, Elsa Negre, Ingo Wolfgang Sarlet, Laura Schertel Mendes, Normann Witzleb and Florian Yger**

The authors, all data protection experts, discuss the status of the relevant data protection regulatory framework on profiling in the business sector in several countries worldwide, from the constitutional level to some individual regulation including the general attitude towards the topic. The EU perspective is presented on the basis of the present directives as well as the General Data Protection Regulation. The United Kingdom, Germany and France, as three of the largest EU Member States with partly highly differing regulatory approaches represent Member State law. Australia, Brazil and the US regulation exemplify the different integration of data protection standards and different models of approaching profiling in the globalised IT world.**

I. Introduction

In surveys, citizens regularly express significant concern about the gathering of profiling information for commercial and other purposes.[1] This fear of becoming a transparent citizen, of being controlled and potentially manipulated by the state or by companies with superior information, has been a prominent reason for data protection from its very beginnings.[2] Information service providers, on the other hand, have long searched for measures to learn more about the behaviour, preferences and decisions of their clients, customers (and potential clients and customers) and citizens on the basis of collective and group information, in order to create contracts and relationships based on more precise predictions and individual evaluations of risk. The rise of high velocity, high volume and high variety data processing, often referred to as 'Big' or 'Smart' Data, has made these analyses not only more likely, but also more accessible. As a result, profiling has become an every-day measure in evaluating counterparts, both by the state and by private companies.

The conflict between the interests of the individual in preserving their privacy and restricting access

* Indra Spiecker genannt Döhmann, LL.M. (Georgetown), holds the Chair in Public and Administrative Law, Information Law, Environmental Law and Legal Theory at Goethe-University Frankfurt a.M., Germany; Olivia Tambou is Associate Professor at the Université Paris-Dauphine, PSL Research University, Cr2D, France; Paul Bernal is Lecturer in Information Technology, Intellectual Property and Media Law at the University of East Anglia Law School, Great Britain; Margaret Hu serves as Associate Professor of Law, Washington and Lee University School of Law, USA; Carlos Alberto Molinaro is Professor at Pontifical Catholic University of Rio Grande do Sul (PUCRS), Brazil; Elsa Negre is Assistant Professor in Computer Sciences at Université Paris-Dauphine, PSL Research University, CNRS UMR 7243, LAMSADE, Data Science TeamFrance; Ingo Wolfgang Sarlet is Professor at Pontifical Catholic University of Rio Grande do Sul (PUCRS), Brazil; Laura Schertel Mendes serves as Professor at the University of Brasília (UnB) and at the Institute for Public Law of Brasília (IDP), Brazil; Normann Witzleb is Associate Professor and Deputy Director of the Centre for Commercial Law and Regulatory Studies at the Faculty of Law, Monash University, Australia; Florian Yger is Assistant Professor in Computer Sciences at Université Paris-Dauphine, PSL Research University, CNRS UMR 7243, LAMSADE, Data Science Team, France.
We would like to thank the Université Paris-Dauphine for their support to a workshop in June 2016 in which this paper and project were developed. Olivia Tambou also thanks Alexandre Lercher for his contributions on the French law; Indra Spiecker thanks Dirk Muellmann for his contributions on the German law.

** This report is part of an ongoing larger project comparing the legal status of profiling initiated by Olivia Tambou. If you are interested in our working group, please contact Olivia Tambou (<olivia.tambou@dauphine.fr>) or Indra Spiecker (<spiecker@jur.uni-frankfurt.de>).

1 See eg European Commission, *Data Protection Report (Special Eurobarometer 431*, 2015) 39 <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf> accessed 11 November 2016; or Office of the Australian Information Commissioner, *Community Attitudes to Privacy survey* (Research report, 2013) 17 et seq <https://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf> accessed 11 November 2016.

2 Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 55.

to and use of their personal information and the interests of companies and states to know more about their customers and citizens in order to provide more targeted and efficient services call for balanced regulation. However, explicit regulation of profiling does not at present exist within consumer protection law, privacy law or data protection law. And even the new EU General Data Protection Regulation (GDPR), which aims to modernise and standardise the data protection framework across the EU from 2018, contains only limited regulation on profiling.

Profiling can be described as the process of gathering information and personal data, combining this individualised data with other (eg, personal, factual, statistical) data and analysing it through algorithms with the aim of predicting a person's future conditions, decisions or behaviour.[3] These different steps do not all necessarily fall under the scope of data protection laws, as not all of them always process personal data. This is true especially for the intermediate steps of combining or reassembling of data, where the personal data is often merged into grouped information about large numbers of individuals and statistical content. It would therefore be desirable to have a regulation that addresses all relevant steps in profiling. As this, however, is not the case, this article, based on informed computer science input about the technical possibilities and restrictions, aims to identify the legal status quo. We focus on profiling laws of general application; we do not analyse sector-specific regulation such as in banking or credit-rating.[4] As profiling uses information available worldwide and produces results that are of interest everywhere in a globalised world, a national approach or even an EU-wide approach would in general not seem to be sufficient. We have therefore adopted a comparative approach that includes reports from prominent EU Member States (*Germany*, *France* and the *UK*[5]) as well as the *US*, *Brazil* and *Australia*. As most Asian countries, in particular China and India, have little regulation and even less enforcement on data protection to date,[6] a comparative view at this point would not be fruitful. We also exclude the use of profiling by state authorities and non-commercial entities such as political parties. They follow to a great extent, the individual public and administrative legal framework of each individual state.

The paper will first describe how profiling operates and what computer scientists view as the mechanisms and restrictions of profiling (II.). It will then continue with the relevant European framework (III.), concentrating on the expected normative standards of the GDPR. As we will show, the GDPR does not provide for strict guidelines on profiling. Thus, the present interpretations and standards in the EU Member States will be of continuing importance, as they present the starting point also for future EU practice, eg, in the consistency mechanism which requires Member States' data protection authorities to cooperate in order to reach a common decision. We will then look at how the various legal issues raised by profiling are dealt with by the jurisdictions under consideration (IV.). The paper concludes with a look at future prospects (V.).

II. What Is Profiling?

In this section, we explain the concept of profiling as understood by computer science. This overview will consider the data acquisition and analysis processes, and also describe techniques to limit the effects of profiling.

1. Data Acquisition

The data acquisition chain is the set of elements necessary to 'capture' data from its creation (by a user or a machine) to its storage for immediate or future use. We focus on the acquisition of data through user profiles (which can contain a large amount of user information including preferences), cookies (which store user navigation data) and traces (which record activity and user identity).

3 A closer technical description of profiling follows infra II.

4 The specific regulation of profiling in the banking sector and by credit agencies will need to be looked at separately. A major concern here is the use of data from one sector for other purposes than the original one.

5 As neither the form nor the full consequences of Brexit are not currently clear, it must be noted that the UK may sooner or later deviate from EU law, and in particular the EU data protection regime.

6 In the case of India, much data processing involving European citizens is performed on the basis of standard contract clauses assuring European level of data protection.

a. User Profile and Preferences

A user profile is a set of personal data associated with a specific user or a customised desktop environment. A profile[7] therefore refers to the digital representation of a person's identity. Profiles can be constructed through explicit or implicit data collection. Data collection is explicit when the user explicitly provides personal information, for example, classifies a collection of items according to his/her preferences or creates a list of interesting features. In contrast, data collection is implicit[8] when preferences/opinions of the user are induced from the actions of the user, ie what elements were viewed, or by keeping track of the user's navigation (purchases; items where the user has lingered, etc). Note that users tend to have little patience and/or willingness to give information about their preferences, so that the systems have a very incomplete picture of the users' preferences. In order to gain more information, additional user preferences are inferred[9] from the induced/elicited or observed preferences, based on assumptions.[10] [11]

b. Cookies

A cookie[12] is a small text file that is downloaded to a user's device and saved in the web browser when users access a particular website. Cookies allow the storage of user data (such as IP addresses, passwords, items in an online shopping cart) or users' browsing activity (including clicking particular buttons, logging in) in order to facilitate navigation and enable some features. Most modern browsers allow users to decide whether to accept or reject cookies. Users can usually also determine the cookie's expiry.[13] While cookies improve the convenience of web browsing, they have always been controversial because they store information that can potentially be exploited by third parties. This is one of the reasons why the EU regulated the use of cookies in the so-called 'Cookies Directive'.[14]

c. Traces

Like a trace left in the snow, a user leaves a certain number of clues in form of data recorded by the server hosting the visited website. Among them are traces related to the computer such as the IP address, the environment variable (information about the operating system running on the computer, usually useful to adapt the display of a website) and traces related to past searches of a user (on a web search engine). The latter traces can reveal user interests (keywords used), visited websites (links chosen within search results), location (via the IP address) and dates of access. A trace can be used for analysing a user's behaviour (eg, in order to enhance the quality of web navigation on the website or in order to display relevant advertisement).

d. Metadata/Data

Contextual information on collected data is called metadata. Metadata can be thought of as data about data, eg the metadata of an email would consist of the sender, the recipient, the timestamp, the IP addresses etc. By its nature, metadata is often less directly protected (for example, it is created by default by most softwares for text and images) and it can often be easier to collect than the data itself. Metadata are simple but structured data, and lots of information can be deduced from it, eg the width, quality and intensity of someone's personal network could be re-

7 Riddhiman Ghosh and Mohamed E Dekhil, 'Discovering user profiles' (*ACM Digital Library*, Proceedings of the 18th international conference on World wide web (WWW '09), Madrid, Spain, 20-24 April 2009) 1233-1234.

8 Alan Mislove et al, 'You are who you know: inferring user profiles in online social networks' (*ACM Digital Library*, Proceedings of the Third ACM International Conference on Web Search and Data Mining (WSDM '10), New York, USA, 3-6 February 2010) 251-260.

9 Dianne Kelly and Jaime Teevan, 'Implicit Feedback for Inferring User Preference: A Bibliography', *SIGIR Forum* 37, 2 (2003) 18 et seq.

10 Nic Wilson, Anne-Marie George, and Barry O'Sullivan, 'Computation and Complexity of Preference Inference Based on Hierarchical Models' in Qiang Yang and Michael Wooldridge (eds), Proceedings of the 24th International Conference on Artificial Intelligence (IJCAI'15) (AAAI Press 2015) 3271 et seq.

11 Vincent Schickel-Zuber and Boi Faltings, 'Inferring user's preferences using ontologies' in Anthony Cohn (ed), *P*roceedings of the 21st national conference on Artificial intelligence - Volume 2 *(*AAAI'06) (AAAI Press 2006) 1413-1418.

12 David Kristol, 'HTTP Cookies: Standards, privacy, and politics' (November 2001) 1(2) ACM Transactions on Internet Technology 151-198.

13 Eg in France, a cookie has a maximum lifespan of 13 months, see <http://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi> accessed 11 November 2016

14 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337/11.

constructed from the email's metadata. In practice, the metadata can be a rough summary of the data itself and it is difficult to make a clear distinction between data and metadata as the metadata can be deduced from the data.

2. Data Analysis/Mining

Data analysis is a process of preprocessing (cleaning and transforming) data and applying relevant models to them in order to automatically discover useful information and to support decision-making. The following items describe different aspects of information selection and evaluation processes that are used in profiling.

a. Data Mining/Machine Learning

Data mining and machine learning are two interdisciplinary subfields of Artificial Intelligence (AI) at the crossing of several other domains (statistics, applied mathematics and computer science). Those two subfields consist of expressing the data in a mathematical framework. They use a particular vocabulary: data will be referred to as population or individuals. A population is the set of individuals a study is interested in. Every individual is described by the same set of characteristics (known as variables or features). Relationships between individuals, between variables or between individuals and variables are sought in order to model behaviour. The philosophy is to involve the human as little as possible in the creation of a predictive model. Thus, the more data are gathered, the better the algorithms will perform (hence the term 'Big Data'). However, if an algorithm is fed with bad, unreliable, noisy or corrupted data, its prediction will be bad as well.

Data mining consists of discovering and extracting non-trivial patterns and behaviour in large datasets (such as traces). Those discovered patterns are then used as a means of analysis and sometimes for prediction of behaviour and decisions. Machine learning is often described as the field giving to computers the ability to learn without being explicitly programmed. The computer is trained to recognise some behaviour from examples (positives or negatives). It then acquires this ability to understand behaviour or complex situations without having been explicitly programmed with a description of those situations. The difference between the two fields is not always simple. In general, however, data mining mainly focuses on the analysis and exploration while machine learning focuses on decision-making.

b. Recommendations

Users face ever-increasing quantities of information, due to increased calculation and storage capacity,[15] which makes it increasingly difficult to know exactly what information to look for and where. Recommender systems[16] guide users in their exploration of data by a specific form of information filtering, in order to obtain relevant information. Generally, based on certain reference characteristics,[17] the recommendation process aims to predict the 'opinion' a user will have of each item and to recommend items with the best predicted 'opinion'.

3. Technologies Invoked to Limit Profiling

The following techniques describe ways how to limit profiling.

a. Data Minimisation

In the context of profiling, data minimisation means extracting only what is relevant to the task to be solved. The goal must be clearly defined beforehand to help decide the life span of the collected data. Such an approach contradicts the usual approach in machine learning and data mining where in principle more data results in better algorithmic predictions. In practice, a trade-off has to be found to reduce the quantity whilst gathering the relevant data.[18] In terms of privacy, storing less data can be good for the individuals. For companies, there is may be also a tip-

15 A study of the UCLA Berkeley estimates the quantity of information newly created each year at approximately two exabytes per year (1 exabyte = 10^{18} bytes) <http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/> accessed 11 November 2016.

16 Elsa Negre, *Information and Recommender Systems* (Wiley 2016) 7.

17 These characteristics may come eg from the information items themselves (a content-based approach) or the social environment (collaborative filtering) and are based on the user profile, some contextual parameters, the knowledge model, etc.

18 Katrin Borcea-Pfitzmann, Andreas Pfitzmann and Manuela Berg, 'Privacy 3.0 := Data Minimization + User Control + Contextual Integrity' (2011) 53(1) Information Technology 34-40.

ping point where even though more data is accumulated, the algorithms will behave the same, and the profit, generated by using those algorithms, will stay the same while the cost of storing data would rise.

b. Encryption

In cryptography, encryption consists in altering the content of a document to prevent its being understood by anyone without the 'key' to the encryption. This 'key' must be communicated between the parties exchanging the document.

Classically, encrypting a document is depicted as putting a lock on a trunk. Knowledge of how a lock operates is not enough to open it without the key. Similarly, knowing the algorithm used for encrypting a document is not enough to access its content without this key. Just as in practice there are many ways to force a lock or to pick it, there are ways to break encryption.

Encryption is a basic tool for protecting data and preventing access to (and diffusion of) it, which is even more important when a database contains sensitive or personal data that was not anonymised. The access to such a database would make the profiling of any particular user whose data are stored in that database an easy task.[19]

c. Anonymisation/Pseudonymisation

Anonymisation consists of modifying the data content (or structure) to make it very difficult (if not impossible) to identify a particular individual. As opposed to encryption, where the sender and the receiver are supposed to be able to read the message, it is designed to prevent the interpretation of the data by anyone and it is intended not to be reversible. Anonymisation of a dataset is a complex task as the data has to be modified in order to make a given user unidentifiable but without significantly reducing the overall quality of the data. Furthermore, anonymisation should not add too much 'noise' or any harmful artefact to the data.[20] [21]

Pseudonymisation can be viewed as a special case of anonymisation where only the most sensitive parts of the data are replaced by aliases, typically names or addresses. Anonymisation and pseudonymisation ensure that the profile of any given user cannot be recognised.[22]

d. Differential Privacy

Differential privacy lies at the interface between machine learning, anonymisation and cryptography and proposes to modify the data (or its structure) in order to maximise the accuracy of queries from statistical databases and at the same time to minimise the chances of identifying its records. In other words, it is a machine learning efficient anonymisation. Hence, it prevents the access to any particular user's profile while ensuring that relevant statistics can be computed on the data.[23]

III. The European Approach to Profiling

1. Council of Europe Recommendations on Profiling and EU Regulatory Framework

The Council of Europe adopted a set of principles for all forms of personal data processing using profiling techniques in 2010, and recommended to Member States that they should be implemented into domestic law.[24] These recommendations do not form part of the EU regulatory framework on profiling, which consists of regulation on three levels:

- Article 7 (respect for private and family life) and Article 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union,[25] together with Article 16 of the Treaty on

19 Murat Ak et al, 'Efficient broadcast encryption with user profiles' (2010) 180(6) Information Sciences 1060-1072.

20 Marcus Schöller, Thomas Gamer and Christoph P Mayer, 'PktAnon – A Generic Framework for Profile-based Traffic Anonymization' (2008) 31(2) Praxis der Informationsverarbeitung und Kommunikation 76-81.

21 UK ICO, *Anonymisation: managing data protection risk code of practice* (2012) <https://ico.org.uk/media/1061/anonymisation-code.pdf> accessed 11 November 2016.

22 Slaughter and May, 'Personal data, anonymisation and pseudonymisation under the GDPR' (July 2016) <https://www.slaughterandmay.com/media/2535637/personal-data-anonymisation-and-pseudonymisation-under-the-gdpr.pdf> accessed 11 November 2016.

23 Cynthia Dwork and Aaron Roth, 'The Algorithmic Foundations of Differential Privacy' (2014) 9(3-4) Theoretical Computer Science 211-407.

24 Council of Europe, *The protection of individuals with regard to automatic processing of personal data in the context of profiling*, Recommendation CM/Rec (2010)13, 2010.

25 Charter of Fundamental Rights of the European Union [2016] OJ C202/389.

the Functioning of the European Union (TFEU),[26] provide the constitutional framework for the protection of personal data.[27] Additionally, Article 8 of the European Convention on Human Rights (ECHR)[28] also protects the right to respect for one's private and family life.

- On the EU secondary law level, profiling falls presently under the Data Protection Directive (DPD).[29] The so-called 'E-privacy Directive'[30] and the Cookie Directive, currently under review, also contain relevant regulation specifying eg the level of consent and the formal requirements for a telecommunication-based consent.
- On a third level, non-binding sources such as recommendations or opinions, in particular those adopted by the Article 29 Working Party, influence the legal regime covering profiling. This European data protection framework has given Member States ample room to develop their own definitions, rules and interpretations on profiling.

This, however, will change when the new General Data Protection Regulation (GDPR)[31] will come into effect in May 2018. The GDPR will be directly applicable to individuals in all Member States with only a limited number of opening clauses leaving Member States a leeway for own regulation.[32] The following sections will give an overview over the changes in law relevant for profiling.

2. Definition of Profiling in the GDPR

While the DPD is silent on profiling, leaving its definition and regulation largely to the Member States, the GDPR expressly refers to profiling 23 times.[33] Article 4 includes the first definition of profiling in EU Law, which will now be directly and identically applicable in the 28 EU Member States:

> Profiling means 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.

Importantly, this definition refers to automatic processing of personal information for the purposes of evaluation. It includes the automatic processing of personal data only, and therefore does not include the collection and the analysis of anonymous data for the creation of profiles, one of the major steps of profiling. The processing of personal data often appears at the last stage of the inference, when the group profile is applied to an individual person. However, this aspect may be covered by the rules governing automated decisions. Also, the very general definition covers several procedures that were previously treated separately in the Member States, eg scoring.

3. Ban on Decisions Solely Based on Automated Processing: Article 22 GDPR

In Article 15, the DPD provided that individuals should not be subject to a decision based solely on automated processing of data where this decision produces legal effects or similarly significantly affects the data subject. The GDPR retains this princi-

26 Treaty on the Functioning of the European Union (Consolidated version 2016) [2016] OJ C 202/47.

27 The CJEU so far has not distinguished between these two provisions, see eg Cases C-92, 93/09 *Schecke, v Land Hessen, Eifert v Land Hessen* [CJEU, 2010] ECR 2010 I-11063 para 52; Cases C-468, 469/10 *ASNEF v Administración del Estado, FECEMD v Administración del Estado* [CJEU, 2011] ECR 2011 I-12181, paras. 40 et seqq; Case C-291/12 *Schwarz v Stadt Bochum* [CJEU, 2013] ECLI:EU:C:2013:670, para 53; Cases C-293/1, C-594/12 *Digital Rights Ireland Ltd. v Minister for Communications, Marine and Natural resources and others, Kärntener Landesregierung and others* [CJEU, 2014] ECKLI:EU:C:2014:238 paras 24, 29 et seq; Case C-131/12 *Google Spain v AEPD* [CJEU, 2014] ECLI:EU:C:2014:317 para 74; Case C-362/14 *Schrems v Data Protection Commissioner* [CJEU, 2015] ECLI:EU:C:2015:650, paras 39, 66.

28 Convention for the Protection of Human Rights and Fundamental Freedoms, 213 UNTS 221.

29 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

30 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37.

31 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 [2016] OJ L119/1.

32 See eg Alexander Benecke and Julian Wagner, 'National Legislation within the Framework of the GDPR' (2016) 3 EDPL 353-361.

33 In eight recitals (24, 60, 63, 70, 71, 72, 73, 91) and nine articles (4, 13, 14, 15, 21, 22, 35, 47, 70).

ple in Article 22, referring in the heading to profiling as being one such form of processing. Recital 71 gives two illustrations, namely 'an automatic refusal of an online credit application or e-recruiting practices without any human intervention'.

While Article 22 GDPR generally prohibits automated decision-making on the basis of profiling, this prohibition is subject to three wide exceptions. These exceptions include that the data subject has explicitly consented [Article 22(2)(c)], or that automated decision-making is 'necessary for entering into, or performance of a contract' [Article 22(2)(a)].[34] When one of these exceptions applies, the data controller shall establish suitable measures to safeguard the data subject's rights, freedoms and interests, including 'the right to obtain human intervention on the part of the controller, to express her or his point of view and to contest the decision' [Article 22(3)]. This does, however, not mean that any human intervention will necessarily result in an outcome that deviates from the decision proposed by the algorithm. Article 22(2)(b) also contains an opening clause under which the Member States can create further exceptions subject to suitable protections.[35] So, the individual is granted the possibility to protest against the phenomenon of the 'algorithmic governability'[36]. This right could help the detection of automated decision-making based on false profiles, but does not restrict the use of profiles as such. This can be derived in connection with the accountability principle and the new obligations for data controllers to conduct prior data protection impact assessments (Article 35) as well as for companies or public authorities whose core activities rely on profiling to have a Data Protection Officer (Article 37).

4. General Data Processing Principles

Outside the scope of Article 22 GDPR, most other regulatory requirements regarding profiling are derived from general principles regarding data processing (Article 5) and provisions regulating the lawfulness of data processing (Article 6). Profiling is permitted if either the data subject has consented or the data processing is necessary for one of the named purposes in Article 6, typically because the processing is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract [Article 6(1)(b)] or because processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, provided these interests outweigh the data subject's rights and interests [Article 6(1)(f)].

5. Further Requirements for Profiling, Especially Impact Assessment

Further requirements stem from the obligation of transparency and the data subject's information and access rights (Articles 13-15). Article 21(1) creates a right to object to data processing including profiling where this processing is based on Article 6(1)(e) or (f), which then requires the controller to 'demonstrate compelling legitimate grounds for the processing'.

The GDPR provides for a new regulatory tool, the 'data protection impact assessment', Article 35 ff. Such an impact assessment is generally required where a 'systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling', is applied [Article 35(3)(a)]. If the assessment indicates that processing would carry a high risk for the fundamental rights of the data subject, the controller must establish measures to mitigate the risk and consult with the supervisory authority (Article 36). If necessary, decisions of the Data Protection Authority (DPA) will be taken within the newly established consistency mechanism, Article 63 et seqq, assuring an identical interpretation and identical measures taken in the Member States. This will not necessarily lead to stricter rules on profiling, but at least to a greater public availability of processing measures taken and potentially to further public attention.

---

34 While the Regulation itself does not define the scope of 'necessary', recital 72 expresses the expectation that the European Data Protection Board will issue guidance on profiling. The use of special categories of data (ie sensitive data) is subject to further restrictions. Recital 71 also notes that profiling should not concern children.

35 Recital 71 envisages authorisations by Member States for the purposes of fraud and tax-evasion monitoring and prevention.

36 Antoinette Rouvroy and Bernard Stiegler, Le régime de vérité numérique, *Socio*, 4/2015, 113-140; Jan Philipp Albrecht and Florian Jotzo, *Das neue Datenschutzrecht der EU* (Nomos 2017) ch 3, paras 61, 64; Ulrich Dammann, 'Erfolge und Defizite der EU-Datenschutzgrundverordnung' [2016] ZD 307, 312 et seqq; Carolin Hohmann, 'Rechte der betroffenen Person' in Alexander Roßnagel (ed), '*Europäische Datenschutzgrundverordnung: Vorrang der Unionsrechts – Anwendbarkeit des nationalen Rechts*' (Nomos 2017), ch 3 IV, 147.

IV. A Comparative View on Profiling

1. General Data Protection Legislation

Within the EU, the DPD continues to apply until 25 May 2018 (at which date it will be replaced by the GDPR). The DPD does not regulate profiling explicitly and is, in any event, subject to transposition into the law of Member States. Additionally, the rules laid down in the E-Privacy Directive (as amended by the Cookies Directive) apply.

The *German* Constitutional Court has derived a right to informational self-determination from Article 1(1), protecting human dignity, and Article 2(1), protecting personal autonomy, of the Basic Law, the German constitution. The Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) and the States' Data Protection Acts provide the general legal framework transposing the DPD. In regard to profiling, the Tele Media Act (*Telemediengesetz*, TMG) also applies, establishing special requirements and privileges in regard to telemedia services, ie Internet-based information services other than telecommunication services. The relevant TMG provisions implement the E-Privacy Directive as well as the Cookies Directive.

The *French* constitution does not contain an explicit guarantee for privacy[37] or data protection. The primary data protection statute is the Act n° 78-17 of 6 January 1978 on Information technology, data files and civil liberties (1978 Act). It has been modified once by Act n° 2004-801 (LCEN) which transposed the DPD, and recently in October 2016 by the Digital Republic Law[38]. The 1978 Act is quoted in more than 130 laws. Some specific legislation, such as Article L. 34-1 and L 34-1-1 of the Postal and Electronic Communications Code, stems from the E-Privacy and Data Retention directives.

The *United Kingdom* has no specifically written constitution. Privacy is protected primarily through the Human Rights Act 1998, which makes the rights in the ECHR enforceable under UK law, including Article 8. The DPD was transposed into UK law through the Data Protection Act 1998 (DPA 1998). The E-Privacy Directive, and subsequently the Cookies Directive, have also been incorporated into UK law through the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 respectively.

In the *United States*, privacy rights protecting against governmental actions are provided for at the constitutional level, eg, in the First Amendment's right to anonymous speech; and, in the criminal law context, the Fourth and Fifth Amendments: the Fourth Amendment's protection against unreasonable searches and seizures which may include a reasonable expectation of privacy analysis, or the Fifth Amendment's right to remain silent. Also, the Supreme Court has suggested that informational privacy rights may fall within the substantive due process protections of the US Constitution for governmental infringements.[39]

Data privacy laws can be enacted at the federal or at the state level. There are multiple federal statutory provisions protecting personal data that may also apply to profiling. Medical and health data are protected under laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Genetic Information Non-discrimination Act. Financial and commercial data are protected under statutes such as the Fair Credit Reporting Act and statutes criminalising identity theft.

As a consumer protection matter, data privacy matters have increasingly fallen within the jurisdiction of the Federal Trade Commission (FTC). For example, section 5(a) of the FTC Act provides that 'unfair or deceptive acts or practices in or affecting commerce ... are ... declared unlawful'. The US Safe Web Act amended the definition in section 5(a) of 'unfair or deceptive acts or practices' to include 'such acts or practices involving foreign commerce that cause or are likely to cause reasonably foreseeable injury within the US or involve material conduct occurring within the United States'.

Australia is a signatory to a number of international instruments which enshrine the protection of the right to private life, including the International Covenant on Civil and Political Rights[40]. Yet, Australia does not have a Bill of Rights protecting fun-

37 Vincent Mazeaud, *Les Nouveaux Cahiers du Conseil constitutionnel* 3/2015 (N° 48) 5 et seqq. An explicit constitutionalisation of privacy came through the caselaw of the *Conseil Constitutionnel* from 1995.

38 Loi N°2016-1321 du 7 octobre 2016 pour une République numérique JORF n°0235 du 8 octobre 2016.

39 See, eg, *Whalen v Roe*, 429 U.S. 589 (1977).

40 International Covenant on Civil and Political Rights, 999 UNTS 171.

damental rights domestically and therefore also lacks a constitutional right to privacy. The legal protection of privacy and personal information in Australian law remains piece-meal and incomplete. Information privacy is protected through statute law, in particular the federal Privacy Act 1988 (Cth) and equivalents in the majority of Australian states and territories. The Privacy Act 1988 adopts a principles-based, rather than a prescriptive, approach to data protection. It contains 13 Australian Privacy Principles (APPs), which govern the collection, use, disclosure and storage of personal and sensitive information, and how individuals may access and correct records containing such information. The APPs apply to most Commonwealth government agencies and large private sector organisations (the so-called 'APP entities').

There is no right to privacy in Australian common law. To close this gap, the Australian Law Reform Commission (ALRC) has repeatedly, but so far unsuccessfully, recommended the introduction of a statutory cause of action to protect privacy.[41] Under current law, civil claims for breach of privacy are only available if, and as far as, other civil causes of action coincidentally cover conduct that affects privacy.[42]

The *Brazilian* Constitution acknowledges the inviolability of private life and also the secrecy of telephonic, telegraphic and data communications. Furthermore, it provides for the writ of habeas data, which gives citizens a means to access and correct data about themselves held by third parties.

Despite the existence of a constitutional guarantee of privacy as well as other laws on the use of personal data, a general law on data protection does not exist. However, currently there are three legislative initiatives in the National Congress which aim to regulate, comprehensively, personal data protection: Draft Bill no 4060/2012 of the Chamber of Deputies (House of Representatives); Draft Bill no 330/2013 of the Senate, and Draft Bill no 5276/2016 of the Presidency of the Republic. Moreover, the Civil Code, the Consumer Protection Code and, more recently, the Civil Rights Framework of the Internet (or Internet Act, Law no 12.965 of 2014) have regulated the protection of personal data more specifically.

Since the entering into force of the Internet Act, Brazil disposes of an advanced legal framework which establishes principles, rights and obligations for the use of the Internet. A substantial portion of the Act deals with privacy and data protection. Article 7 Internet Act provides rights and guarantees for internet users. Among them, Article 7 subsections I, II, III, VII and VIII guarantee the inviolability of privacy and intimacy, the inviolability and secrecy of all internet communication and private information which can be lifted only on behalf of a judicial warrant. Furthermore, they guarantee that personal data will not be supplied to third parties, save upon free, expressed and informed consent, as well as the right to clear and complete information about the collection, usage, storage, processing and protection of personal data, which can only be used if the collection is justified, not prohibited by law and if so specified in the terms of service or in internet application contracts. Besides this, in Article 7 subsections X and XIII, the Statute guarantees a right to erasure of personal data provided by the internet user after the termination of the legal relationship between parties and foresees the application of consumer protection rules to the consumer relations in the internet domain.

2. The Absence of a Legal Definition of Profiling

While the aforementioned 2010 Council of Europe Recommendation on Profiling defines profiling, this instrument is not legally binding on Member States. It defines profiling as an automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.[43]

In *Germany*, no legal definition of profiling has been established to date. § 6a(1) BDSG, transposing Article 15 of the DPD concerning automated decision-making, mentions 'personal aspects' as a component of a profile, but not the profile itself. § 15(3)1 TMG

41 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108, 2008), Recommendations 74-1–74-7; Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123, 2014).

42 *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63, (2001) 208 CLR 199.

43 Council of Europe (n 24) app 1(e).

uses the phrase 'usage profile', characterised in legal commentary variously as 'a data record giving a part-image of a personality'[44] or, less strictly, 'any kind of systematically compiled usage data containing information about the behaviour and habits of a user'[45]. Legal scholarship has offered a variety of definitions for profiling[46] without one having been established as the leading one. Scoring for credit purposes, as a special kind of profiling, is subject to a specific provision, § 28b BDSG.

There is also no specific definition of profiling in *French* law. Nevertheless, there is a legal framework regarding profiling, defined by two laws. The first one is Article 10 of the 1978 Act which is a transposition of Article 15 of the DPD adopted in 2004. The second one is Article L.581-9 Environmental Code which requires prior approval by the *Commission nationale de l'informatique et des libertés* (CNIL), the French data protection regulator, of any system which automatically measures the audience of advertising devices in a public space (such as billboards) or analyses the typology or behaviour of individuals passing by such devices. In addition, there is a recommendation by the CNIL of 16 December 2013 regarding the use of cookies.

Though the DPA 1998 and PECR provide the framework in which profiling would be covered, there is no official definition of profiling in the *UK*, and there has not been a significant debate over it. There are, however, specific provisions in the DPA governing 'automated decision-taking', not directly covering the creation of profiling data, but potentially governing the use of that data if used automatically.[47]

In the *US*, data profiling is a term that appears to be related to data analytics - eg, a tool to provide metrics and assess data quality, such as whether metadata is accurately descriptive. In the data privacy context of consumer protection, many discuss concerns surrounding the work of data brokers which the FTC has defined as 'companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud'.

The FTC has recommended to Congress that it consider the enactment of legislation to increase the transparency of consumer profiling by data brokers and to give consumers the ability to exercise more control over data collection and use by corporate entities. In 2016, another federal agency, the Federal Communications Commission, released new privacy regulations that now require broadband companies to seek subscriber permission to collect and use data on web browsing, app use, and on geolocational and financial information.

There is no statutory or otherwise official definition, or specific regulation, of profiling in *Australia* or *Brazil*, and no significant debate over it aside from some scholarly discussions. Generally, profiling is understood as profile creation, or as the act of automated collection and processing of information about users, with the intention of building presumptions about their personalities and, therefore, predicting future behaviour.

3. The Concept of Personal Data

Data protection laws only apply to the extent that 'personal data' are collected, processed or otherwise handled. As mentioned in the introduction, profiling consists of several steps, not all of which need to involve personal data. For example, when profiling includes an assessment, recombination and evaluation of anonymised or statistical data with no reference to any individual, data protection laws do not apply to these processes. Once personal data are collected, processed or stored in order to create a profile of an individual, data protection laws will become applic-

44 Representing many others Silke Jandt and Philip Laue, 'Voraussetzungen und Grenzen der Profilbildung bei Location Based Services' [2006] K & R 316, 317.

45 Stephan Bauer, 'Personalisierte Werbung auf Social Community-Websites' [2008] MMR 435, 437; Kerstin Zscherpe in Jürgen Taeger and Detlev Gabe (eds), *BDSG und Datenschutzvorschriften des TKG und TMG* (2nd edn, R&W 2013) § 15 TMG, para 58.

46 Eg Peter Schaar, 'Persönlichkeitsprofile im Internet' [2001] DuD 383, 385 et seq; Heike Rasmussen, 'Datenschutz im Internet' [2002] CR 36, 38; Bruno Baeriswyl, 'Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut?' [2000] RDV 6, 7; Petra Wittig, 'Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken' [2000] RDV 59; Philip Scholz in Spiros Simitis (ed), *Bundesdatenschutzgesetz* (8th edn, Nomos 2014) § 6a, para 22; Jandt and Laue (n 44) 316, 318.

47 Data Protection Act 1998 (UK) s 12; see also Information Commissioner's Office, *Guide to data protection*, Principle 6 – rights <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/automated-decision-taking/> accessed 11 November 2016.

able. Despite the centrality of 'personal data' to the application of data protection laws, the concept remains contentious, even within the EU.

The DPD of the *EU* defines personal data as 'any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, economic, cultural or social identity', Article 2(a). The definition under the GDPR remains largely unchanged but contains some clarifications, because it explicitly includes location data, online identifiers and genetic identity as further potential identifiers. Thus, under the definition in Article 4(1) GDPR, personal data is 'any information relating to an identified or identifiable natural person; an identifiable [...] person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity'. The Court of Justice of the EU (CJEU) recently clarified that an objective approach (meaning that it suffices for the construction of personal information if a person can be identified by means available to anyone) should be followed to determine identifiability.[48] Special categories of personal data are subject to additional protections under Article 9 GDPR, covering data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation.

In *Germany*, the BDSG defines personal data in § 3(1) BDSG as any 'particulars concerning the personal or material circumstances of an identified or identifiable person'; the major contrast to the DPD/GDPR being the reference to 'particulars'. Therefore, it is sometimes doubted whether group and statistical information attached to a single person can be considered to be personal information. The definition of special categories of personal data in § 3(9) BDSG is identical to the DPD. In regard to a subjective or objective approach to determining identifiability, regulators and DPAs usually follow the objective approach,[49] so eg cookies are considered to generally process personal data.[50] The discussion over it, leading to the recent CJEU judgment on dynamic IP addresses, should now end; special data is highly protected. Non-personal data is in general only protected if copyright law is applicable or if the data is considered to be a business secret.[51]

In *France*, the 1978 Act originally only referred to 'nominative information', which was narrower than the term 'personal data' later introduced by the DPD. The current definition of 'personal data' in Article 2 of the 1978 Act is very similar to the wording of the DPD and based on a comprehensive approach of identifiability. Personal data means any information relating to a natural person who is or can be identified, directly or indirectly. The only difference is that Article 2 provides that in order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to, should be taken into consideration. The DPD mentions in recital 26 that only 'all the means likely reasonably to be used' by these should be taken in account. The French definition of personal data is broader than the one of the DPD because it includes all the cases where a re-identification of the person is possible. Furthermore, this broad definition embraces the nominative identity (names but also genetic and biometric features etc) and the virtual or digital identity of the person such as any pseudonym, avatar, logging code, cookies or IP addresses.[52] Finally, Article 8 includes a specific regime for sensitive data.

In the *UK*, the definition of personal data is intended to follow that in the DPD, but the case of *Durant*[53] narrowed the interpretation, suggesting that person-

48 Case C-582/14 *Breyer v Bundesrepublik Deutschland* [CJEU, 2016] ECLI:EU:C:2016:779 paras 39, 43, 46.

49 See Düsseldorfer Kreis, *Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten* (decision from 26/27 November 2009); Thomas Dreier and Indra Spiecker genannt Doehmann, *Die systematische Aufnahme des Straßenbildes – zur rechtlichen Zulässigkeit von Online-Diensten wie "Google Street View"* (Nomos 2010) 67 et seqq; Matthias Bergt, 'Die Bestimmbarkeit als Grundproblem des Datenschutzrechts' [2015] ZD 368.

50 Ulrich Dammann in Spiros Simitis (ed), *Bundesdatenschutzgesetz* (8th edn, Nomos 2014) § 3, para 65; Peter Schaar, *Datenschutz im Internet* (Beck 2002) paras 177 et seqq, 186; Johann Bizer, 'Web-Cookies – datenschutzrechtlich' [1998] DuD 277, 280.

51 See BVerwG,case 6 B 59/04 [2005] in [2005] CR, 194, 195; BVerfG, cases 1 BvR 2087/03, 1 BvR 2111/03 [2006] in [2006] NVwZ 1041, 1042; BGH, case VI ZR 156/13 [2014] in [2014] NJW 2014, 1235, 1237; also regulated explicitly in several regulations.

52 Anne Debet, Jean Massot and Nathalie Metallinos, *Informatique et libertés, la protection à caractère données personnelles en droit français et européen* (Lextenso 2015) 248.

53 *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

al data 'should have the putative data subject as its focus' and referred to 'biographical significance', meaning 'information that affects [a person's] privacy, whether in his personal or family life, business or professional capacity'.

The courts in the UK have subsequently been broadening the definition again, bringing it closer to the definition in the DPD. In the case of *Edem*,[54] the Court of Appeal noted that the contentious requirement in *Durant* should only apply in 'borderline' cases.[55] The court specifically endorsed the guidance of the UK Information Commissioner (ICO) over what constitutes personal data, a guidance that aligns much closer with the wording of the Directive.[56]

As the UK considers its future approach to data protection in the light of Brexit, it is possible that the historical attitude to the definition of personal data is retrenched. Whether cookies are considered personal data is contextual: the ICO notes that though the PECR apply to all cookies, the DPA applies only to cookies that 'process personal data', implying that 'anonymised' cookie data do not constitute personal data,[57] while whether IP addresses constitute personal data under UK law remains uncertain.

In the *US,* the concept of Personally identifiable information (PII) is defined as:

> [A]ny information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[58]

In recent years, Congress has not passed federal legislation expressly defining the legal scope of 'personal data' despite increased efforts for a more encompassing definition. The Obama Administration promulgated efforts to coordinate a data privacy legislative reform in the 'Consumer Privacy Bill of Rights'. In the White House 'Discussion Draft of the Consumer Privacy Bill of Rights Act of 2015', for example, personal data is defined as any data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or, as a practical matter, linkable by the covered entity, to a specific individual. Interestingly, sufficient is also the link to a device that is associated with or routinely used by an individual. In that sense, personal data can be, eg, (among others) the name, address, telephone/social security/passport/driver's licence number, biometric identifier (eg fingerprint) or any unique persistent identifier, including an alphanumeric string that uniquely identifies a networked device, financial account number, health care account number or any required security code, access code, or password that is necessary to access an individual's service account. Also, unique identifiers or other descriptive information about personal computing or communication devices are included in the list. Moreover, any data that are collected, created, processed, used, disclosed, stored, or otherwise maintained and linkable, are mentioned.

Australia uses the concept of 'personal information'. Since 2014, the Privacy Act 1988 defines 'personal information' in section 6 as '[...] information or opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in material form or not'.[59]

Unlike the Organisation for Economic Co-operation and Development (OECD) Guidelines, which define personal data as 'information relating to an iden-

54 *Edem v IC & Financial Services Authority* [2014] EWCA Civ 92.

55 'Roll out the bunting: Durant judgment is good as dead and buried' (*Amberhawk*, 19 February 2014) <http://amberhawk.typepad.com/amberhawk/2014/02/roll-out-the-bunting-durant-judgment-is-good-as-dead-and-buried.html> accessed 11 November 2016.

56 Information Commissioner's Office, *Guide to data protection*, *Key definitions* https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/ accessed 11 November 2016.

57 See Information Commissioner's Office, *Guide to Privacy and Electronic Communications Regulations* <https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/> accessed 11 November 2016.

58 US National Institute of Standards and Technology, US Department of Commerce, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* Special Publication 800-122 (April 2010) <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf> accessed 11 November 2016.

59 Privacy Act 1988 (Cth) s 6(1). 'Sensitive information' is given greater protection under the APPs than other information. Sensitive information includes information about a person's racial or ethnic origin; political opinions; religious or philosophical beliefs; sexual orientation as well as health, genetic or biometric information.

tified or identifiable individual',[60] the Australian definition refers to information 'about' an individual. It has been suggested that this may make a difference in cases where information has only tenuous connection with an individual, in particular where information identifies a device rather than an individual.[61]

This is illustrated by the ongoing so-called Grubb litigation, in which the Administrative Appeals Tribunal (AAT) held that the words 'about an individual' in the definition of personal information raised a threshold question that needs to be addressed before the determination whether that individual is identified or identifiable. AAT Deputy President Forgie decided that mobile phone service metadata was information about a service, not about an individual[62] – notwithstanding the fact that the individual who obtained the service was ascertainable from this information. Similarly, it was held that a dynamic IP address is not information about an individual because 'the connection between the person using a mobile device and an IP address is ... ephemeral'.[63] The contentious decision that such metadata was not personal information is currently under appeal. The decision of Full Court of the Federal Court is highly anticipated because it will provide the first interpretation by an appellate court of the Australian definition of 'personal information'. The exact scope of that term will be of critical importance in cases where information can be linked to an individual only through indirect means, such as the interrogation of, and matching across, multiple databases. The Grubb litigation has evident relevance also for tracking of individuals through their use of electronic devices. To the extent that cookie technology only ascertains IP addresses rather than a person, it remains currently doubtful in Australia whether the information collected and stored is personal information.[64]

In *Brazil*, the concept of personal data is expressed in the Draft Bills, and is defined as: any information relating to an identified or identifiable individual, directly or indirectly, including every address or identification number of a terminal used for connection to a computer network. The recent Decree no 8,771/2016, which regulates the Civil Rights Framework of the Internet, defines personal data, in item I of Article 14, as data related to identified or identifiable natural persons, including identifying numbers, electronic identifiers or locational data when they are related to a person. Three types of data can be the object of analysis: (1) General Personal Data – data related to an identified or identifiable natural person, electronic identifiers or locational data, ie birth dates, addresses, passwords, profile descriptions, etc; (2) Sensitive Data – personal data revealing racial or ethnic origin, religious, philosophical or moral convictions; data concerning the health or sex life, as well as genetic data; and (3) non-personal data – data relating to a data subject that cannot be identified, either by the controller or by any other person, taking into account the number of susceptible means reasonably to be used to identify the data subject.

4. Consent and Other Legitimate Grounds for Profiling

According to *European* standards under the DPD, decision-making based solely on automated processing of personal data is in general forbidden, but it is lawful when based on consent or another specified ground. This will remain intact under the GDPR.

In *Germany*, the requirements of lawful data processing differ, depending on whether the profiling is done by the data processor for his or her own commercial purposes (§ 28 BDSG) or whether it is done for the commercial purpose of transferring the results to a third person (§ 29 BDSG). Both provisions require a balancing of interests. The DPAs agree that advanced user profiles beyond the individual contract need to be pseudonymised.[65] Under § 28b BDSG, businesses are allowed to generate and use a statistical value on a person's future behaviour for the establishment, execution or termination of a contractual relationship. This scoring method may be used on a mathematic-statistical basis only, but not for past-related evaluation of data, hence prohibiting the

60 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013) pt I 1b).

61 Eg Mark Burdon and Alissa McKillop, 'The Google Street View Wi-Fi Scandal and its Repercussions for Privacy Regulation' (2013) 39 Monash University Law Review 702, 712.

62 *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991, 112.

63 ibid 113.

64 Robert Slattery and Marilyn Krawitz, 'Mark Zuckerberg, the Cookie Monster – Australian Privacy Law and Internet Cookies' (2014) 16 Flinders Law Journal 1, 16.

65 Düsseldorfer Kreis, *Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten* (decision from 26./27 November 2009).

generation of personal profiles,[66] which are conducted by algorithm analysis.

By collecting and creating more data than necessary for the individual purpose, profiling often conflicts with the principles of necessity and data scarcity and also with the principle of appropriation as profiling is executed to find new scopes for existing data and create meta-data. The balancing test therefore regularly comes down in favour of the legitimate interest of the data subject.[67] This applies all the more as the legitimate interest of a data subject of not being profiled increases as more data about him or her is compiled.[68] The Cologne Civil Court of Appeals ruled that a company did not have the right to establish profiles comparing former customers under § 28 BDSG.[69]

A comprehensive personal profile is seen as the upper limit of what data collection and processing are allowed to create. Uncontrolled compilation of personal data, indexing the personality of a human being and making him or her the pure object of information, is inconsistent with the German constitution[70] and also, considering the data retention decision of the CJEU,[71] with European law.

As informed consent under § 4a BDSG is bound by its purpose, profiling can be based on consent only if the purposes of the profiling are specified before the processing. However, undefined profiling or a general profiling for any not pre-determined purpose is not permissible.

In the *French* legal context, there is no real prohibition of profiling but rather specific conditions for allowing it. First, the collection of the data for a profiling use must adhere to the main principles of the 1978 Act: fair and lawful processing (Article 6 § 1) for specified, explicit and legitimate purposes and only for those purposes (Article 6 § 2). The processing has to be based on legitimate grounds (Article 7), consent of the data subject being one of them. The pursuit of the data controller's legitimate interest is also frequently invoked. Most of the time, a balancing of interest has to be done.

Secondly, specific requirements must be met for the collection and the processing of special data. Article 8 provides ten possibilities for profiling of sensitive data. Sensitive data may be profiled with the explicit consent of the data subject or if the data subject himself or herself disclosed these sensitive data, except if a law prohibits it.[72] French law also imposes an obligation to obtain authorisation by the CNIL before the implementation of such processing.[73]

In the *UK*, the legal limits are those governing data in general. The UK government and the ICO gave support to an internet-based profiling and advertising business that intercepted an ISP subscriber's web traffic and built up a profile of the subscriber for commercial reasons claiming to apply an 'anonymisation' technique.[74] In another case, the ICO found an app that analysed people's tweets to assess whether they were in a vulnerable mental state to be in breach of the rules concerning sensitive personal data. The ICO made it clear that data protection rules apply even on public data from the public tweets.[75]

In the *US*, notice and consent requirements are encouraged by the FTC's Fair Information Practice Principles (FIPPs):[76]

66 Kai von Lewinski in Heinrich Wolff and Stefan Brink (eds), *Datenschutzrecht in Bund und Ländern* (Beck 2013) § 28b, para 1; Peter Gola and Rudolf Schomerus, *BDSG: Bundesdatenschutzgesetz Kommentar* (12th edn, Beck 2015) § 28b, para 6.

67 Spiros Simitis in Spiros Simitis (ed), *Bundesdatenschutzgesetz* (8th edn, Nomos 2014) § 28, para 138 et seqq; Thomas Paefgen, 'Datenbankmanagement als Führungsinstrument' [1994] CR 65 et seqq; Astrid Breinlinger, 'Datenschutzrechtliche Probleme bei Kunden- und Verbraucherbefragungen' [1997] RDV 249 et seqq; Thilo Weichert, 'Datenschutzrechtliche Probleme beim Adresshandel' [1996] WRP 522, 527.

68 See Jürgen Taeger, 'Datenschutz im Versandhandel' [2007] BB 785, 789 et seq.

69 OLG Köln, case I-6 U 70/09 [2010] in [2010] NJW 90.

70 BVerfG cases 1 BvR 209/83 and others [1983] in BVerfGE 65, 1, 48; BVerfG case 1 BvL 19/63 [1969] in BVerfGE 27, 1, 6.

71 *Digital Rights Ireland* (n 27) and *Kärntener Landesregierung* (n 27) paras 27 et seqq, 32 et seqq, 52 et seqq.

72 See art 1111-8 of the Code of Public Health which prohibits paid transactions of personal health data even with the consent of the data subject. However, a lot of profiling processing due to connected objects or smartphone applications should not be covered by this exemption.

73 See art L. 581-9 of the Environmental Code requires prior approval by the CNIL of any system which automatically measures of the audience on an advertising device in a public space (such as billboards) or analyses the typology or behaviour of individuals passing by such devices.

74 See eg Paul Bernal, 'Rise and Phall: Lessons from the Phorm Saga' in Serge Gutwirth et al (eds), *Computers, Privacy and Data Protection: An element of choice* (Springer 2011).

75 Information Rights and Wrongs (Blog), 'ICO: Samaritans Radar failed to comply with Data Protection Act' (*Information Rights and Wrongs*, 25 April 2015) <https://informationrightsandwrongs.com/2015/04/25/ico-samaritans-radar-failed-to-comply-with-data-protection-act/> accessed 11 November 2016.

76 Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998) <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf> accessed 15 December 2016.

1. Notice/Awareness (to the individual about information collected, maintained and used by the entity);

2. Choice and Consent (on the part of the individual about that information, including whether it is collected in the first instance and how and under what circumstances it is disclosed to third parties);

3. Access/Participation (whether the individual has access to that information and the ability to correct any mistakes);

4. Integrity/Security (the administrative, technical and physical safeguards of the information, including notice if the information is leaked);

5. Enforcement/Redress (legal, policy, contractual or ethical).

The FIPPs are understood to be conceptual guidelines, not laws.[77] The adherence relies upon corporate self-regulation. In the US, no federal statute provides consumers with the right to learn what information data brokers have compiled about them, nor provides a requirement of consent or 'opt out' options to prevent data brokers from collecting, sharing or publishing their personal information.

Profiling in *Australia* is subject to the general data processing regime under the Privacy Act 1988 (Cth). As stated above, the APPs only apply to the handling of personal information, so profiling on the basis of de-identified information is not regulated in the Privacy Act.

Consent is a critical concept underlying a number of the APPs. It can provide an exception from a general prohibition of handling data in a particular way. For example, under APP 3.3, an APP entity can collect sensitive information about an individual only with that person's consent. Under APP 6.1, an APP entity must not use personal information for a secondary purpose (ie a purpose other than the particular purpose for which the data was collected) unless the individual consents (or an exception applies).

Part IIIA of the Privacy Act 1988 sets out the types of personal information that credit providers and credit reporting bodies are permitted to collect about an individual for the purpose of inclusion in that individual's credit report. That part also provides safeguards in relation to the handling of that information, including who is permitted to access an individual's credit report and for what purposes.

There is also a self-regulatory guideline for third party online behavioural advertising (OBA), developed by the online advertising sector. The Guideline states that no '[p]ersonal information is collected or used for OBA' and distinguishes OBA from customer profile advertising (which is based on the personal information of an individual user). Also, third party OBA is subject to seven self-regulatory principles, among them that third parties who want to combine OBA data with personal information must treat the OBA data as if it is personal information and in accordance with the Privacy Act. Other principles include a requirement to provide clear information to users, to give users choice over the collection of data for OBA, to keep data for no longer than necessary and to seek explicit consent for sensitive market segments.

In different situations, the *Brazilian* legal system protects the individual by imposing a requirement of prior consent for numerous acts of civil life. In the digital context, the Civil Rights Framework to the Internet in item IX of Article 7 assigns rights to the data subject, among these the clear manifestation of consent for operations concerning his/her personal data.

Law no 12.414/2011 (Credit Report Act) grants the consumer power over the creation, transfer and cancellation of his/her credit history. Consumer consent is, hence, the touchstone of this framework, as provided by Article 4. Furthermore, according to Article 5, consumers may obtain the cancellation of the record upon request and, as determined by Article 9, the sharing of information is permitted only if expressly authorised by the consumer.

5. The Challenges of Transparency, Remedies and Enforcement

Transparency, ie the obligation on data controllers to be open and honest about their data handling practices, is an important aim of data protection laws.

Under the DPD of the *EU*, the general rights of data subjects also apply in the context of profiling. Thus, the data subject may request information about stored data, may require erasure or correction and, if rights were violated, may in general claim damages. The DPAs are entitled to control whether the law was obeyed and may enact sanctions. In several judgments, the CJEU has strengthened the position

77 Robert Gellman, *Fair Information Practices: A Brief History* (rev. June 17, 2016) <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf > accessed 15 December 2016.

and independence of DPAs also vis-à-vis the European Commission.[78] Under the GDPR, the DPAs are required to make use of a consistency procedure in cross-border cases; the fines for violations have been raised, but other than that, the general structure of remedies remains unchanged.

In *Germany*, the provider of Internet services is subject to stricter data protection duties than a data processor under general data protection law. Under § 13 (1) 1 TMG, the data subject is to be notified about the character, extent and purpose of the collection and use of his or her personal data.[79] For automated processing that enables the later identification of users and prepares the collection of personal data, § 13 (1) 2 TMG also establishes a prior duty to inform the data subject.[80] The declaration of consent and the notification have to be executed separately from the other information and declarations [§ 13 (2) TMG] and can be done electronically. As illegal profiling infringes a person's right on informational self-determination, the data subject can apply for an injunction[81] and also for damages, according to § 823 (1 and 2) Civil Code (BGB) and § 7 BDSG. However, as German law only exceptionally grants damages for non-pecuniary losses arising from injury of personality rights, these monetary remedies are often fruitless.

In case of automated decision-making, the data subject may also claim information about the technology behind the decision, ie the algorithms and the data; however, the *Bundesgerichtshof*, the highest German Civil Court, has restricted access in credit-scoring cases due to prevailing interests of the scoring company.[82]

In *France*, the right to be informed (Article 32 of the 1978 Act), the right to object (Article 38) and the right to access and to rectification (Article 39) can be used by the data subject in the context of profiling.

In the *UK*, advice and support is provided by the ICO. Due to restraints in resources, in practice, data subjects rely on civil society or pro-active lawyers and other groups to both discover that they have been illegally profiled and to learn about potential remedies.

In the *US*, the FTC has released a report in May 2014 calling for greater transparency and accountability measures in regulating data brokers. In the corporate context, commercial databases are increasingly subjected to a regulatory framework that falls within Section 5 enforcement of the FTC.

Consumers in the US generally have no federal right to know what information data brokers have compiled about them. According to the FTC, no current federal laws require data brokers to maintain consumer data privacy unless the data is used for credit, employment, insurance, housing, or other related purposes. Also, no federal law provides consumers with the right to correct inaccuracies in the data. However, the Fair Credit Reporting Act (FCRA) regulates consumer reporting agencies (CRAs), which are entities that assemble consumer data into consumer reports (credit reports) for credit scoring systems. The FCRA applies to data brokers if the data is used by issuers of credits or insurances, or by employers, landlords, and others in making eligibility decisions affecting consumers. Several experts have recently called for greater regulation of data mining, including regulation of government data mining and regulation of private data brokers.

Enforcement of data privacy laws and promulgation of federal data privacy regulation can be accomplished through agencies; many federal agencies have created a Privacy Officer. On the private sector side, consumers may file a complaint with the FTC, for example. However, the jurisdiction is limited to what congressional statutes may have been enacted to support the agency's enforcement activities.

Under constitutional provisions, citizens can attempt to vindicate constitutional rights in federal court. For example, in the No Fly List litigation, which remains active, the plaintiffs have asserted both procedural due process and substantive due process violations.[83]

In *Australia*, the declared object of APP 1 is 'to ensure that entities manage personal information in an open and transparent way'. This includes that an APP

78 Case C-518/07 *Commission v Germany* [CJEU, 2008] ECLI:EU:C:2010:125 paras 24 et seq; Case C-614/10 *Commission v Austria* [CJEU, 2012] ECLI:EU:C:2012:631 para 42 et seqq; Case C-230/14 *Weltimmo v Nemzeti Adatvédelmi és Információszabadság Hatóság* [CJEU, 2014] ECLI:EU:C:2015:639 paras 19 et seqq; Indra Spiecker gen. Döhmann, 'Anmerkung zu EuGH Rs. C-518/07 – Unabhängigkeit der Datenschutz-Aufsichtsbehörden im nicht-öffentlichen Bereich' [2010] JZ 787 et seqq with further references.

79 Flemming Moos in Jürgen Taeger and Detlev Gabel, *BDSG und Datenschutzvorschriften des TKG und TMG* (2nd edn, R&W 2013) §13, paras 4, 9.

80 ibid para 10.

81 ibid § 28, para 237.

82 BGH, case VI ZR 156/13 [2014] in [2014] NJW 1235, 1237.

83 See, eg, *Latif v Holder* 686 F.3d 1122, 1124, 1126 (9th Cir. 2012) (No Fly List litigation by plaintiffs alleging, inter alia, due process violations).

entity has a clearly expressed and up-to-date privacy policy about how it manages personal information (APP 1.3). APP 5 requires that APP entities take reasonable steps to inform individuals of the fact and circumstances, as well as the purposes, of the collection of personal information and to which third parties the information will usually be disclosed. It depends on the circumstances of each case what steps need to be taken to ensure compliance with this Principle. Under APP 12.1, an APP entity that holds personal information must on request give the individual access to the information. The legal remedies against breaches of privacy are effectively limited to regulatory responses. A person alleging a breach of their privacy rights under the Privacy Act 1988 can complain to the Office of the Australian Information Commissioner. The Commissioner has traditionally adopted a 'light touch' approach to regulation, under which most complaints were resolved through conciliation. When the Commissioner makes use of his power to make a determination, he may require the respondent to change its practices or to take reparative action, including pay compensation, make an apology or provide another suitable remedy. As there is no common law right to privacy, invasions of privacy are not actionable in civil courts.

In Article 7, VIII, the *Brazilian* Civil Rights Framework of the Internet approaches transparency and purpose. Article 7, VI and VIII establish that privacy policies or any terms of use applicable to personal data shall be clear and understandable. The need for 'clear and comprehensive' information is a consequence of the adoption of the informed consent mechanism. All treatments of personal data shall be known and transparent to the data subject, in their existence and characteristics.

Like the Consumer Protection Code, the Credit Report Act establishes the rights to the access, rectification and cancellation of data (Article 5, II and III). Furthermore, it grants the consumer access to the main criteria used in the credit rating process, that is, the consumer has the right to know the criteria upon which a calculation of credit risk is based (Article 5, IV).

Data subjects who may wish to know about their personal data stored at databases may require access to this information. If denied the same, data subjects have recourse to a constitutional writ of habeas data, regulated by Federal Law no 9.507/97. Based on Article 7, it shall be granted: to ensure knowledge of information relating to the person of the petitioner stored at public databases (I) or, for the correction of data, when the petitioner does not prefer to do so through confidential, judicial or administrative proceedings (II).

6. Automated Decision-Making

The *EU* regulates automated decision-making currently through the DPD and, in future, through the GDPR. However, the regulatory effects can be considered as rather limited so far.[84]

In *Germany*, § 6a BDSG prohibits that decisions with legal or other significant effect are based exclusively on an automated processing of personal data. Aside from this, the use of profiling is only rarely forbidden, eg in health or insurance law for reasons of consumer protection; a general provision does not exist.

In *France*, the ban of automated decision-making had been originally envisaged in the 1978 Act (Articles 2 and 3).[85] Currently, Article 10 of the 1978 Act provides that no decision having a legal effect on an individual may be taken solely on the basis of automatic processing of data intended to define the profile of the data subject or to assess some aspects of their personality. The Article has a theoretical scope. It has only be quoted by the CNIL in order to remind the data controller that he has to proceed to a human intervention or to give the data subject the opportunity to give his/her point of view. The failure to comply with this obligation is not punishable by law. Under Article 10 of the 1978 Act, the CNIL and the judges can only provide a review of a decision that involved a human intervention.

In the *UK*, there are specific provisions in the DPA governing 'automated decision-taking', not directly covering the creation of profiling data, but potentially governing the use of that data if the data is processed automatically. No further regulation exists aside from the specific area of credit rating which is regulated mostly by the Consumer Credit Act 1974, which defines a 'credit reference agency' as 'a person

84 See also above 3.3.

85 The original 1978 Act had opted for a larger material scope including all administrative or private decision which implies an appreciation on the human behaviour and not only a decision having legal effect on individual.

carrying on a business comprising the furnishing of persons with information relevant to the financial standing of individuals, being information collected by the agency for that purpose.' Credit reference agencies (CRAs) are regulated by the Financial Conduct Agency (FCA) rather than the ICO, and the credit reports they provide may also legally be used to '...verify the identity, age and residency of individuals, to identify and track fraud, to combat money laundering and to help recover payment of debts.'[86]

The FCA requires CRAs to supply credit rating information to individuals in a timely manner and at a low cost, but not the logic or underlying systems through which ratings are calculated.

In the *US*, there are no specific rules or regulations that govern automated decision-making processes as a whole. Companies may use them in a range of business environments, including in credit and mortgage lending and employment decisions. To the extent that guidance is provided on automated decision-making, it would likely be applied pursuant to an already existing regulatory regime. For instance, the Fair Credit Report Act of 1970 regulates the collection, dissemination and use of consumer information, including consumer credit information, and fairness and accuracy in credit decision-making. In regard to data processing between the EU and the US, the Article 29 Working Party has commented that the new US-EU Privacy Shield does not provide any guarantees in relation to control of automated decision-making.[87]

In *Australia*, profiling abuses can arise when decisions are made on the basis of unjustifiable profiling, including decisions made on an automatic basis.[88] There is currently no specific regulation in Australia of automated or computer-assisted decision-making although it is becoming increasingly widespread.[89] Anti-discrimination legislation may provide redress in cases in which decisions are based on non-permissible grounds such as race, sex or disability.

7. The Scarcity of Case Law on Profiling

There is no *EU* case law on profiling. The data retention decision of the CJEU, which concerned the collection and use of telecommunications data,[90] has some bearing on profiling because it defined narrow limits for general and blanket data retention.

In *Germany*, the *Bundesgerichtshof* refused to grant a data subject access under § 34 BDSG to the calculation method of a credit scoring agency. The so-called 'score formula' was judged to be part of a company's protected business secrets; access rights were limited to information about the data used and the conclusion.[91] The decision has been criticised as reducing the rights of data subjects too far.[92]

The *Bundesverfassungsgericht*, the German Constitutional Court, has ruled several times that overreaching profiles by the state are not legitimate under the Constitution,[93] however, data retention is possible.[94] This ruling also applies indirectly to profiling by private entities.

In *France*, case law on profiling, as well as data protection in general, is remarkably scarce. The majority of decisions relate to the informed consent of the data subject regarding cookies, usually following CNIL investigations into the use of cookies in certain sectors (dating web sites or news websites) or by companies (Google, Facebook).[95] In some cases, the storing of the data was excessive in time.[96] Furthermore, globalised information service companies such as Google and Facebook were criticised by the CNIL[97]

86 Information Commissioner's Office, *For the public: Credit* <https://ico.org.uk/for-the-public/credit/> accessed 11 November 2016.

87 Article 29 Data Protection Working Party, 'Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision' (13 April 2016) 2.1.5, 17-18.

88 Lyria Bennett Moses and Janet Chan, 'Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools' (2014) 37 University of New South Wales Law Journal 643.

89 The Hon Justice Melissa Perry and Alexander Smith, 'iDecide: the Legal Implications of Automated Decision-making', Speech at the University of Cambridge, Cambridge Centre for Public Law Conference 2014: Process and Substance in Public Law, 15-17 September 2014 <http://www.fedcourt.gov.au/digital-law-library/judges-speeches/justice-perry/perry-j-20140915> accessed 11 November 2016.

90 *Digital Rights Ireland* (n 27) and *Kärntener Landesregierung* (n 27) paras 27 et seqq, 32 et seqq, 52 et seqq.

91 BGH case VI ZR 156/13 [2014] in [2014] NJW 1235, 1237.

92 Ulrich Schulte am Hülse and Markus Timm, 'Anmerkung zu BGH, Urt. v. 20.01.2014, VI ZR 156/13' [2014] in [2014] NJW, 1235, 1239; Christian Kirchberg, 'Anmerkung zu BGH, Urt. v. 29.01.2014, VI ZR 156/13' [2014] in [2014] NVwZ 747, 752.

93 BVerfG cases 1 BvR 209/83 and others [1983] in BVerfGE 65, 1, 53; BVerfG case 1 BvL 19/63 [1969] in BVerfGE 27, 1, 6.

94 BVerfG cases 1 BvR 256/08 and others [2010] in BVerfGE 125, 260, 321.

95 Decision 2016-007 of 26 January 2016 in which the CNIL revealed that the large scope of the surveillance made by Facebook.

96 See the Deliberation 2013-420 of the CNIL regarding Google Privacy Policy.

97 ibid.

for compiling all the information across all of their services or across Internet users without legal basis.

In its deliberation 2015-255, the CNIL disallowed the practice of estimating pedestrian flow in a Parisian district by using information from tracking the addresses of mobile phones within the reach of 25 metres. The decision was based on Article 7 of the 1978 Act and the lack of informed consent. The CNIL estimated that the data controller's legitimate interest has to be compatible with the right to be previously informed of the data subject. The CNIL also pointed to the lack of proportionality between the risks of the processing and the guarantees created for the data subject.

In the *UK*, due to the general 'light touch' approach of the ICO, many of the key examples in this field never reach court and ICO's opinions sometimes come to public attention only as a result of Freedom of Information requests.[98]

One profiling case that did come to court has been the 'blacklisting' system that had been used by major construction firms for many years.[99] Secretly established profiles of workers on union activity, health and safety issues etc. were used to 'blacklist' and prevent them from being employed.[100] The case was finally settled out of court for tens of millions of pounds of damages from the blacklisters;[101] the basis, however, was breach of confidence and defamation rather than any specific profiling or data protection law.

Other critical cases include *Vidal-Hall*[102] concerning Google's tracking of people for targeted advertising overriding the privacy settings in the browser. Effectively, the court ruled that for the tort of 'misuse of private information'[103] to apply, and for a breach of the Data Protection Act in addition to that, there was no need for pecuniary harm. In other words, the distress alone of having one's private information gathered against one's wishes was a breach – which leaves the possibility for profiling itself to be seen as a breach.

With regard to credit scores, the *Brazilian* Superior Court of Justice (STJ)[104] has recently decided that this commercial practice is authorised by Article 5, IV and by Article 7, I of the Credit Report Act. Therefore, credit score data banks are a lawful commercial practice. But, data subjects must authorise the inclusion of their information in the database (Article 2, II), thus making a further consent by the consumer to make use of it unnecessary. However, if consumers request information about the sources of data used, these shall be provided (Article 2). The violation of these rights may give rise to liability of the service provider, the person responsible for the database, the source and the person or company that made use of the information (Article 16) for the occurrence of moral damages in the event of use of excessive information or sensitive data (Article 3, § 3, I and II), and in cases of improper denial of credit using incorrect or outdated data.[105]

Especially interesting for profiling studies is the *Oi/Phorm* case, investigated and decided by the National Consumer Bureau (SENACON) of the Ministry of Justice. The SENACON issued a fine of $1.6 million to one of the country's largest telecommunications companies (Oi) for invading the privacy of subscribers to its broadband Internet service by tracking their web usage and offering this data for behavioural advertisement without consent.[106]

V. Conclusion and Outlook

Profiling is a worldwide practice of analysing information and making use of personal data to evaluate aspects of individual personality and to predict human behaviour. Big and Smart Data analytics make this practice potentially more accessible, more reliable, and therefore economically more lucrative.

There is a dearth of decided cases, making it difficult to assess whether the differences in regulatory approaches have much effect on the actual practice. Consumer protection rights, telecommunications

98 Eg the Samaritans Radar app, see UK section (n 75) 18.

99 For a detailed discussion of this story, see Dave Smith and Phil Chamberlain, *Blacklisted – the Secret War Between Big Business and Union Activists* (New Internationalist 2015).

100 Information Commissioner's Office, *For the public: Construction blacklist* <https://ico.org.uk/for-the-public/construction-blacklist/> accessed 11 November 2016.

101 See 'Construction workers win payouts for "blacklisting"' (*BBC News*, 9 May 2016) http://www.bbc.co.uk/news/business-36242312 and 'Vidal-Hall v Google Inc' (*5RB*, 16 January 2014) <http://www.5rb.com/case/vidal-hall-ors-v-google-inc/> accessed 11 November 2016.

102 *Vidal-Hall v Google Inc* [2014] EWHC 13 (QB).

103 As established in *Campbell v MGN Ltd* [2004] UKHL 22.

104 The STJ is responsible for the final judgment of civil and criminal cases not involving constitutional matters thus standardizing the interpretation of federal law.

105 STJ -Resp. 1419697 RS, Rel. Ministro Paulo de Tarso Sanseverino, Segunda Seção, julgado em 12/11/2014, DJ 17/11/2014 <http://zip.net/bxtxbk> accessed 11 November 2016.

106 Phorm is the same company referred to in the UK section (n 74).

law, data protection frameworks and general privacy rights, to name just a few, all compete with each other without setting clear standards or providing clear outcomes. Legal scholarship is only beginning to address the conflict of interests arising from the use and economic benefits of commercial profiling, on the one hand, and its effect on personal dignity, autonomy and privacy, on the other hand.

While the use and applications of commercial profiling are likely to increase, many questions remain to be answered. In the age of Big and Smart Data, of ubiquitous computing and self-learning machines, a clearer approach to the regulation of profiling that gives proper consideration to both its promises and risks, is urgently required. This report provided a first overview and comparative stock-take.