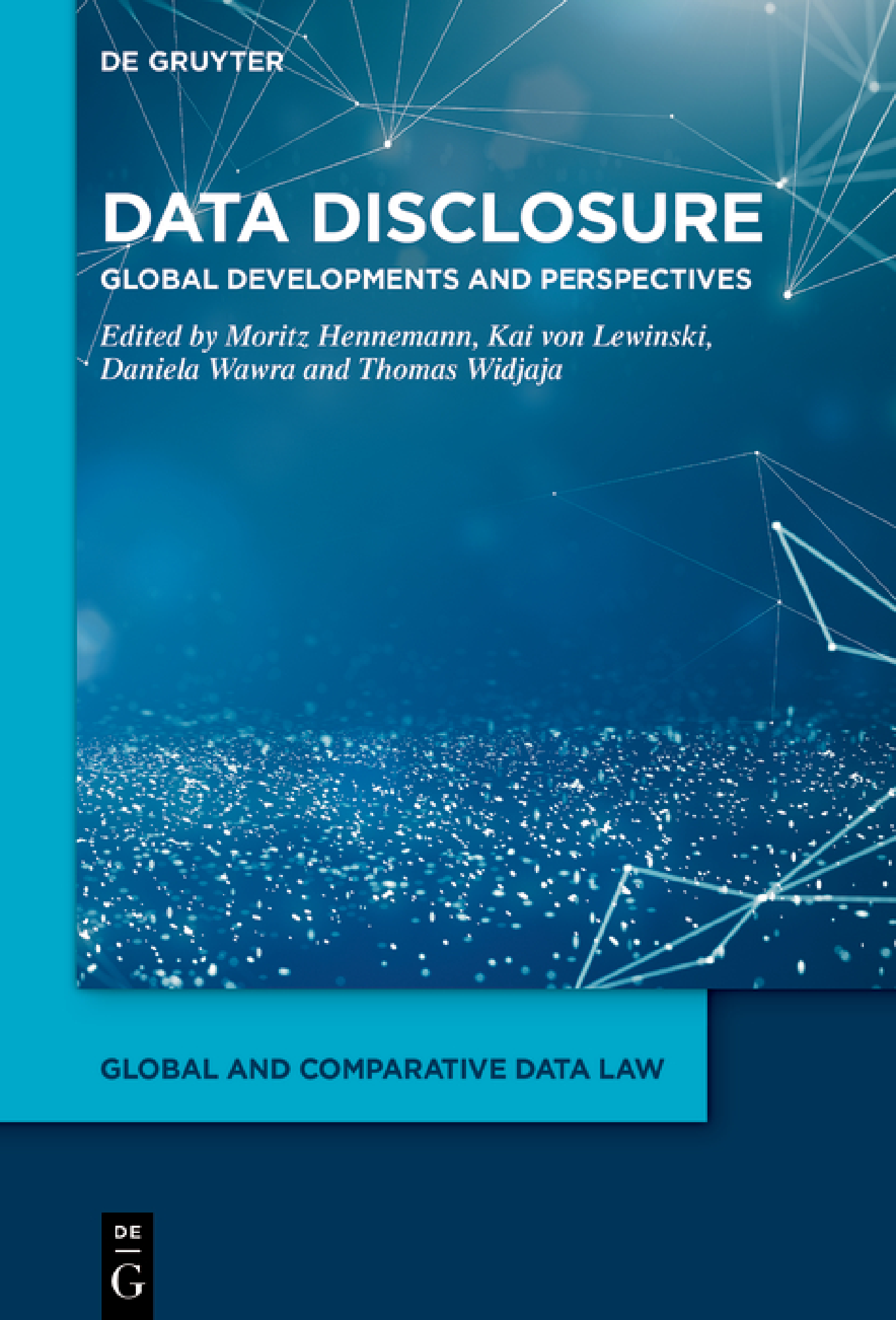
DE GRUYTER
DATA DISCLOSURE
GLOBAL DEVELOPMENTS AND PERSPECTIVES
Edited by Moritz Hennemann, Kai von Lewinski, Daniela Wawra and Thomas Widjaja
GLOBAL AND COMPARATIVE DATA LAW
DE G

Data Disclosure

Global and Comparative Data Law

Edited by
Moritz Hennemann
Lea Katharina Kumkar
Linda Kuschel
Björn Steinrötter

Volume 2

Data Disclosure

Global Developments and Perspectives

Edited by
Moritz Hennemann
Kai von Lewinski
Daniela Wawra
Thomas Widjaja

DE GRUYTER

This research project and the publication of this volume is funded by the Bavarian Research Institute for Digital Transformation (bidt), an institute of the Bavarian Academy of Sciences and Humanities. The authors are responsible for the content of this publication.

ISBN 978-3-11-100985-8
e-ISBN (PDF) 978-3-11-101060-1
e-ISBN (EPUB) 978-3-11-101176-9
ISSN 2751-0174
DOI https://doi.org/10.1515/9783111010601

Library of Congress Control Number: 2022952376

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the internet at http://dnb.dnb.de.

Cover image: peshkov / iStock / Getty Images
Printing and binding: CPI books GmbH, Leck

www.degruyter.com

Foreword

Fellow reader,

Our interdisciplinary research project "Vectors of Data Disclosure" combines legal, cultural studies, and information systems perspectives. The 2021–23 project is kindly funded by the Bavarian Research Institute for Digital Transformation (bidt) – a support for which we are more than grateful. The principal investigators are Moritz Hennemann (Law), Kai von Lewinski (Law), Daniela Wawra (Cultural Studies), and Thomas Widjaja (Information Systems).

The generous funding of the bidt enables in-depth comparative studies of data disclosure processes, legal frameworks, and cultural settings – most importantly its interdependencies. The project team strives to answer in which way and to what extent do regulatory frameworks and cultural settings shape (or do not shape) data disclosure decisions in different parts of the world. The project team engages not only with different disclosure scenarios, but also puts a special focus on transnational transfer settings. To this end, and in the first half of the project, we have prepared country reports covering the regulatory and cultural dimensions. A general matrix was developed to standardize (and potentially de-bias) our review of different countries. The data disclosure decision (process) was modelled by our information systems string. Furthermore, the first empirical studies were prepared and partly already conducted – gaining *inter alia* insights from a behavioral science perspective.

Against this background, the project team organized – with utmost joy – in June 2022 a "Vectors of Data Disclosure" conference in the wonderful rooms of the Bavarian Academy of Sciences and Humanities in Munich. The conference served two central purposes. First, to present preliminary project results to receive qualified feedback from an interdisciplinary audience. Second, to get impulses from distinguished experts presenting their research – widening our perspectives and laying the ground for an (on-going) exchange of thoughts. Two days we enjoyed in every way – in a stimulating, focused, and open-minded atmosphere. This second volume of the *de Gruyter Global and Comparative Data Law Series* presents the conference proceedings – combining the contributions by our distinguished speakers with our research conducted so far.

First and foremost, we do tremendously thank the authors contributing to this volume. We thank the project team's academic research assistants, Peer Sonnenberg, Veronika Thir, Martin Richthammer, Timo Hoffmann, and Sebastian Kasper, as well as the student research assistants, Nico Göbel, Lukas Illek, Hannah Mösbauer, Thao Phuong Nguyen, and Lorenz von Westerholt, for thoughtfully managing the process – and the burdensome formatting… We also deeply thank Urs

https://doi.org/10.1515/9783111010601-001

Gasser (TUM | Harvard) who supports the project team as an external expert with critical thoughts, innovative ideas, and invaluable advice. Finally, Friederike Buhl and Anna Spendler of de Gruyter deserve our applause for managing the publishing process in a thoughtful and frictionless manner.

Moritz Hennemann Kai von Lewinski Daniela Wawra Thomas Widjaja

Table of Contents

List of Abbreviations

ACCC	Australian Competition and Consumer Commission
ACT	Australian Capital Territory
AHRC	Arts and Humanities Research Council
AI	Artificial Intelligence
ALR	Australian Law Reports
ANPD	(Brazilian) Autoridade Nacional de Proteção de Dados
APEC	Asia-Pacific Economic Cooperation
APPI	(Japanese) Act on the Protection of Personal Information
APPs	Australian Privacy Principles
bidt	Bavarian Research Institute for Digital Transformation
CAC	Cyberspace Administration of China
CCPA	California Consumer Privacy Act
CIGI	Centre for International Governance Innovation
CJEU	Court of Justice of the European Union
CLOUD Act	(US) Clarifying Lawful Overseas Use of Data Act
CLR	Commonwealth Law Report
COPPA	Children Online Privacy Protection Act
CoV	Commonwealth of Virginia
CPRA	California Privacy Rights Act
CPRN	Comparative Privacy Research Network
CSL	(Chinese) Cyber Security Law
Cth	Commonwealth
DPA 2006	(Russian) Data Protection Act
DPA 2012	(Ghanaian) Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSG	(Swiss) Datenschutzgesetz
EDÖB	(Swiss) Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFF	Electronic Frontier Foundation
EStG	(German) Einkommenssteuergesetz
EVS	European Value Study
EWCA Civ	England and Wales Court of Appeal (Civil Division)
FADP	(Swiss) Federal Act on Data Protection
FCAFC	Federal Court of Australia – Full court
FCRA	Fair Credit Reporting Act
FCR	Federal Court Reports
FTC	(US) Federal Trade Commission
GDPR	General Data Protection Regulation
GPLR	Global Privacy Law Review
HCA	High Court of Australia
HIPAA	Health Insurance Portability and Accountability Act
HKLRD	Hong Kong Law Reports and Digest
ICCPR	International Covenant on Civil and Political Rights

https://doi.org/10.1515/9783111010601-002

IDV	Individualism Index
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMD	International Institute for Management Development
IoT	Internet of Things
IRDG	Institut für das Recht der digitalen Gesellschaft
IS	Information System
ITU	International Telecommunication Union
LGPD	(Brazilian) Lei Geral de Proteção de Dados Pessoais
M	Median
MCI	(Brazilian) Marco Civil da Internet
NJW	Neue Juristische Wochenschrift
NRW	Nordrhein-Westfalen
NSW	New South Wales
NSWCA	New South Wales Court of Appeal
NT	Northern Territory
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OAIC	Office of the Australian Information Commissioner
OECD	Organization for Economic Co-operation and Development
OVG	Oberverwaltungsgericht
PDI	Power Distance Indicator
PIPL	Personal Information Protection Law of the People's Republic of China
PPC	(Japanese) Personal Information Protection Commission
Qld	Queensland
RSA	Response Surface Analysis
SA	Southern Australia
SCS	Social Credit System
SD	Standard Deviation
SLR	Structured Literature Review
StGB	(German) Strafgesetzbuch
Tas	Tasmania
TOMs	Technical and Organisational Measures
TUM	Technische Universität München
UA	Uncertainty Avoidance
UAI	Uncertainty Avoidance Index
UNTS	United Nations Treaty Series
U.S.	United States of America
USCOA	United States Court of Appeal
VCDPA	Virginia Consumer Data Protection Act
Vic	Victoria
VSCA	Victoria Court of Appeal
WA	Western Australia
WDCR	World Digital Competitiveness Ranking
WEIRD	Western, educated, industrialized, affluent, and democratic societies
WIPO	World Intellectual Property Organization
WTS	Willingness to share
WVS	World Value Survey

ZD	Zeitschrift für Datenschutz

Timo Hoffmann

The Laws of Data Disclosure

Examining the Regulation of Individuals' Personal Data Disclosure in Brazil, China, the European Union, Ghana, Japan, Russia, Switzerland and the United States of America

Consolidated Report on the basis of the country reports by Timo Hoffmann, Sarah Hünting, Benedikt Leven, Kai von Lewinski, Elisabeth Saponchik, Peer Sonnenberg & Pietro Luigi Pietrobon de Moraes Vargas.

Timo Hoffmann is an academic research assistant at the Chair of European and International Information and Data Law (Prof. Dr. Moritz Hennemann) at the University of Passau, timo.hoffmann@uni-passau.de.

Acknowledgement: The author would like to thank Lukas Illek, Hannah Mösbauer and Niklas Ziegler, all current or former student assistants at the aforementioned chair, for their assistance in compiling the material for this conribution.

https://doi.org/10.1515/9783111010601-003

Introduction

I The Legal Vectors of Data Disclosure

The research project "Vectors of Data Disclosure"[1] aims to examine various aspects of individuals' disclosure of their personal data from an interdisciplinary, interna-

1 The full title of our interdisciplinary research project is *Vectors of Data Disclosure – A comparative study of the use of personal data from a legal, cultural studies, and information systems per-*

tional perspective. Looking at regulatory, cultural and behavioral elements, the project aims to examine the various factors influencing individuals when deciding on whether to share their data with recipients. By examining these factors, the research project hopes to give concrete (policy) recommendations to stakeholders and legislators, support companies in conceiving data-based business models, and contribute to global cooperation, coordination and harmonization in the area of data and information law and regulation.

Within the research project, the group focusing on legal research focused on identifying different legal "vectors" that may possibly influence individuals' data disclosure decisions. In a first step, the objective was to analyze different jurisdictions' laws relevant for individual data disclosure in order. Within the greater project, the identification and description of various provisions relevant for individual data disclosure was a necessary step, allowing further research on the influence such provisions may have on individual decision-making in different countries and in different cultural environments. For this, eight country reports were created, focusing on the various *Laws of Data Disclosure* around the world.[2] This contribution is a summary of these eight reports.[3]

II Research Design

Within the research project, one of the first steps was to select the eight countries / jurisdictions to be examined. The aim was to achieve a widely spread representation of regions around the globe, restricting the scope to a manageable number of jurisdictions (eight) while allowing for diversity, explicitly focusing on the inclusion of nations in the global south. The aim of achieving diversity is related especially to the interdisciplinarity of the greater research project, as in cultural studies, greater differences likely allow for more noticeable differences in empirical analysis

spective. It is funded by the Bavarian Research Institute for Digital Transformation (<https://www.bidt.digital/> accessed 07.02.2023). Lead principal investigator: Moritz Hennemann; further principal investigators: Kai von Lewinski, Daniela Wawra, and Thomas Widjaja; external expert: Urs Gasser.

2 Eight parallel reports on *Cultural Influences on Personal Data Disclosure Decisions* were created by the group focusing on cultural studies research, examining individuals' perceptions of privacy and related issues concerning decisions to disclose personal data. All legal and cultural reports are available at Institut für das Recht der digitalen Gesellschaft, 'Research Paper Series – Universität Passau' <https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/> accessed 07.02.2023.

3 The presentation held by the author of this contribution at the conference "Vectors of Data Disclosure" was an early version of the summary presented here.

and thus also make the drawing of conclusions easier. The jurisdictions selected were Brazil, China, the European Union, Ghana, Japan, Russia, Switzerland, and the United States of America. Of these jurisdictions, the European Union stands out as the only non-nation state – nonetheless, the EU was selected due to the relevant laws on data protection, particularly with the GDPR, existing primarily on the EU level, rather than on that of the individual member states. Where legislation was not on the EU level, Germany was examined. In the cultural studies reports, the focus of observation was also Germany. Thus, the jurisdiction/country examined might be more properly described as "EU/Germany".

The general approach to examining the individual jurisdictions' laws relevant for personal data disclosure has its roots in classical methods of comparative law, which divides the act of comparison into descriptive country report and the comparative evaluation.[4] In line with this method, the aim was to craft such descriptive country reports.

In order to allow for a certain degree of homogeneity, a detailed report structure was established, looking at various aspects of legal systems, from a broad view of the legal system in general to more detailed individual provisions, in an iterative approach including interdisciplinary feedback from the business information systems and cultural studies research groups. The report structure was then used as the outline for the country reports, and consisted of section and subsection titles as well as keywords showing the intended meaning of the examination. This report structure was then disseminated between the authors of the country reports, who researched and wrote the reports. After the writing of the reports, an internal review process followed, incorporating interdisciplinary feedback as well as input from legal experts well-versed in the examined jurisdictions.

III How to Read this Report

This report is a summary of eight different legal country reports on the matter of law concerning individuals' disclosure of personal data, each focusing on a different country or jurisdiction, these being Ghana,[5] Japan,[6] Germany/the European

4 See Uwe Kischel, *Rechtsvergleichung* (C.H. Beck 2015) 119.

5 Timo Hoffmann, 'Data Protection Act(ion): Report on the Law of Data Disclosure in Ghana' (2022) 22(01) <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/IRDG_Research_paper_Series_Country_Report_Ghana_Final.pdf> accessed 07.02.2023.

6 Timo Hoffmann, 'Data Protection by Definition: Report on the Law of Data Disclosure in Japan' (2022) 22(03) <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/

Union,[7] Brazil,[8] the United States of America,[9] Russia,[10] China[11] and Switzerland.[12] Together, they compose over 200 pages of detailed analysis of various legal provisions relevant for the act of individual disclosure of personal data.[13]

The aim of this contribution is to provide a reasonably concise summary of these reports. To this end, particular attention is paid to highlighting provisions or rules that are generally similar to one another on one hand, while showing notable divergences from the standard on the other hand. In order to mirror the content of the reports, this summary replicates the structure of the individual country reports, beginning with 'Generalities',[14] concerning the overall political and legal environment shaping regulation of individuals' disclosure of personal data, before moving to 'Information Regulation in General',[15] which broadly deals with aspects of information regulation from a more general perspective, before examining 'Regulations Concerning Disclosure of Personal Data'.[16] In accordance with the titles, the sections move from a highly abstract view to a more detailed perspective on

Research_Paper_Series/Hoffmann_Data_Disclosure_Japan_Data_Protection_by_Definition.pdf> accessed 07.02.2023.

7 Kai von Lewinski, 'Informational Gold Standard and Digital Tare Weight: Country Report on Data Disclosure in the European Union' (2022) 22(05) <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/von_Lewinski_EU_L%C3%A4nderbericht_23.03.2022.pdf> accessed 07.02.2023.

8 Timo Hoffmann and Pietrobon de Moraes Vargas, Pietro Luigi, 'LGPD Et Al.: Report on the Law of Data Disclosure in Brazil' (2022) 22(06) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-06.pdf> accessed 07.02.2023.

9 Benedikt Leven, 'Land of the Free: Legal Country Report on the United States of America' (2022) 22(12) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-12.pdf> accessed 07.02.2023.

10 Elisabeth Saponchik, 'Digital Citadel – Country Report on Russia' (2022) 22(13) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-13.pdf> accessed 07.02.2023.

11 Sarah L Hünting, 'Endeavour to contain Chinas' Tech Giants: Country Report on China' (2022) 22(15) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22_15.pdf> accessed 07.02.2023.

12 Peer Sonnenberg and Timo Hoffmann, 'Data Protection Revisited: Report on the Law of Data Disclosure in Switzerland' (2022) 22(17) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22_17.pdf> accessed 07.02.2023.

13 All available at Institut für das Recht der digitalen Gesellschaft (n 2).

14 See *infra,* A.

15 See *infra,* B.

16 See *infra,* C.

individual rules. As a consequence, the last section is both the most extensive and detailed section, composed of numerous subsections about different aspects of personal data disclosure regulation.

For the sake of readability, this report omits most citations present in the foundational eight country reports as well as citations of the country reports themselves. However, due to the reports having a structure identical to this report, further references are readily available through going to the corresponding section in the individual country report. Readers wishing to gain a perspective of the various jurisdictions in full detail should thus read this summary in conjunction with the individual country reports cited above.

This report is thus to be seen as a more abstract summary of the jurisdictions analyzed, together with a summarizing comparison focusing especially on con- and divergence in internationally different approaches to the regulation of individuals disclosure of their personal data. In each section and sub-section, a brief explanation of its focus will occur, followed by an overview of the research results, together with a short analysis of notable aspects.

A Generalities

I Cultural Vectors of Data Disclosure

Section A-I concerns itself with the general preconditions for the regulation of personal data and informational issues in the different jurisdictions, including cultural preconditions, parameters and narratives concerning individual data disclosure, and the discourse on data protection and privacy, including calls for reform.

In this regard, several observations could be made. First of all, there is a certain divide between jurisdictions with a long-standing history of data protection: this includes most notably the EU and Germany, as well as Switzerland to a certain extent. Japan also has a long history of the personal information and the law, with privacy recognized by courts early on. On the other hand, discourse and legislation concerning data protection in Brazil, China, Russia and Ghana are comparatively recent. The United States occupy a somewhat special position, as they were quite involved in the early phase of discourse on privacy,[17] going back to the 1890s,[18] with respect to academic debate, and the 1960's and 1970's concerning leg-

17 The term data protection is not particularly common within the United States.

18 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193.

islative initiative. Despite this, the United States remains the only jurisdiction examined not to have a comprehensive data protection or privacy law framework – however, it has some strong sectoral regulations, as in the area of healthcare privacy.

Another divide can be found in relation to economic development. Of the countries examined, particularly Ghana, and, to a lesser extent, Brazil, suffer from relatively less development as well as high inequality.[19]

The notions of issues of data protection and privacy also diverge between the examined countries and jurisdictions. In general, some countries have a more individualist focus regarding privacy and data protection, such as United States as well as the EU/Germany and Switzerland, with different nuances in discourse. Some countries focus strongly on the economic usage of data, bringing a more commercial outlook to the table, such as Switzerland, Japan, and the United States. The Chinese approach is notable for its collectivist outlook, with data protection and privacy regulation focused on private companies, but does not focus on government activity. Similarly, the Russian discourse on personal data use is influenced by the post-Soviet experience, leading to a high level of mutual distrust in society, but technological developments are seen relatively uncritically. The Brazilian discourse was influenced by problematic practices of personal data use. In Ghana, data protection is still not a widespread phenomenon, but rapid technological advances, particularly concerning mobile payments, may change this.

Concerning cross-border influence on legislation dealing with personal data, the most relevant player that may be identified is the European Union: Swiss data protection law is notably influenced by requirements put forth in international agreements between Switzerland and the EU, Japanese data protection law was reformed in order to obtain an EU adequacy decision, and the Brazilian, Ghanaian as well as Russian laws on data protection laws resemble, to varying degrees, the EU's GDPR[20] or its predecessor, the Data Protection Directive.[21] Other laws, however, have not been recognizable as international templates.

19 The country report on Russia was largely completed before the 2022 Russian invasion of Ukraine and does therefore not address the possibly significant changes in economic capability.
20 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L119, 1–88.
21 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, 31–50.

II Legal System and Lawmaking

Section A-II includes an overview of the central characteristics of the respective legal systems. Included in the analysis are the relevant sources of law, legal hierarchies, the classification of the legal systems as belonging to certain spheres, but also the nature of lawmakers and influential societal movements. Among these characteristics, a significant difference can be seen in the form of government, with the United States, Switzerland, Ghana, Germany, Brazil and Japan being democratically governed as opposed to authoritarian regimes in Russia and China. As opposed to the others examined, the EU is not a nation-state, but rather a supranational organization with regulatory capacities superseding the law of the member states in certain areas.

All of the countries examined have a legal system based on a written constitution and a formalized legislative process, with Switzerland forming an outlier due to its many elements of direct democracy. In this regard, Ghana is notable, as its constitution explicitly acknowledges customary law, for the development of which the National House of Chiefs is responsible. China, on the other side, is notable for its often-diffuse multi-level system of law and a wide range of sub-law administrative provisions, which may significantly diverge while nominally being in force in parallel to one another, and which are interpreted by the government in a flexible manner tailored to the needs of the situation, as well as by case law, which resolves some incompatibilities. A commonality in the countries examined is the presence of constitutionalized fundamental rights – however, the actual observance of the rights is markedly different in the authoritarian countries: in China, public (government) interest is seen to generally supersede individual fundamental rights, and these are often not enforced. In Russia, fundamental rights exist in law, but are often failed to be applied by the courts in practice – further, the exit from the Council of Europe following the Russian invasion of Ukraine has had impact on individual rights arising from international law.

Concerning international influences, Western European and American influences can be seen in several countries. This includes the influence of English common law on Ghana, a former colony, but also a variety of continental European influences such as Portuguese, French, Italian, German, but also that of the United States, in Brazil. Similarly, Japanese law was historically influenced by French and German law, but also, especially regarding the constitution, that of the United States. Russian law is part of the broader Romano-Germanic tradition. Swiss law is characterized by a variety of French, Italian and, especially, German influences, and more recently closely linked to legislative developments in the EU. EU law is influenced by a blend of different member state traditions.

The examined jurisdictions also differ in regard to varying degrees of federalism or centralization. Switzerland and the United States have particularly pronounced powers of the cantons/states, while different degrees of federalism are present in Brazil, China, Germany and Russia. Ghana and Japan, on the other hand, are comparatively more centralized.

Significant differences also exist with regard to the cultures of legal dispute: While Brazil is notable for the exceptional litigiousness of its people, Japan is the opposite, with litigation and adversarial legal action comparatively rare when compared to countries with similarly-sized economies.

B (General) Legal System of Information Law

I Structure of Information Law

Section B-I of the country reports deals with the general structure of information-related laws, focusing on the prevalence of relevant constitutional and basic rights, but also on the regulatory structure concerning informational issues such as intellectual property protections, secrecy and cybercrime, focusing also on the question of relevance of international law provisions in these areas.

In most examined countries, informational provisions are entrenched in or at least derived from the respective constitution: this is the case in Russia, Brazil, Ghana, the EU, Switzerland, China,[22] and Japan. In the United States context, one should note the overturning of *Roe v Wade*[23] which could have great effects due to its doctrinal reliance on the recognition of a right to privacy as existent in the US Constitution.[24] Besides constitutional protections for informational aspects, all examined countries have dedicated intellectual property laws, which are highly homogenous internationally due to numerous international treaties and membership in relevant international organizations. All countries have some form of provisions concerning cybersecurity or cybercrime, as well as multiple individual laws dealing with different forms of informational issues. Common are also forms of laws mandating individuals' access to government-held information, such as in

22 However, consider that the report on China mentions that "enshrinement in constitutional law would not grant effective and individually enforceable protection."

23 Note that our report on the United States was finalized prior to this.

24 Jack Morse, 'Americans' privacy threatened by Supreme Court's Roe decision, experts say' *Mashable* (24 June 2022) <https://mashable.com/article/supreme-court-roe-wade-digital-privacy> accessed 07.02.2023.

Brazil and the United States. Authoritarian influences show: in Russia, extensive restrictions of the right to freedom of expression exist by means of content blocking, and in China, tight censorship is ubiquitous. However, the United States are also notable with regard to sweeping powers of surveillance for the sake of national security.

II Allocation of Informational Legal Positions

In B-II, the country reports examine the question of commoditization of informational legal positions, particularly with regard to intellectual property, but also other forms of declaring certain types of informational positions to be individually or collectively held.

Concerning intellectual property positions such as patents and trademarks, there is an impressive level of homogeneity between all countries, which is likely due to detailed international treaties and the aspiration towards cross-border compatibility. Some countries diverge from the standard mode of regulation by implementing additional categories of protection, such as Brazil with a special copyright law concerning software, providing for rights with regard to computer applications, and Japan, where certain forms of "big data" are protected under competition law. A notable feature mentioned in the Brazilian report is that of *habeas data*, a right of access to publicly held data about an individual, which is common within South American countries.[25]

In some countries, intellectual property rights are approached with a certain level of protectionism: China requires a "confidentiality examination" for inventions developed in China regarding applications for patents abroad.

Notable for its non-existence in any of the examined jurisdictions is *data ownership* or property rights to personal data not stored physically: while many countries know legal positions including rights to peoples' "own" personal data, data ownership is not amongst them.

25 See for example Marc-Tizoc Gonzalez, 'Habeas Data: Comparative Constitutional Interventions from Latin America against Neoliberal States of Insecurity and Surveillance' (2015) 90(2) Chicago-Kent Law Review 641.

III Institutions

This section deals with the institutions involved in the information regulatory environment in the different jurisdictions examined. Relevant institutions identified include intellectual property regulatory authorities, communication authorities, consumer protection facilities, data protection supervisors, civil society actors or non-governmental organizations (NGOs) concerned with the development of the legal framework, and cyber security authorities. In most countries, there is a wide variety of such organizations. Due to the complexity and multi-level nature of the information regulatory framework in all countries, the result in most is a plural system built of a multitude of different institutions. Amongst these, particularly Brazil and the EU are notable for the large number of active civil society organizations, reflecting the size of the jurisdictions on one hand and the intensity of the discourse on the matter on the other, while in Russia, relevant NGOs face significant persecution. In most countries, antitrust regulators are separate from regulators responsible for matters of information – however, in the US, the Federal Trade Commission (FTC) combines both. In Russia, contrary to the multitude of government agencies responsible elsewhere, there exists a significant institutional monism with *Roskomnadzor*, which is responsible for numerous different avenues of enforcement.

International organizations relevant across the board include the World Trade Organization (WTO), World Intellectual Property Organization (WIPO), and the Organization for Economic Co-operation and Development (OECD). In the area of data protection, several countries have connections to the Council of Europe's Convention 108.

IV Procedural Aspects

As part of the section on information regulation in general, this section looks at the different methods employed for control and enforcement in the various jurisdictions. Frequently, there are three types of enforcement – civil, administrative and criminal. Despite this general theme, some differences emerge between the examined jurisdictions.

Some notable aspects include the following: In Brazil, there exist strong possibilities of collective litigation, with litigation through the Public Ministries, a public organization that is a specialty of the Brazilian institutional setup, which may litigate in favor of collective interest, an additional building block. Similarly, collective litigation in the form of class action lawsuits play an important role in the US in certain contexts; another notability in the US is the existence of the instru-

ment of *amicus curiae*, where third parties can be included in litigation where they demonstrate a plausibly infringed interest. In China, there exist certain shaming mechanisms such as a "list of dishonest persons" – on the other hand, there is a severe lack of enforcement in some areas, especially in the realm of intellectual property. Within the EU, enforcement diverges between member states – however, the Court of Justice of the European Union (CJEU) has significant influence but may in most situations act only "on request" of national courts. In Japan, enforcement greatly relies on administrative authorities – these however often take a cooperative approach, working together with addressees rather than administering fines or similar. In Switzerland, administrative enforcement has thus far not played a primary role, with civil litigation being more prominent.

C Regulations Concerning Disclosure of Personal Data

The third main section of the report is again divided into several subsections, dealing with various areas of regulation, and again moving from more general points at the beginning to a more detailed discussion of certain regulatory instruments. Section C thus begins with a discussion on the "legal structure of data disclosure" in subsection I, before examining the "concepts and terms for such data" (II), which looks at the objects and parties subject to regulation, before moving to the legal "relationship between discloser and recipient" (III), and finishing with "objective legal obligations of the recipient" (IV), which are not dependent on a multi-party relationship. Of these subsections, subsections III and IV are the most detailed, containing two levels of subsections of their own. With this focus on the general structure and questions of applicability and general terminology in the beginning, followed by a detailed report on the individual measures in place, the country reports aimed to give a detailed picture of the legal situation in the entire process of individuals' disclosure of their personal data in all eight jurisdictions.

I Legal Structure of Data Disclosure

In the section on the legal structure of data disclosure, the reports focus on whether data protection laws or similar were present and in what form. This includes assessments of the outer form of regulation (constitutional protections, codified laws, self-regulation, *inter alia*) as well as of the general mode of regulation, including the degree of preventive prohibition of data processing, the question of privi-

leged areas possibly exempt, and the question of risk-orientation of the individual frameworks.

In this examination, the first core finding is that, with the exception of the US, all examined jurisdictions had a comprehensive data protection law of some kind addressing the processing of personal data of individuals. Switzerland is currently in the process of revising its core data protection law: the new *Datenschutzgesetz* (DSG[26]) was passed in 2020 and is expected to enter into force in September 2023 – the country report examines both the old and new DSG and contrasts them. In the United States, some states have passed laws similar in scope to such comprehensive data protection laws – on the federal level, there currently exist only sectoral regulations, such as in the areas of healthcare or financial services.

In addition to such general data protection laws, civil code / civil law protections of personal data and privacy allowing for the seeking of damages are very common, if different in concrete scope, existing in most jurisdictions examined. Despite these similarities of legislation in principle, there exist significant differences regarding mode and intensity of enforcement. Furthermore, there are strong differences as to whether governments and public authorities are bound by data protection legislation, as well as to the extent of territorial and extraterritorial scope of the laws. Constitutional or constitutional-derived fundamental rights to data protection or privacy were also very common.

The laws examined often have a similar structure to the European GDPR, most pronouncedly in Brazil, and often replicated general concepts from the GDPR or its predecessor, the Data Protection Directive, which supports the concept of the "Brussels Effect" as discussed in literature.[27] Of the examined laws, those of Brazil, the EU, Ghana and Russia are based on the legislative style of a preventive ban of data processing subject to permission, either by consent or other valid reasons for processing, often enumerated explicitly in the law. The Swiss approach stopped short of this, requiring a valid reason for processing only where the processing reached the threshold of a possible violation of an individual's personality. Other countries, such as Japan, took a more nuanced approach, requiring consent or another reason for processing only in certain circumstances.

Among notable regulatory instruments are the social credit system in China, which has, however not been codified thus far and is still fragmented, and a criminal ban of the purchase or sale of personal data in Ghana. The Japanese approach,

26 In order to avoid confusion with other laws, we chose not to abbreviate the Swiss Federal Act on Data Protection (FADP) in English in this contribution.

27 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020); see also Moritz Hennemann, 'Wettbewerb der Datenschutzrechtsordnungen' (2020) 84(4) RabelsZ 864.

in the Act on the Protection of Personal Information (APPI), stands out through its differentiation of different types of personal data by degree of individual identifiability with matching variation in intensity of regulatory obligation, while the Swiss approach is notable for its strong conceptual focus on the individual right to personality. Russian law on personal data contains strong data localization provisions, which mandate the keeping of personal data of Russian citizens within Russia. In the US, owing to the lack of a comprehensive data protection or data privacy law, the focus of enforcement has thus far been on violations of competition law.

II Notions

1 Personal Data as Object of Protection

In this subsection, the reports look at the concept of personal data or other categories of data / information, where terminology varied. The reports found that, while the terms describing personal data vary ("personal information" is often used), there is strong convergence in the general definition: common is the description of such as information or data about (related to) an identified or identifiable natural person. In all definitions examined, the possibility of individual identification is decisive for the classification as personal data. Thus, anonymous data (from the beginning or rendered such *ex post*) is considered outside the scope of application in most countries. This is slightly different in Japan, where certain types of (partially) anonymized personal data are subject to certain protections (lighter in intensity when compared to directly identifiable personal data). However, the foundational elements of this definition, the words data or information, are not often clearly defined. In China, the interpretation is found to be very contextual.

Another identified commonality in the jurisdictions examined is the presence of a legal category for personal data deemed especially sensitive, deemed "sensitive data" or "special personal data" (Ghana). This type of personal data typically includes personal data relating to health, religion or political views of the individual concerned, but varied considerably in its concrete scope amongst the examined jurisdictions.[28] In the US, this concept varies considerably between states or is not defined at all in others. The US also stands out for its conceptual focus on the notion of "privacy" rather than "protection of personal data", which is a slightly different, and sometimes vaguer, sometimes broader concept.

28 See on data sensitivity Daniela Wawra, in this volume, at 169, 172 et seqq.

2 Attribution of Data to a Person

Beyond the definition of personal data in the previous subsection, this subsection focuses on the manner of attribution linking individual persons to the protected data. In the definition of personal data, such attribution is usually by personal reference, often phrased as being "about" a person. This is not the case in the US, at least on the federal level, due to the lack of a federal law establishing the concept of a data subject or similar. Furthermore, there is no "property" attribution in the form of "data property" in any of the examined jurisdictions. The concept of *titularidade* of personal data in Art. 17 of the Brazilian *Lei Geral de Proteção de Dados* (LGPD) only provides for moral rights of the data subject, not full ownership, similar to a civil law protection of personality. Commonly problematic, as not addressed by legislation, is the problem of multi-referential data referring to more than one individual. In Japan and Russia, the degree of protection differs between citizens and foreign nationals – in Japan, this is due to the supplementary rules implemented in order to obtain an EU adequacy decision, which requires stricter standards for data originating from persons in the EU. In Russia, this takes the form of data localization obligations for those who process personal data, which only applies in relation to Russian citizens. Another specialty of Russian law is the protection of deceased persons' data: in this case, heirs are responsible where consent is needed. Similarly, in China, under Art. 49 of the Personal Information Protection Law (PIPL), the "next of kin" is allowed to exercise rights on behalf of the deceased.

Generally, only natural persons were subject to protection under the definition of personal data. The only exception to this is the case of the protection of legal persons in the current Swiss data protection law, the DSG, with roots in the traditional perspective that legal entities can have a certain "commercial honor" which should also entitle them to data protection rights. However, this peculiarity is set to be eliminated with the overhaul of the DSG.

3 Reception and Recipients

After establishing the "what" and "who" regarding the notion of personal data relevant for individuals' disclosure of personal data in the preceding two subsections, this subsection deals with the person of the recipient, understood in our report as the party receiving the personal data disclosed by an individual. For this purpose, the report paid attention to the legal relevance of different categories of such recipients of personal data, and points of differentiation such as that between recipients and third parties, and local and international reception of personal data.

In this context, there is again a great degree of convergence on the level of the overarching concepts, with almost all jurisdictions, such as the EU, Brazil, Ghana, Japan, Russia and Switzerland differentiating between a form of "controller", the party responsible for the reception / processing of the disclosed personal data, and a form of "processor", a third party responsible for processing such personal data for a controller.

There are commonly categories of recipients given privileged status, such as natural persons for private, non-economic purposes, journalism, art, health, etc., but also public agencies for the sake of public/national security, amongst others.

Fairly common are some forms of differentiation between company size or volume of data processing, typically in form of laxer requirements for small companies, which was the case in some form in countries such as Brazil, China and Switzerland.

There are very commonly stricter requirements for the transfer to foreign, or in the case of the EU, *third* countries, requiring some form of "adequacy", be it in the narrow sense of adequacy agreements in the EU context or with vaguer requirements concerning standards of data protection in the target country, as in Ghana or Switzerland.

The public is not considered a *recipient* in the structure of the different data protection laws. However, publicly available personal data is often less strictly dealt with legally, as in Brazil, the EU, Ghana or Switzerland, albeit in different forms, sometimes dependent on whether the personal data was originally made public voluntarily.

III Relationship between Discloser and Recipient

1 Provisions for Disclosure

In this subsection, the country reports examine the general provisions for the disclosure of individuals' personal data in the relationship between the individual and the party to whom such data is disclosed, giving an overview of the relevant legal provisions.

A notable finding is that many countries have adapted the concept of the "right to informational self-determination" or an equivalent right: this was found to be the case within the EU, at least in the case of Germany, Brazil and Switzerland – in the US, the concept of "informational autonomy" can be identified. Regarding

commercialization of personal data, it is notable that the laws examined did not include provisions explicitly promoting the commercialization of personal data.[29]

In Brazil, the LGPD, as a comprehensive data protection law, formed the main framework for the regulation of situations where individuals disclose their personal data. Similarly, the EU had the GDPR as an overarching data protection law – however, while it formed the only comprehensive law concerning data disclosure or data sharing, this will change in the form of various pieces of legislation concerning data currently still on their way. In China, the situation was more fragmented, with various different provisions on multiple levels of the legal hierarchy addressing data disclosure alongside the Personal Information Protection Law (PIPL). Ghana, Japan, Russia and Switzerland also had a comprehensive data protection law applicable in situations of data disclosure. Generally speaking, individuals' disclosure of their personal data was considered "processing" of personal data in all the aforementioned jurisdictions.

The US, at least on the federal level, stood out due to its lack of a comprehensive data protection law – leading to a wide freedom of action with few legal restrictions concerning such acts of disclosure.

a Prohibited Disclosures

This subsection addresses provisions relevant for data disclosure in the form of prohibitions of disclosing certain kinds of personal data, such as protections of secrecy.

In this, the first finding is that, in all examined jurisdictions, individuals were generally free to disclose their data in whatever manner they would like. However, some types of data are commonly subject to prohibitions, with secrecy provisions of various types, such as for (legal) professionals, data relating to trade secrets, banking secrecy and contractual secrecy provisions (commonly known as non-disclosure agreements, or NDAs). A frequent exception from such disclosure prohibitions are provisions aiming at the protection of whistle-blowers – individuals exposing misconduct, usually from within companies or organizations.

Notable provisions included the Japanese prohibition of "handling" of "specially designated secrets" designated such by the state, and the high degree of protection of banking secrecy in Switzerland.

---

29 Regarding monetization of personal data under Californian law, see Lothar Determann, in this volume, at 21, 124 et seqq.

b Disclosure Obligations

Mirroring disclosure prohibitions, the following subsection in the country reports looks at obligations for individuals to disclose their personal data.

Such obligations are particularly common in form of obligations to declare one's income for tax purposes, in the context of commercial registers, ie, for company ownership, and public identification registries, which contained information such as civil status or residence. Such registries of residence exist in various forms, such as the "Hukou" system in China, which was formerly used for migration control.

Obligations to disclose personal data also exist in the context of compliance duties, for example in the form of identification requirements when opening a bank account for the prevention of fraud.

c Voluntary Disclosure/Voluntariness

This subsection looks at the question of volition, examining how the various laws deal with enabling individual decision-making in the context of personal data disclosure situations. To this end, the subsection also looks at the qualification of dependency and hierarchy contexts, the possibility of voluntary commercialization, and incentives to the disclosure of personal data and provisions aiming to protect individuals in such situations.

The most common legal building block for this is the requirement of individual consent for the processing of personal data in certain situations. Most commonly, consent is one of the default bases allowing the processing of personal data by a recipient/controller: this is the case in Brazil, the EU, Japan, Switzerland, and Russia. However, the degree of detail in the elaboration of the concept varies highly, with only some jurisdictions giving more precise requirements for (legally valid) consent.

A provision protecting individuals' ability to decide on individual aspects of disclosure can be found with prohibitions of "coupling", the requiring of unnecessary provision of personal data for unrelated services: this exists in the EU, Brazil (in contractual contexts) and, for specific contexts, in Switzerland. Frequent are special provisions for consent in unequal constellations, particularly in employment relationships and for the protection of minors and adolescents.

In China, the social credit system, through incentives, on the contrary encourages the sharing of additional data voluntarily.

2 Recipient Obligations

This subsection deals with regulatory requirements from the perspective of the party receiving personal data from an individual, or "recipient" in the terminology we use. This subsection is divided into two parts – the first dealing with obligations preceding the act of data disclosure, the second for handling personal data after reception from the disclosing individual.

a Requirements for Personal Data Reception

In this part of the section on recipient obligations, the country reports look at requirements preceding the act of data disclosure, such as information requirements, formal requirements to be observed, as well as other necessary warnings or assurances.

Generally, the focus of regulation is on such obligations for the recipient of individuals' personal data. Most prominent are regulatory requirements mandating some form of purpose limitation, whereby those processing personal data must restrict their use of the data to certain, mostly pre-determined purposes, as well as information requirements. This requires those processing received personal data to determine such purposes before reception rather than deciding what to do with data after it has been received. Information requirements are commonly necessitated – however, there are significant differences regarding the mode of information, particularly in the question as to how actively individuals must be informed. For example, in Japan, certain information needs only to be "made available to the public" rather than explicitly be shown to the individual affected.

Common contents of information requirements are details about purpose and duration of processing, the legal rights of individuals and information about how to exercise such rights, as well as the contact information of the company or the responsible officer.

Informational requirements in the form of privacy policies or notices, especially on websites, are one of the areas where the US has concrete requirements for those processing data despite its lack of overarching data protection laws.

b (Procedural) Obligations Concerning the Handling of Received Personal Data

This part in the country reports deals with the handling of personal data after reception, including technological and organizational measures, the handling of deletion and retention of such data, as well as rules for the further transmission of personal data received.

Again, broad international convergence can be found with forms of purpose limitation, which restricts the use of the personal data received to certain purposes

formulated before reception. In case of a change in purpose after reception, there are commonly additional requirements, such as the need to obtain consent, as was the case in Japan.

A common feature in data protection laws is the statement of enumerated principles guiding the use of personal data altogether – this is the case in Brazil, the EU, Ghana, Russia, and Switzerland, perhaps unsurprisingly the jurisdictions comprised of or inspired by EU-style data protection legislation.

Very interesting differences were identified when examining the allowed time period for retention of personal data and obligations for deletion. Explicit deletion requirements for personal data after the purposes for the use of the data have been fulfilled exist in Brazil, the EU, Ghana, Japan, and Switzerland. In Brazil, Ghana, Japan and Switzerland, anonymization is explicitly allowed as an alternative to deletion. Whether this is allowed in the EU is a contentious matter.[30] Such deletion requirements are, however, often mirrored by retention requirements for certain personal data, such as in Brazil, where the Marco Civil da Internet (MCI) requires certain collection logs and internet application logs to be kept by internet providers. This is similar in Russia, where law enforcement access is still more pronounced, and in China, where cybersecurity legislation includes monitoring requirements.

Very common are restrictions to the onward transferal of obtained personal data, especially where such personal data is to be transferred abroad, sometimes requiring specific consent, such as in Russia, or, for the transfer of medical information, in the US.

3 Control by Discloser

This subsection deals with elements conferring possibilities of control to individuals disclosing their personal data. It is divided into a part on (rights to obtain) transparency and information, provisions ensuring individuals' co-determination in the usage of their personal data, and provisions dealing with *ex post* revocation of authorization of the processing of personal data received from individuals disclosing their personal data to the recipient, followed by a section on procedural aspects for the exercise of associated rights.

30 Alexander Roßnagel, 'Datenlöschung und Anonymisierung: Verhältnis der beiden Datenschutzinstrumente nach DS-GVO' [2021] ZD (Zeitschrift für Datenschutz) 188.

a Transparency and Entitlement to Information

Rights to obtain information or transparency are common: in this regard, there is often a two-part approach: general rights to information or information requirements creating obligations to inform individuals about how their personal data is processed, and rights allowing individuals to request access to or obtain a copy of their data as processed by the recipient.

Some notable provisions in the area of transparency and information include the existence of "naming and shaming" as an administrative sanction in Brazil, possibly allowing individuals to avoid recipients with a history of noncompliance with the law. Further such provisions can be found in general requirements that network operators publicize the "rules for collection" in China under the Cyber Security Law or in the publicly available data protection register in Ghana, where individuals can check whether the recipient is properly registered with the supervisory authority. In Switzerland, certain public and private collections of personal data must be registered to be made public by the supervisory authority. Further, in California, in the US, consumers are granted a right to access information collected about them in the last 12 months, including the purposes for the collection.

b Co-Determination and Co-Decision Concerning Data Use

This part of the country reports deals with regulatory instruments aiming at allowing control over the processing of their personal data by the affected individuals. In summary, the most common ways of ensuring this are provisions requiring consent for certain acts of processing personal data, provisions allowing revocation of consent or ex-post deletion, and rights aiming at the correction of faulty data held about the data subjects.

Among the examined jurisdictions, the revocation of consent or *ex-post* deletion requests aiming at stopping processing that was previously lawful does not exist in Ghana, Japan, China, and, due to the lack of a law, on the federal level of the US. In Japan, a right to request the cease of the use of the data or deletion exists where the original purpose for processing is not adhered to or in case the recipient uses "deceit" or "improper means". This is similar in Brazil, where data subjects can request deletion or anonymization in case of non-compliance with the law.[31] A right to correction of personal data containing errors exists in Brazil, the EU, Ghana, Japan, and Russia.

---

31 See the following section in the Brazilian country report on "revocation" for information on this right.

c Revocation

This part examines more explicitly control rights relevant at the end of the data life cycle, including rights to deletion, data portability, and rights "to be forgotten".

Such a right to be forgotten exists in some form in the EU, Japan, and Switzerland. In Russia, it is limited to rights vis-à-vis internet search engines concerning the deletion of links from search results. In Japan, such a right must be balanced with society's "right to know".[32] In Brazil, such a right has so far not been recognized – however, case law by the Supreme Court suggests it may be recognized in the future. In China, a court decision on the matter has so far yielded the result that there is no such right to be forgotten under Chinese law.

Rights to data portability, understood as a right to request a transfer of the personal data held by a controller to either a third party or the individual, are also common, existing in Brazil, China and the EU. In Switzerland, such a right is poised to become law with the revision of the DSG in the near future, albeit limited to personal data originally disclosed to the recipient by the data subject. In Brazil, anonymized data is explicitly excluded from the scope of data portability. In the US, the California Consumer Privacy Act (CCPA), for example,[33] also recognizes a right to data portability, but no such right exists on the federal level.

d Procedural Aspects

Among other procedural aspects regarding control rights, such as whether requests are to be made in writing, the most notable differences were provisions determining the question of whether individuals may be charged fees for controllers' costs for complying with requests. In Brazil, the EU, Russia and Switzerland, the exercise of subject rights must generally be free of charge. In Japan, fees must be "within a range recognized as reasonable considering actual expenses", while in Ghana, the right to confirmation of whether personal data about an individual held must be done "at reasonable cost".

4 Enforcement

In this subsection, in accordance with the general structure of the country reports, they examine the question of enforcement of rights within the relationship disclo-

32 See in particular Frederike Zufall, 'Challenging the EU's 'Right to Be Forgotten'? Society's 'Right to Know' in Japan' (2019) 5(1) European Data Protection Law Review 17.

33 More recently, a right to data portability was also introduced in Colorado, see § 6–1–1306 (1) (e) Colorado Privacy Act.

ser-recipient. As the greater section deals with this relationship, enforcement by authorities can be found in the part on enforcement in the section on objective legal obligations.[34] This subsection is split into an examination of the modality of obtaining damages and compensation and the relevant procedural aspects.

a Damages and Compensation

Concerning civil liability for misconduct, obtaining damages is possible in all examined jurisdictions. In this context, provisions allowing such are often based in the specific data protection law itself, but also commonly grounded in tort law more generally as compensation for the violation of personality or privacy rights. A core problem in obtaining damages is often the difficulty of quantifying damages, be they material or immaterial, as the real damage to an individual whose personal data has been misused is hard to grasp. In Russia, damages granted are often very low, with sums awarded reaching low single-figure Euro amounts, and are often redacted from court records when granted, making a systematic analysis difficult.

Generally, the examined provisions allowed for the recovery of both material and immaterial damages: this was explicitly stated in the data protection laws of Brazil, the EU, Ghana (through a provision referencing "compensation for distress"), and Russia. In China, Japan, Switzerland, and the US, compensation or damages are not founded in data protection law, but based on the respective civil code or tort law. Most jurisdictions examined allow only for the granting of compensatory damages. The US, however, allows recovery of punitive damages in addition to compensation, allowing for very high sums. In China, determination of damages granted can be based on not only the damage to the affected individual, but also on the benefits gained by the party that has wrongfully processed personal data.

b Procedural Aspects

This part on enforcement in the relationship discloser-recipient focuses on the avenues available to enforce compliance or obtain damages, looking at questions such as the threshold for accessibility, court pathways, and methods for alternative dispute resolution in the context of individuals' disclosure of their personal data. Notably, Switzerland mandates alternative dispute resolution in the form of *Friedensrichter* ("judges of peace") in certain situations.

---

34 See *infra,* C.IV.3.

The most common mode of enforcement is individual, private litigation, available in all jurisdictions examined. Collective litigation is also possible in multiple jurisdictions, such as Brazil, China and the US, sometimes via consumer agencies, eg, in China. In Brazil, a notable form of litigation is the so-called "public civil action", initiated by the Public Ministries, which litigate to pursue damages to diffuse and collective interests. In Ghana, where the government is the target of a complaint, individuals can address the Commission on Human Rights and Administrative Justice. In Switzerland, administrative courts are responsible for action against public authorities. There are no separate administrative courts in the other jurisdictions examined – in the EU, administrative courts do not exist on the EU level, but may in the individual member states.

Differences can also be seen in the different attitudes towards litigation: Brazil is notable for its extraordinary litigiousness, on the other hand, disputes in Japan are rarer, with comparatively few cases pursued in court.

IV Objective Legal Obligations of the Recipient

In this greater subsection, the country reports look at legal obligations in the varying jurisdictions that are not tied to the relationship discloser-recipient of personal data, but still have impact on the way individuals' personal data is treated. The subsection divides into parts on (objective) duties concerning the handling of received data, monitoring duties, and, as in the previous section, on enforcement of the respective regulation.

1 Duties Concerning Received Data

a Dependence on Authorization

General requirements for preliminary authorization in order to process are largely not existent. An exception can be found in Ghana, where all those processing personal data are required to register with the Data Protection Commission; processing personal data without registration is an offence under the Data Protection Act. In China, there are only (rare) pre-clearance requirements in certain industrial sectors.

b Notification Obligations

Duties to notify individuals, the public, or authorities in certain contexts are very common. However, with the exception of the duties mentioned *supra* for China and

Ghana, these were not general duties preceding processing of personal data, but only for specific circumstances.

A common notification duty exists in the context of security incidents such as data breaches. Such notifications were directed at informing the individuals whose data was affected and the responsible supervisory authority. The details of such obligations, however, varied between the different jurisdictions.

Other notification duties exist in Brazil, where internal governance rules must be made public and where the data protection authority must be explicitly made aware of situations of data-sharing from public authorities to private entities. In Japan, onward transfer of personal data to third parties may require notification of the data protection authority. In Ghana, regulations are in place regarding changes of information relevant for the register, in Russia, regarding the necessity to notify the regulator of the start of data processing, and in Switzerland, regarding the reporting of data files when controllers were regularly processing sensitive data, and in some situations where transferring data abroad.

c Documentation

Other common objective requirements for the handling of individuals' personal data are provisions mandating forms of documentation to ensure accountability.

A related general principle of accountability can be identified in the EU, Brazil and Ghana. Explicit general requirements to keep records of personal data processing activities exist in Brazil, China, the EU, and in Switzerland (under the revised DSG). In other jurisdictions, such record-keeping can be necessary *de facto* due to it otherwise being impossible to comply with other provisions, such as data subject rights. In Japan, the supplementary rules establishing stricter rules for personal data originating from the EU, for example, lead to a *de facto* requirement to mark data as such in order to be able to distinguish it from other personal data.

d Processing Requirements

This part on objective requirements in the country reports examine requirements for the processing of individuals' personal data, looking at whether there is a general prohibition subject to permission including the modalities of processing under such a prohibition, how the balancing of interests functions, and whether there are wider restrictions for business practices or other acts.

In countries where there is a general prohibition of processing personal data subject to permission, allowed processing of personal data worked via enumerated bases of allowance for processing. These differ strongly between jurisdictions. Differences also exist in the position of consent – while sometimes, consent is just one

amongst several bases for processing personal data, it is sometimes clearly visible that consent is intended as the default justification for processing. A balancing of interests was often necessary where processing was allowed on the basis of legitimate/prevailing interest, which was the case in Brazil, the EU, Ghana, Russia and Switzerland (only necessary where a violation of personality rights was possible), but not in China, or Japan (which does not use a general prohibition as a regulatory concept). In the US, this question was irrelevant due to the lack of an existing data protection law. However, a prohibition subject to permission cannot be identified in the existing sectoral or federal laws of the US.

Restrictions on certain business practices are not common within data protection law, but rather originated from other areas of the law, such as consumer protection law, which is the case in for example Brazil or the US.

e Prohibitions and Obligations

Prohibitions and obligations of certain actions by those processing personal data are not common, but occur in certain circumstances, targeting certain practices deemed particularly harmful in the respective jurisdiction. Such prohibitions are usually quite specific in focus.

In Brazil, such prohibitions included the complete privatization of databases considered relevant for national security and the communication or shared use of sensitive health data to obtain an economic advantage. In China, provisions prohibit the theft and unlawful sale of personal information, as well as unreasonable different treatment, and the collection of personal data for personal identity recognition for purposes other than public safety. In the US, certain sectoral prohibitions existed, such as a prohibition of the disclosure of information from alcohol or drug withdrawal treatments, or the resale of data collected under the Illinois Biometric Information Privacy Act. The most notable general prohibition existed in Ghana, where the purchase and sale of personal data was subject to a general criminal prohibition.

Specific obligations for the handling of personal data were common in the form of provisions prohibiting certain forms auf automatic decision-making.

2 Monitoring

This subsection, as part of the examination of objective requirements directed at parties having received personal data from individuals, deals with various monitoring requirements. The subsection is divided into multiple parts, first focusing

on self-monitoring before looking at regulated forms of self-regulation, oversight by supervisory authorities, specific criminal prosecution, and procedural aspects.

a Recipient Self-Monitoring

Apart from natural necessity to put into place structures which allow for compliance with the relevant data protection provisions, some jurisdictions mandate the setup of structures to allow for internal compliance with the relevant laws, as is the case in the EU. In other countries, the setting up of a compliance mechanism is merely encouraged, such as in Brazil or Japan. In Switzerland, the revised DSG will require controllers to structure data processing alongside compliance requirements. In China, certain large internet platforms are subject to strict internal compliance requirements – a previously mandated yearly self-inspection was eliminated, with regular companies only needing to perform impact assessments in specific situations.

Very common are rules concerning the appointment of data protection officers (DPOs), responsible for tasks such as internal monitoring and handling complaints put forward by affected individuals. The appointment is mandatory in Brazil, China, the EU and Ghana. This was commonly subject to thresholds, with smaller companies often exempt. In Ghana, appointment of a DPO is optional for companies and only mandatory for government agencies subject to the Data Protection Act. In Switzerland, the appointment of a data protection advisor is completely voluntary, but the appointment eases further (legal and *de facto*) compliance burdens. In Japan and Russia, no obligation to appoint a DPO existed. However, in Japan, such obligations can arise under self-regulation guidelines, and companies may opt to be "covered" by accredited personal information protection organizations. In the US, such an obligation can arise under the Health Insurance Portability and Accountability Act (HIPAA) – irrespective of this, privacy officers are common in the US, at least in larger companies.

b Regulated Self-Regulation

Multiple jurisdictions acknowledge codes of conduct or similar self-regulatory measures, often created by industry associations, in their data protection legislation, amongst these the EU, Brazil, Japan and Switzerland (under the new DSG). In Brazil, the adherence to such a code of conduct is mentioned by the law as a circumstance to be taken into account by the regulatory authority when administering fines, thus creating incentives for those processing personal data. Also in Brazil, the authority itself can suggest standards and best practices to public sector organizations, which is also the case in Switzerland, where such recommendations are also addressed at the private sector. In Russia and Ghana, there are no provi-

sions concerning such self-regulatory instruments. However, in Ghana – there is a vague obligation to adhere to generally accepted practices and industry rules. In China, a public-private partnership including several large technology companies create templates for compliance. In the US, there is no general obligation to adhere to self-regulatory measures – however, such self-regulatory measures are apparently still very common.

c Supervisory Authorities

Of the examined jurisdictions, five out of eight have dedicated supervisory authorities responsible for data protection: Brazil, with the *Autoridade Nacional de Proteção de Dados* (ANPD), the EU, with a great number of individual authorities in the member states, Ghana, with the Data Protection Commission, Japan, with the Personal Information Protection Commission (PPC) and Switzerland, with the *Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter* (EDÖB). In China and Russia, other public authorities deal with data protection as part of their portfolio. In the US, the relevant regulator has thus far been the Federal Trade Commission (FTC), in principle an antitrust and competition law enforcement authority, and sectoral authorities responsible for enforcing the various different sectoral and federal privacy laws.

d (Specific) Criminal Prosecution

Specific criminal prosecutors explicitly tasked with handling criminal offences regarding data protection and privacy in the context of data disclosure could not be identified in the various jurisdictions. The relevant supervisory authorities are usually tasked with referring such cases to the competent government authorities, such as (federal) police, public security authorities or public prosecutors/attorney generals' departments. In Switzerland, the EDÖB can influence criminal proceedings to a certain extent under the new DSG, which gives the authority the rights of a private claimant.

e Procedural Aspects

This part looks at the investigation powers available to the relevant regulatory authorities. Of the jurisdictions examined, almost all give powers to investigate violations of data protection and privacy provisions to supervisory authorities. In Ghana, contrastingly, the Data Protection Act does not address powers available to the Data Protection Commission. The powers available vary significantly between jurisdictions and authorities.

In Brazil, the ANPD has not yet initiated relevant investigation proceedings at the time, with more relevance of consumer protection organizations and the public ministries responsible for certain collective litigation proceedings. In China, the Cyberspace Administration of China (CAC) plays a leading and coordinating role, with enforcement otherwise decentralized throughout different apartments at various different levels. In Japan, the PPC is afforded detailed investigation and inspection powers, including the right to enter offices and start inquiries. In Russia, *Roskomnadzor*, the communications regulator, has the right to conduct scheduled and unscheduled governmental data protection audits, the frequency dependent on the "risk category" of the organization inspected. In the US, the FTC can, through "consent orders", implement audits of companies' privacy practices by an independent auditor.

3 Enforcement

This subsection on enforcement looks at the different actions to be taken in the relationship between the relevant supervisory authority and the party processing individuals' personal data.[35] This section in the country reports is divided in different modes of enforcement, from intervening in data processing itself, intervention regarding certain business models, and the issuing of penalties to both processors of personal data and individuals involved, again followed by a section regarding procedural aspects.

a Intervention Concerning Data Processing

This part in the country reports looks at authorities' intervention in acts of data processing, including the restriction and prohibition of such data processing acts. While all examined jurisdictions know some form of intervening in data processing, these possibilities were considerably different, coming in various different forms and degrees of intensity, ranging from the blocking of personal data, the blocking of entire websites, to the issuance of recommendations. The intensity of the measure implemented is commonly dependent on the intensity of the violation. Of the jurisdictions examined, the Japanese approach to intervention is particularly notable: instead of issuing binding orders, the PPC primarily acts on the basis of non-binding "guidance and advice", pursuing a cooperative approach to ensure those handling personal data to comply with the Act on the Protection of

35 See *supra*, C.III.4, regarding enforcement in the relationship between individuals and those processing personal data.

Personal Information (APPI). Switzerland (only under the not revised DSG) followed a similar approach, where recommendations of the EDÖB could only be enforced by an administrative court. In the US, corresponding to the competition law framing of privacy regulation, the FTC is able to issue orders targeting "unfair practices".

b Intervention Concerning Business Models

While intervention in practices concerning the processing of personal data is commonly possible in the realm of data protection law, intervention concerning business models is not explicitly named as mode of regulation in data protection legislation in any of the examined jurisdictions. Interventions focused on business models, sometimes with relevance for questions of data disclosure and data protection and / or privacy regulation, are usually done via antitrust and competition law. Such antitrust and competition law frameworks exist in all jurisdictions except for Ghana, which also does not have a dedicated competition regulator, with the only relevant act of legislation being very limited in scope. In this regard, the Swiss approach stood out: Due to comprehensive actions by EU institutions, the Swiss competition agency, the *Wettbewerbskommission*, often felt no need to intervene by itself, instead relying on the decisions of EU authorities and adherence to them by Swiss companies. In the US, as mentioned numerous times already, the entire approach is very centered on competition law aspects – thus, intervention concerning business models is possible, as privacy infringements are often seen as an "unfair or deceptive act or practice".

c Sanctions for Data Processors

Regarding penalties for data processors, the approaches are mostly similar across the different jurisdictions, with common instruments including orders of rectification, administrative sanctions and fines. Two jurisdictions, Ghana and Switzerland, are notable for their approach: instead of including administrative fines on the organizational level, their data protection laws provided only for criminal penalties targeting individuals responsible. In Switzerland, organizations are only (criminally) culpable under specific circumstances.

There are also substantial differences in height of the fines: in the EU, China and Brazil, large fines can be administered based on revenue. In the EU and China, this is calculated on the basis of worldwide revenue. In Brazil, the fines are slightly less imposing, and calculation possible only on the basis of revenue in the Brazilian market. In the US, incredibly large fines are possible in the case that FTC orders are violated, ranging up to 5 billion USD. In Japan, Russia and Switzerland, possible

fines are significant, but still much lower when compared to the aforementioned jurisdictions. In Ghana, fines are considerably less high.

In China, other harsh non-financial sanctions are possible, including the suspension of business, with a revocation of a business license possible, and the confiscation of illegally obtained income part of the portfolio. In Ghana, the Data Protection Act notably stipulates a general penalty applicable to any violation of the act as a catch-all provision. Various shaming instruments were also identified, including the publicization of infractions in Brazil and public announcements of non-compliance in Japan.

d Sanctions for Individual Actors

In contrast to the previous part on organizational-level sanctions, this part of the country reports examines sanctions to be imposed upon individuals held responsible for non-compliance. Responsibility for processing personal data is the decisive features in the examined jurisdictions, such as data processing agents and managing directors. As mentioned above, some jurisdictions primarily revolve around individual responsibility. In some jurisdictions, penalties for individuals are purely of administrative nature, such as Brazil and the EU, while others, such as Switzerland, Ghana, and Japan, rely primarily on criminal penalties. Within companies, general liability for managing directors can also obtain relevance where companies infringe on data protection or privacy regulation, sometimes extending to third parties in case of gross negligence or knowing action, as in Japan. In the US, FTC enforcement against individuals is possible entirely in parallel to enforcement against organizations.

e Procedural Aspects

At last, this part focuses on the procedural aspects of enforcement, examining the current developments in the examined jurisdictions. Especially notable are the differences in equipment across the various public authorities responsible for enforcement. In the EU, the data protection authorities are quite well equipped, while in Ghana, the data protection authority is severely understaffed when compared to other countries, with as little as five full-time employees responsible for the entire country. In Russia, the US and Switzerland (though this might change with the new DSG), there is an impression of low priority of data protection violations in practice. In Brazil, the ANPD's enforcement is difficult to assess, as it was only recently established.

Conclusion

Altogether, the country reports allowed us to understand key similarities and differences between the examined jurisdictions. They also allowed us to see the extent of internationalization present in the area of data protection law across the globe. Particularly striking were the similarities in the general modalities of regulation – with the exception of the United States, with their focus on the concept of privacy rather than data protection, all jurisdictions had considerable similarity. This was especially pronounced with respect to the notions of "personal data" and "processing" or "handling" of personal data. Furthermore, the focus on establishing enumerated legal grounds allowing processing of personal data was widespread. EU influence was very visible, with many originally European concepts and regulatory approaches evident.

Within the context of the "Vectors of Data Disclosure" research project, the country reports allowed us to build a macro-level understanding of the various legal orders examined, enabling us to conduct further research on the influence of different modalities of laws concerning individuals' disclosure of their personal data on individual-level disclosure decisions, together with other "vectors", particularly the influence of cultural differences regarding personal data disclosure. Detailed comparative analysis is, especially with regard to a possible categorization of differing regulatory approaches, still outstanding.

Building on the results of the country reports on the laws of data disclosure, several avenues for follow-up research are in preparation. Notable regulatory approaches are to be researched in more depth, such as methods of reputational sanctioning.[36] Our experiences in the crafting of the country reports gave insight on practical approaches to macro-level comparative law, especially with regard to research design and key hurdles to overcome in this regard, which are to be examined in a decolonial[37] context.[38] Insights from the country reports are also to be used as a baseline in the research project's goal to craft international collisional rules for data protection law.[39] Additionally, the identified rules and regulations

36 Sebastian Kasper and Timo Hoffmann, 'Targeting Reputation: Publizität von Rechtstreue als datenschutzrechtliches Regulierungskonzept im Rechtsvergleich' [2023] forthcoming.

37 See Lena Salaymeh and Ralf Michaels, 'Decolonial Comparative Law: A Conceptual Beginning' (2022) 86(1) RabelsZ 166.

38 Moritz Hennemann and Timo Hoffmann, 'Decolonial Comparative Data Law' [2023] in preparation.

39 See Kai von Lewinski, in this volume, at 195.

are to be used to construct a comprehensive regulatory taxonomy focusing on their influence on individual-decision making.[40]

With regard to the broader goals of the research project, the country reports allow us to compare and contrast the different regulatory measures with views and perceptions on privacy and data protection across the observed jurisdictions, and hopefully understand how these different factors, together with a behavioral economics perspective, come together to influence individuals in their decision-making process regarding the disclosure of their personal data.

40 See also Martin Richthammer and Thomas Widjaja, in this volume, at 35.

Martin Richthammer, Thomas Widjaja

Vectors of Data Disclosure – The Information Systems Perspective

A Introduction

In recent years, various countries adjusted or newly introduced their regulations on the topic of data privacy to protect and inform individuals during disclosing data online. Examples of some adjusted or new regulations are the General Data Protection Regulation (GDPR) in Europe which got introduced in 2016, the California Consumer Privacy Act (CCPA) of 2018 in California which will already be extended by the California Privacy Rights Act (CPRA) in 2023, the Lei Geral de Pro-

Martin Richthammer is an academic research assistant and doctoral candidate at the Chair of Business Information Systems (Prof. Dr. Thomas Widjaja) at the University of Passau, martin.richthammer@uni-passau.de.
Thomas Widjaja is a professor of Business Information Systems at the University of Passau, thomas.widjaja@uni-passau.de.

https://doi.org/10.1515/9783111010601-004

teção de Dados in Brazil introduced in 2018 or the Personal Information Protection Law in China just recently implemented in 2021.

All these regulations have some aspects in common, as can be seen in more detail in this volume.[1] Nevertheless, there are also significant differences in the content of the data protection regulations. Some countries have sector-specific regulations, for example, different rules for health data compared to financial data, and others have so-called omnibus regulations where nearly every data set is treated the same. The CCPA, for example, also sees predicted data – data that is not directly collected but calculated by AI from other data – as personal data, in contrast to the GDPR.

Some of these approaches are seen as successful, while other approaches are heavily criticized. Our project aims to contribute to this discussion by increasing the understanding of how regulation impacts individuals' decisions to disclose data. For example: What aspects of regulation do individuals consider in their process of a disclosure decision?

Our approach to gaining first insights into the topic of regulation and data disclosure decisions was threefold, as Fig. 1 illustrates.

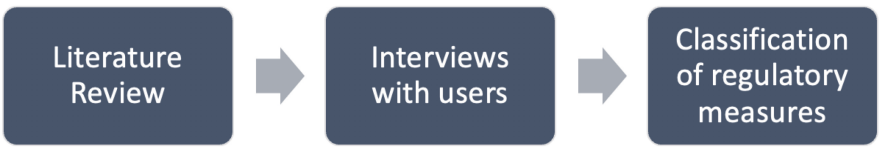

Fig. 1: Illustration of our research process.

First, we started with a literature review to gain an overview of the existing research findings on regulation and data disclosure. Second, as the literature review revealed a focus on rational, high-effort decisions of existing research, we conducted interviews to examine how individuals describe the influence of regulation in low-effort disclosure situations. Third, as the interviews revealed shallow knowledge about data protection regulations and a low perceived impact of regulation overall, we discussed the mechanisms of how regulatory measures influence individual decisions within the interdisciplinary research team of the project "Vectors of Data Disclosure" of the Bavarian Research Institute for Digital Transformation (bidt). The project aims to provide insights on questions like whether the willingness of an individual to disclose data depends on cultural, regulatory and individual factors and how these factors are intertwined. Based on the results of the in-

1 See especially Timo Hoffmann, in this volume, at 1.

terdisciplinary workshops, we identified two possible categories of regulatory measures: those that assure a fixed amount of privacy and those that allow users to choose their preferred privacy options. Each of these steps will now be described in more detail.

B Structured Literature Review

I Method

To answer how regulation impacts the individual decision to disclose data, we started with a structured literature review (SLR). Thereby, we wanted to gain an overview of the existing knowledge inside the Information Systems (IS) literature regarding the topic of influences of regulation on individual data disclosure. We followed the suggestions of vom Brocke and others[2], who segment a literature review into five steps: the definition of the scope of the review, the conceptualization of the topic, the analyzing as well as synthesizing of the identified literature, and last proposing of a research agenda. As a result of the step of analyzing and synthesizing, we will retrieve concepts from the found literature.[3] A concept here means a dimension of the topic at hand – influences of regulation on individual data disclosure – that can be used to answer the research question, how regulation impacts the disclosure decision.

We conducted the literature search in 2021 in top IS journals that are part of either the Association for Information Systems Senior Scholars' Basket of Journals or the Financial Times Research Rank 50. The literature search was based on a search string that consisted of two parts: The first part consisted of "regulation" and synonyms like "law," "government," or "restriction," and the second part included "information disclosure," and synonyms like "self-disclosure" and "data sharing."

2 Jan vom Brocke and others, 'Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research' (2015) 37(1) Communications of the association for information systems 9 205–224.

3 Jana Webster and Richard T. Watson, 'Analyzing the past to prepare for the future: Writing a literature review' (2002) 26(2) MISQ XIII-XXIII.

II Results of the Structured Literature Review

The search string resulted in a total of 937 articles. After scanning the titles of the articles, 35 remained for further examination. These were reduced to 28 articles after reading the abstracts. After full-text analysis, seven articles remained. An additional forward and backward search revealed another seven articles. Thus, the final number of articles was 14.

These 14 articles were then categorized based on the suggestions of Webster and Watson.[4] A snippet of the final concept matrix can be seen in Fig. 2. Each dimension of the concept matrix was identified by answering one of the following questions: Which type of regulation is examined? What kind of disclosure decision is made? What is the effect of regulation on data disclosure? We identified five concepts: *regulation*, *influence on*, *influenced by*, *data type*, and *level of effort. The regulation* dimension answers the question, which type of regulation is examined. Three dimensions, *influence on*, *influenced by*, and *data type*, answer the question, what effect regulation has on data disclosure. The *level of effort* depicts which type of disclosure decision is made (high-effort vs. low-effort). In the following, the dimensions will be described in more detail.

References	Regulatory difference	Legal Space	Perspective	Operational-ization	Influence on	Influenced by	Data type	Level of effort
Adjerid, I. (2016).	Consent giving	US, ++[c]	Law in action	Reg. measure	PC, benefits	-	Health	High-effort
Anderson, C. L. (2011).	HIPAA[a]	US	Law in the books	-	PC, trust	-	Health	High-effort
Bellman, S. (2004).	Sectoral - Omnibus	US, ++	Law in action	Reg. preferences	PC, reg. preference	Culture	Unspecified	High-effort
Benamati, J. H. (2021).	Reg. existence	US, Indian	Reg. perception	Reg. preferences	-	Culture, PC[c], risk, trust	Financial, commerce	High-effort
Cao, Z. (2018).	Nudging, Quota	-	Law in action	Reg. measure	ITD[g], privacy harm	-	Unspecified	High-effort

Fig. 2: Snippet of the final concept matrix with all retrieved concepts.

1 Regulation

This dimension describes the type of regulation examined. It entails four sub-dimensions: *regulatory difference*, *legal space*, *perspective*, and *operationalization.* These sub-dimensions were to hint at research gaps. We identified that the main differences in the examined regulations were based on either the regulation itself,

4 Ibid.

concerning, for example, its generalizability or restrictiveness (*regulatory difference*), the examined region of the regulation(s) – for example, common law or civil law – (*legal space*), whether the research is concerning regulations as it should be applied in theory – law in the books – or as it is actually enacted – law in action – (*perspective*), or the regulatory concept was, for example, the preference of an individual on how it should be versus the regulation as it actually is (*operationalization*).

The sub-dimension *regulatory difference* describes what aspect of the regulation differs between two models that get compared. There are many different measures that get compared across the identified articles. The first main difference between the regulations identified is the generalizability of regulations. Some articles compared regulations that consisted of sectoral laws with regulations that introduced overall omnibus-laws.[5] A second aspect that differed between examined regulations was their restrictiveness. Some look at regulations that enable individuals to help themselves by granting them rights, while others work via leaving the industry to self-regulation.[6] Those regulations that grant individuals rights can also differ in the degree of autonomy a user is granted and, for example, how many restrictions regarding data handling are prescribed by the regulation. In addition to these, there are regulations that require companies to request a permit from an individual to use their data. Differences between the regulations could also be found in who is made responsible for the level of privacy of a decision, the individuals themselves, the industry, or the government.[7] Some of the articles, however, did not compare different types of regulations but the effects of implementing a new measure into existing regulations.[8] We observed that different entities are re-

5 Steven Bellman and others, 'International differences in information privacy concerns: A global survey of consumers' (2005) 20(5) Information Society 313–324; Heng Xu and others 'The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services' (2009) 26(3) Journal of Management Information Systems 135–173.

6 Sandra J Milberg and others, 'Values, personal information privacy, and regulatory approaches' (1995) 38(12) Communications of the ACM 65–74.

7 Sandra J Millberg, H Jeff Smith and Sandra J Burke, 'Information privacy: Corporate management and national regulation' (2000) 11(1) Organization Science 35–57; Xu and others (n 5); Heng Xu and others 'Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services' (2012) 23(4) Information Systems Research 1342–1363.

8 Eg Idris Adjerid and others, 'The Impact of Privacy Regulation and Technology Incentives: The Case of Health Information Exchanges' (2016) 62(4) Management Science 1042–1063; Zike Cao, Kai-Lung Hui and Hong Xu, 'An Economic Analysis of Peer Disclosure in Online Social Communities' (2018) 29(3) Information Systems Research 546–566; Benoît Otjacques, Patrik Hitzelberger and Fernand Feltz, 'Interoperability of e-government information systems: Issues of identification and data sharing' (2007) 23(4) Journal of Management Information Systems 29–51.

sponsible for privacy, ie, governments[9] or organizations[10]. Besides the comparisons of regulatory differences, Benamati, Özdemir and Smith[11] used a subjective measure where participants rated the existing regulation regarding their sufficiency. So, the examined articles differ in looking at aspects of generalizability and restrictiveness of underlying regulations. They compare different responsibilities for privacy based on the laws and sometimes only examine one specific regulatory measure.

The sub-dimension of *legal space* differentiates between the region of the in the articles examined regulatory frameworks. This is important to consider as not all regions are represented in the literature yet. Most research is conducted with reference to US law with its various state-specific frameworks.[12] Extending this view, some articles compare the US perspective with other national regulations, for example, the ones of China, Brazil, Japan, and Europe.[13] Besides this, we also identified articles that only focus on European regulations.[14] In addition to that, one study analyzes the impact of the European GDPR when commanded by US companies.[15] Similarly, the effects of US law are tested in Singapore.[16]

The sub-dimension *perspective* comprises whether the regulations examined are looked upon as laws in the books or laws in action. This differentiates between the analysis of laws as they should be applied in theory (law in the books) or as they are actually enforced (law in action). This differentiation is important as most people will be guided more by laws in action and social norms than by the laws in the book. We classified most of the articles as representing the law

9 Catherine L Anderson and Ritu Agarwal, 'The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information' (2011) 22(3) Information Systems Research 469–490; Johanna Strycharz and others, 'No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies' (2021) Computers in Human Behavior 120; Yibo Zhang, Tawei Wang and Carol Hsu, 'The effects of voluntary GDPR adoption and the readability of privacy statements on customers' information disclosure intention and trust' (2020) 21(2) Journal of Intellectual Capital 145–163.

10 Huseyin Cavusoglu and others, 'Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook' (2016) 27(4) Information Systems Research 848–879.

11 John Benamati, Zafer D Özdemir and H Jeff Smith, 'Information Privacy, Cultural Values, and Regulatory Preferences' (2021) 29(3) Journal of Global Information Management.

12 Adjerid and others (n 8); Anderson and Agarwal (n 9).

13 Bellman and others (n 5); Millberg and others (n 6); Milberg, Smith and Burke (n 7).

14 Otjacques and others (n 8); Strycharz and others (n 9).

15 Zhang and others (n 9).

16 Xu and others (n 5); Xu and others (n 7).

in the books perspective.[17] But there are few articles using the law in action perspective as well.[18]

The sub-dimension *operationalization* expresses that the variables measuring regulatory approaches were implemented very differently across the identified articles. To get an overview, we developed two terms that can be used to summarize the different conceptualizations, regulatory approaches – including specific regulatory measures – and regulatory preferences. Regulatory approaches thereby look at regulation as a whole, like the degree of involvement of governments in privacy decisions or how organizations and people get involved in the protection of privacy.[19] Some articles specifically look at single regulatory measures which are implemented through regulation. Those measures comprise for example of nudging or consent giving.[20] As these measures stem out of regulations, we will subsume these articles under the category of regulatory approaches. *Regulatory preferences* describe how much people want governments to be involved in their decision about and providing of privacy while disclosing data.[21]

2 Influence on, influenced by, data type

The three dimensions of *influence on*, *influenced by*, and *data type* answer the question about how regulation influences the data disclosure decision of an individual. The dimension *influence on* categorizes the articles based on which variables were influenced by the regulatory variable. The main influenced variable identified was data disclosure behavior[22] or the intention to disclose data[23]. Some articles did not directly measure disclosure but based their assumptions on the APCO model[24] and

17 Eg Tamara Dinev and others, 'Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts' (2013) 22(3) European Journal of Information Systems 295–316; Milberg and others (n 6); Otjacques, Hitzelberger and Feltz (n 8).

18 Eg Adjerid and others (n 8); Benamati and others (n 11); Cao and others (n 8).

19 Millberg and others (n 6); Milberg and others (n 7); Xu and others (n 5); Xu and others (n 7).

20 Adjerid and others (n 8); Cao, Hui and Xu (n 8); Otjacques, Hitzelberger and Feltz (n 8); Zhang, Wang and Hsu (n 9).

21 Bellman and others (n 5); Benamati, Özdemir and Smith (n 11); Milberg, Smith and Burke (n 7).

22 Cao, Hui and Xu (n 8); Cavusoglu and others (n 10); Strycharz and others (n 9).

23 Xu and others (n 5); Zhang, Wang and Hsu (n 9).

24 Tamar Dinev, Allen McConnell and H Jeff Smith, 'Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box' (2015) 26(4) Information Systems Research 639–655.

thus measured privacy concerns instead of disclosure.[25] So, regulation seems to influence the disclosure behavior of individuals either directly or indirectly via for example, privacy concerns.

The dimension *influenced by* subsumes factors that influence the regulatory variable. This means that the effect of regulation on data disclosure can also be influenced indirectly by other variables. A first example for a variable influencing regulation are so-called cultural dimensions.[26] Cultural dimensions are used to describe certain aspects of how people of a culture act and the dimensions can also be used to explain differences between the behavior of people of different countries. Privacy concerns are identified as another influential factor on regulatory preferences.[27] Regulation operationalized as a regulatory approach can even influence the regulatory preference of individuals.[28] There are also moderator variables that indirectly influence the impact of regulatory variables like a user's privacy sensitivity or self-protective behavior of an individual.[29] Overall, we can see that regulation not only influences the disclosure behavior of individuals, but its effect is also dependent on contextual factors and user characteristics like culture, data sensitivity, or privacy-related behavior and also external factors as well as third parties.

The dimension *data type* describes which data was examined in the articles. The key categories of data types were medical and health data,[30] disclosures on social media[31] and location[32] and one article examined the disclosure of financial data[33]. This dimension is important as some types of data are treated differently in some regulations.

3 Level of effort

The dimension *level of effort* categorizes the articles based on whether they are based on a high-effort or a low-effort data disclosure decision process. High-effort

25 Adjerid and others (n 8); Anderson and Agarwal (n 9); Bellman and others (n 5); Xu and others (n 7).

26 Bellman and others (n 5); Benamati, Özdemir and Smith (n 11); Millberg and others (n 6); Milberg, Smith and Burke (n 7); Otjacques, Hitzelberger and Feltz (n 8).

27 Bellman and others (n 5); Milberg, Smith and Burke (n 7).

28 Milberg, Smith and Burke (n 7).

29 Cavusoglu and others (n 10); Xu and others (n 5).

30 Adjerid and others (n 8); Anderson and Agarwal (n 9).

31 Cavusoglu and others (n 10); Dinev and others (n 17).

32 Xu and others (n 5); Xu and others (n 7).

33 Benamati, Özdemir and Smith (n 11).

processes are related to a rational choice that makes full use of all available information, and low-effort processes are based on mental shortcuts like heuristics and stereotypes to save cognitive energy.[34] All 28 identified articles of the SLR examined a decision process based on high-effort assumptions. Anderson and Agarwal[35] were the only ones that incorporated emotions into their research model, but they did not connect emotions directly to regulation. Because of this underrepresentation of possible low-effort decisions, we decided to conduct interviews with internet users on whether and how they recognize regulation to have an impact on their decision process.

C Interviews

I Method

As the dimension *level of effort* revealed, low-effort decision-making was only barely considered in the identified articles. To gain insights in that regard, we conducted interviews to explore the effects of regulations on a low-effort data disclosure decision. Interviewees had to complete a scenario task that they had to share during an online video call that also got recorded. They were asked to visit a weather website and look up the weather forecast for their current location. Based on this research setting, we were able to see how the people interacted with the cookie banner. We deliberately chose the context of cookie banners as this represents an extremely low-effort scenario. After this task, a semi-structured interview started. The questions of the interview covered three categories. First, the interviewee's satisfaction with and knowledge about the decision they made with the cookie banner was evaluated. Then, the interviewees were asked about their knowledge of the respective regulations regarding cookies and how those regulations influenced their decisional process. The last category of questions was about how trust and transnationality influenced the interviewee's data disclosure.

34 Eg Richard E Petty and John T Cacioppo, *'The elaboration likelihood model of persuasion'* (1986, Academic Press) in *Advances in Experimental Social Psychology*, 123–205.

35 Anderson and Agarwal (n 9).

II Results of the Interviews

We interviewed a total of n = 20 young German adults with a medium age of *M* = 26,7 years. For the cookie scenario, we could identify that the people seem not to be influenced by regulation or their trust in it. Results showed a rather low privacy literacy. People possess only scarce knowledge about the decision they make when accepting or declining cookies (14 of 20). They also possess scarce knowledge about the regulation behind cookies (15 of 20). In addition to that, the interviews showed that the involvement of the interviewees in the decision situation was quite low, as we expected because of the cookie scenario. Eight of 20 interviewees stated that they are "indifferent" about their decision on cookies. Another insight that the interviews brought up was that people perceive high response costs when having to interact with cookie banners all the time. The interviewees reported that they were bugged by being forced to give their consent each time they visited a (new) website (12 of 20). In addition to these results, the interviews also showed that there is a tendency to high trust in German regulation. Especially in the context of transnational data flows, interviewees stated that they had more trust in German companies and regulations compared to non-European countries and companies. They were even more willing to disclose data to the former (11 of 20). Thus, regulation and trust in regulation might have an impact on the individual decision in a transnational data disclosure context.

D Classification of regulatory measures

I Method

The main insights of the structured literature review and the interviews motivated us to take a closer look at how regulations differ from each other and that people do not exactly know what regulatory measures there are to provide privacy. We compared the regulations of seven different countries and thereby tried to classify the different regulatory measures we could identify. In the next step, we want to use this knowledge to develop a taxonomy based on the approach of Nickerson, Varshney and Muntermann.[36] The classification should differentiate the regulatory measures based on differences in how they provide privacy to an individual re-

36 Richard C Nickerson, Upkar Varshney and Jan Muntermann, 'A method for taxonomy development and its application in information systems' (2013) 22(3) European Journal of Information Systems 336–359.

garding their disclosure of data. Thus, researchers on the relationship between regulations and data disclosure can further use the classification and, later on, the taxonomy to situate the measure they have a look at inside the taxonomy. In doing so, they can compare their findings to studies that look at regulatory measures which are classified in the same section of the taxonomy. To gain first insights, we scanned the data privacy regulation of the European Union, the GDPR, for regulatory measures it includes to provide privacy when disclosing data online. In the future, we will use regulations of other countries to enhance the classification and address the differences in legal frameworks as found to be an important factor in the structured literature review. In addition, looking at the other regulations will lead to a mitigation of biases that are involved when only looking at one certain type of regulatory framework, in our case the GDPR.

II Results of the classification of regulatory measures

We identified user action as the main dimension that determines how regulatory measures provide privacy. From this perspective, two characteristics can be distinguished: First, measures that provide *privacy without user action,* and second, measures where a user gets the possibility to select their own desired level of privacy, *privacy through user action.* Another interesting aspect is the second dimension, the timing when the privacy should be provided to the user. It consists of two characteristics, as the measures can have an impact either *before/while disclosing* or *after disclosing.* As the third dimension for classification, we identified that regulations differ in the modality how privacy gets provided. Two characteristics can be distinguished: They either come along with *transparent information about data handling processes* and/or with possibilities for *actions concerning the data.*

1 Privacy without user action

Under the characteristic of *privacy without user action*, we categorize regulatory measures that provide privacy by placing requirements on companies, thereby forcing them to provide predefined privacy assurances. Here, a user is uninvolved in the process of determining the level of privacy of data disclosure. The user does not have to invest any additional resources, and thus, these measures are considered to mainly be supportive in low-effort decisions. An example for a right where a user does not have to act is the law on purpose limitation (Art. 5 Sec. 1 lit. b GDPR), where a company is obliged to define what purpose they are going to use the requested data for. Regulatory measures falling into this category might re-

quire the individual to have a certain amount of knowledge about the measures,[37] and they need to trust the regulator, the enforcement of regulations, and the service provider to oblige to the regulations.[38]

2 Privacy through user action

Under the characteristic of privacy through user action, we categorize measures that give users the ability to self-select their preferred level of privacy. An example for privacy through user action is the possibility to request information about collected user data via the right to information (Art. 15 GDPR). With these measures, the users themselves must act to be able to choose their desired amount of privacy. Thus, regulatory measures that are related to user-selected levels of privacy primarily affect situations where a user puts high-effort into the decision.[39] In addition to that, users might have to be aware of the decision, the options they have, and the regulation that is in place, as well as the identification with possible alternatives.[40]

3 Before / while disclosing

Regulations that act before disclosing data are, for example, restrictions placed on a company that forbid them to collect data in the first place, for example, the law on purpose limitation (Art. 5 Sec. 1 lit. b GDPR), which only allows collecting data that is needed to fulfill a predefined purpose for the company. While the purpose limitation in fact becomes effective immediately after the disclosure of data, we still categorize it under the characteristic of *before disclosure* as the data recipient needs to consider the purpose before acquiring any data.[41] Another example is Art. 9 Sec. 1 GDPR, which prohibits the processing of special categories of personal

---

37 Eg Strycharz and others (n 9).

38 Eg Matthias Söllner, Axel Hoffmann and Jan M Leimeister, 'Why different trust relationships matter for information systems users' (2016) 25(3) European Journal of Information Systems 274–287.

39 Eg Jiangning He, Xiao Fang, Hongyan Liu and Xindan Li, 'Mobile app recommendation: An involvement-enhanced approach' (2019) 43(3) MIS Quarterly 827–849.

40 Eg James R Averill, 'Personal control over aversive stimuli and its relationship to stress' (1973) 80(4) Psychological Bulletin 286–303; Mary J Culnan, 'Consumer awareness of name removal procedures: Implications for direct marketing' (1995) 9(2) Journal of Direct Marketing 10–19.

41 Cf Hoffmann, in this volume, at 1, 19.

data like ethnic origin or genetic data, unless an exception is met (see Art. 9 Sec. 2–4 GDPR). In addition to that, users must be informed about the data handling practices of a company before they disclose data. This is regulated in Art. 12–14 GDPR.

4 After disclosing

Regulations that act after the disclosure of data has already happened, for example, require a company to document how the collected data gets processed further, as Art. 5 Sec. 2 GDPR states. Another example is the right of a user to restrict the processing of certain data (Art. 18 GDPR). Overall, companies are required to document every step of data processing. Art. 5 Sec. 1 lit. e GDPR is related to the storage of acquired data and states that this data must be saved in a way that prevents a data subject from being identified for longer than needed.

5 Transparent information about data handling processes

The characteristic of *transparent information about data handling processes* subsumes all regulatory measures that give users information about data handling processes, the options they have, and the consequences of these options. They are regulated with so-called information obligations (Art. 12–14 GDPR). Furthermore, users have the possibility to request information about their collected data via the right to information (Art. 15 GDPR).

6 Actions concerning the data

The characteristic of *actions concerning the data* subsumes all regulatory measures that do not contain information, but force companies to take certain actions concerning the data they are about to acquire or already have. An example of a measure categorized here is the purpose limitation (Art. 5 Sec. 1 lit. b GDPR). There are also regulatory measures that give users options to modify their preferred level of privacy. Examples of regulations that offer options to re-modify the privacy level are the right to deletion (Art. 17 GDPR), the right to withdraw consent (Art. 7 Sec. 3 GDPR), or the right to rectification (Art. 16 GDPR). Each of them gives a user the ability to *inter alia* demand the change of for example erroneous data or change the type and amount of data that is allowed to be collected. In addition to company action and user action, there are also regulations that grant separate

data protection authority enforcement permissions (Art. 58 Sec. 2 GDPR). These permissions enable the authority to control the law abidance of companies.

E Discussion

The aim of the research project "Vectors of Data Disclosure" is to identify how regulatory measures influence individual data disclosure processes. To contribute to this aim, we started with a structured literature review to gain a better understanding of the existing knowledge on how regulation influences data disclosure. As this led to the insight that most existing work focused on rational, high-effort decision-making, we conducted interviews with internet users to examine how they rated the influence of regulation on their data disclosure in a low-effort disclosure situation. The interviews revealed that most participants only had little knowledge of data privacy regulations and did not note a specific influence of these regulations on their disclosure behavior. Based on the insights of the structured literature review – that the differences between regulations need to be examined in more detail – and the interviews – that there is not much knowledge about the regulations –, we scanned for different regulatory measures in the data protection regulations of at first Germany. We later on want to enhance this with the regulations of USA, Brazil, China, Japan, Ghana, and Russia together with our project colleagues over the course of about two months. Until then, we want to gather at least ten different measures per country. We compared the measures identified in the GDPR and classified them. We then identified that there are two main types of regulatory measures, the ones that assure user privacy without any user action and those that allow a user to adjust their privacy preferences themselves. Further, regulations seem to differ in the point of time they affect a disclosure process and their desired effect, through action, or information.

The next steps in our part of the research project 'Vectors of Data Disclosure' will be to: First, further develop the classification of regulatory measures with regulations of other countries into a taxonomy. Second, examine the effects of differently classified regulatory measures on individual user behavior in different disclosure situations. Therefore, we will conduct a scenario-based survey among internet users of the different countries we used to identify the regulatory measures. The results can be used to evaluate whether different regulatory measures fit different data disclosure situations better in providing privacy to an individual. Third, we will advance these insights by considering transnational data disclosure and data flows in a disclosure scenario. Thus, we will see if the insights of the inter-

views on trust into a country, government and regulation influence the disclosure decision.

Daniela Wawra

Parameters of Personal Data Disclosure Decisions in Cross-Cultural Comparison

A Introduction

The aim of this contribution is to compare people's attitudes towards the collection of personal data cross-culturally. The motivation for this undertaking and the relevance of such an approach are summarized by Li as follows:

> As many technologies have become available around the world and users increasingly share personal information online with people and organizations from different countries and cultures, there is an urgent need to investigate the cross-cultural differences in users' privacy attitudes and behaviors in the use of these technologies. Such investigation is important to understand how users in different cultures manage their information privacy differently and to inform the privacy design for technologies that are used globally.[1]

Daniela Wawra is a professor of English Language and Cultural Studies at the University of Passau, daniela.wawra@uni-passau.de.

1 Yao Li, 'Cross-Cultural Privacy Differences' in Bart P Knijnenburg and others (eds), *Modern Socio-Technical Perspectives on Privacy* (2022).

https://doi.org/10.1515/9783111010601-005

Furthermore, it is important for data recipients, legislators, and regulators to be aware of the prevailing views in their country and possible cross-cultural differences to ensure that they serve the people with their data protection measures, and that they provide appropriate frameworks for domestic and, in particular, cross-cultural data flows. Therefore, research into "the concrete cross-cultural differences in users' privacy attitudes and behaviors is most warranted"[2].

This contribution discusses five central parameters of data disclosure: 'General Value of Informational Privacy,' 'Benefits Associated with Data Disclosure,' 'Privacy Concerns and Risks,' 'Trust in Data Recipient,' and 'Transparency / Communication on Data Use.' The parameters 'Data Protection Laws,' 'Data Sensitivity,' as well as 'Data Protection Literacy' are the subject of further contributions to this volume.[3] All these parameters on which we focus in our research project *Vectors of Data Disclosure* capture the narrower cultural context of common data disclosure situations.[4] Figure 1 below provides an overview:

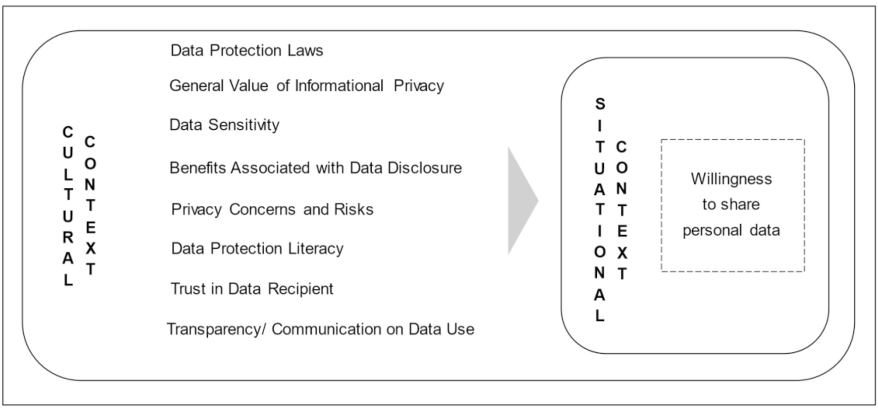

Fig. 1: Central Cultural Parameters of Data Disclosure.[5]

In what follows, large-scale survey data on issues relating to the selected central parameters of data disclosure (see above) will be compared and discussed cross-

2 Ibid.

3 See Daniela Wawra, in this volume, at 169.

4 Cf Daniela Wawra, 'The Cultural Context of Personal Data Disclosure Decisions' 22(2) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/Intro_bidt_Wawra_University_of_Passau_IRDG_Research_paper_Series.pdf> accessed 07.02.2023.

5 Adapted from ibid 8.

culturally. This macro-perspective[6] offers a better understanding of prevailing cultural attitudes towards and assessments of factors that may influence the willingness to share personal data. Whenever possible, the following seven countries are included in the cultural comparison: Brazil, China, Germany, Japan, Russia, Switzerland, and the United States. For each of these countries, individual cultural reports were compiled, most of which have already been published (with the exception of the report on Switzerland, which, however, will be published shortly).[7] Details about the surveys (eg, sociodemographic data, representativeness, etc.) that are discussed in the following chapters can be found there. The number of respondents for each country was generally between 500 to 1000, with few exceptions. In some cases, items were not surveyed in all countries, so they had to be excluded from the comparative study. Let us begin by looking at survey results that first of all relate to the general value that is placed on informational privacy in a culture.

6 Cf ibid.

7 Cf Sarah Howe, 'Cultural Influences on Personal Data Disclosure Decisions: German Perspectives' 22(14) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-14.pdf> accessed 07.02.2023; Lena Kessel, 'Cultural Influences on Personal Data Disclosure Decisions: US-American Perspectives' 22(04) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/Country_Report_USA_publication_LK_Final.pdf> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Brazilian Perspectives' 22(08) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-08.pdf> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Chinese Perspectives' 22(09) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-09.pdf> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Japanese Perspectives' 22(10) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-10.pdf> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Russian Perspectives' 22(11) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-11.pdf> accessed 07.02.2023.

B General Value of Informational Privacy

Informational privacy is understood "'as the claim of an individual to determine what information about himself or herself should be known to others'[8] and as the demand to be protected from unwanted access to personal data"[9].[10] The parameter indicates how important or unimportant respondents consider this demand. As a general tendency, "it is assumed that the more value people generally place on their informational privacy, the more cautious they will tend to be when asked to disclose personal data"[11].

Let us start by taking a closer cross-cultural look at people's attitudes towards different kinds of personal data collection by the government.

I General Value of Informational Privacy Vis-à-Vis the Government

What are people's attitudes towards video surveillance by their government in public places? As the following diagram (Fig. 2) shows, a clear majority of respondents in all countries surveyed accept governmental video surveillance in public. China stands out with a particularly high approval rate of 82%. We can conclude that majorities of respondents across all countries surveyed do not see their informational privacy threatened by video data collection in public. In this context, the value placed on informational privacy is thus low in all seven cultures. It is lowest in China and highest in Brazil.

Furthermore, people were asked whether they thought their government should have the right to collect information about anyone living in the country without their knowledge (Fig. 3).

China is the only country where a majority of no less than 52.8% of the respondents believe that the government should have the right to collect information about anyone living in the country without their knowledge. In the other countries, clear majorities are not of this opinion. In Germany and Switzerland, informational privacy has the highest value in this general context. In the United States, the second-most respondents approve of the government collecting information

8 Alan F Westin, 'Social and Political Dimensions of Privacy' (2003) 59(2) Journal of Social Issues 431, 431.

9 Beate Rössler, *Der Wert des Privaten* (2001) 25.

10 Wawra (n 4) 9.

11 Ibid.

about people living in the country. Compared to China, the percentage of those in favor is significantly lower at 28.1%. This nevertheless remarkable result could still be due to the traumatic experience of 9/11 and the fact that the United States is still a prime target for terrorists. After 9/11 and the proclamation of the 'war on terror,' the acceptance of surveillance measures for national security at the expense of privacy has increased.[12] In addition, the United States' major problems with illegal immigration must also be factored in here.[13]

12 Cf eg Daniela Wawra, 'Privacy in Times of Digital Communication and Data Mining' (2004) 25/2, *Anglistik* 15, 16.

13 Cf eg Erin Duffin, 'Illegal Immigration in the United States: Statistics & Facts' (2021) <https://www.statista.com/topics/3454/illegal-immigration-in-the-united-states/#topicHeader__wrapper> accessed 07.02.2023.

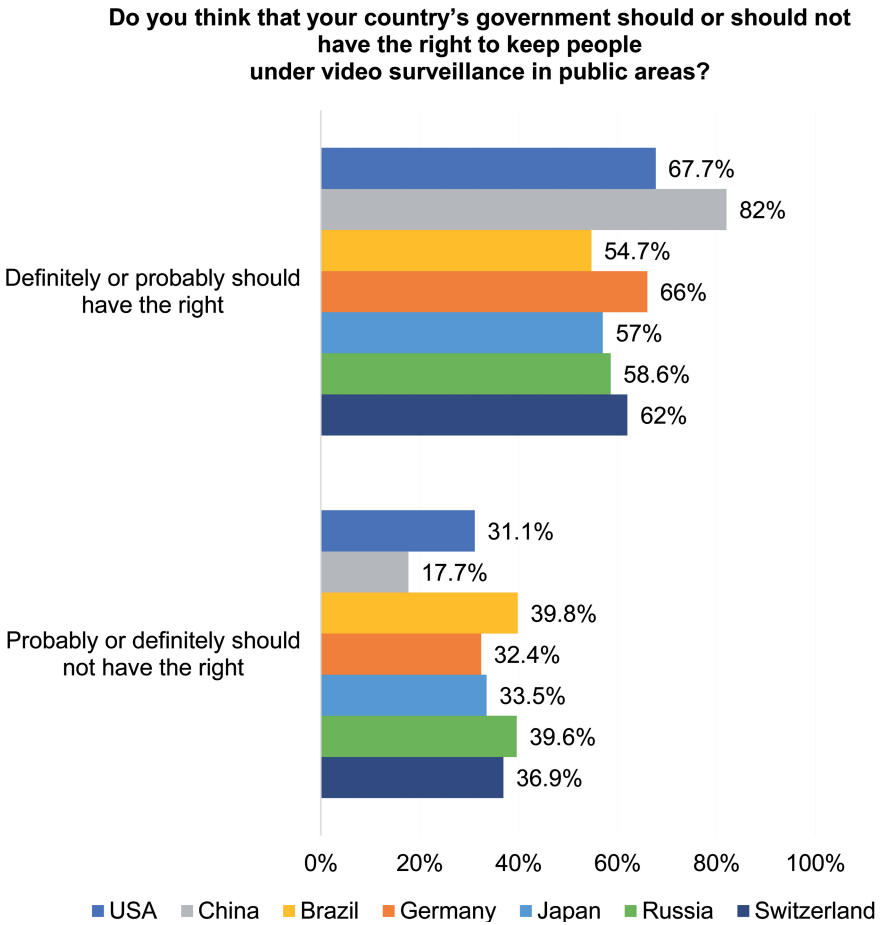

Fig. 2: Respondents' attitudes towards video surveillance by their government in cross-cultural comparison.[14]

Next, we will take a look at people's opinions on government monitoring of e-mails and other information exchanged on the Internet.

14 EVS/WVS, 'European Values Study and World Values Survey: Joint EVS/WVS 2017–2022 Data-Set' (2022) Version 3 436, 437 <https://www.worldvaluessurvey.org/WVSEVSjoint2017.jsp> accessed 07.02.2023.

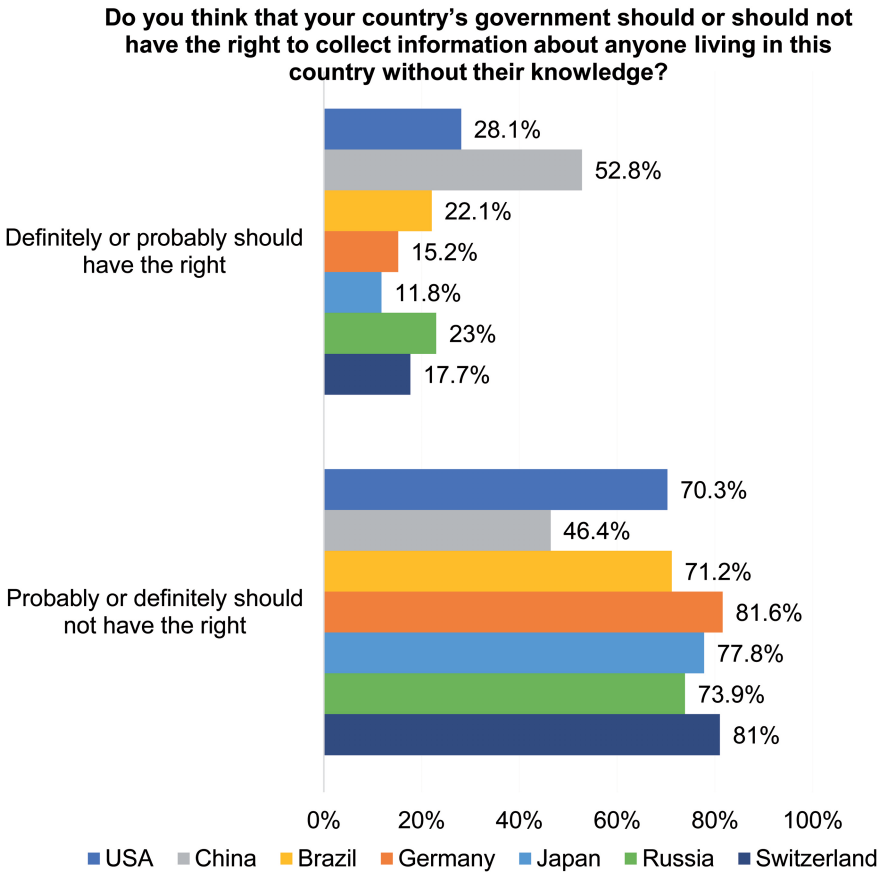

Fig. 3: Respondents' views on data collection by the government without knowledge and consent in cross-cultural comparison.[15]

China again attracts attention as it is the only country where a majority (60.6 %) accepts their government's monitoring of email and Internet. In all other countries, only slightly more or less than a quarter of respondents believe that their government should have this right. The percentages of all countries except China are very close to each other and only differ by a maximum of just under 5 % (4.7 %). This means that people in all cultures considered here, with the exception of China, place great value on their informational privacy when writing emails and exchanging information online.

15 Ibid 440, 441.

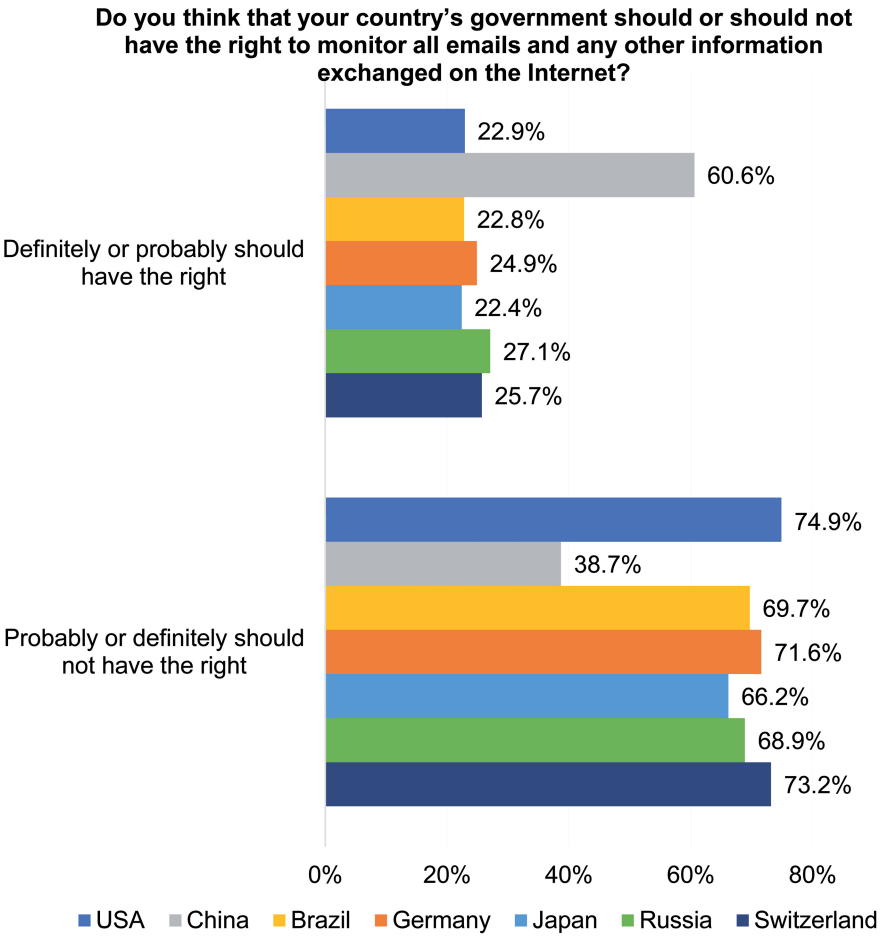

Fig. 4: Respondents' attitudes towards email and Internet monitoring by their government in cross-cultural comparison.[16]

The majority of Chinese respondents agree with the disclosure of data in all situations discussed here. This underlines the low value they place on their informational privacy in these disclosure contexts. Similarly, in the other countries, the majority of respondents do not object to the disclosure of data through video recording in public without their consent. However, most respondents oppose non-consensual data collection by their government in general and with regard to

16 EVS/WVS (n 12) 438, 439.

email contents and online information exchange. This emphasizes the high value they place on their informational privacy in these disclosure contexts.

Overall, Chinese respondents place by far the least importance on their informational privacy vis-à-vis their government, according to these surveys. How can this be explained (for more explanatory factors, see also in this volume[17])? Looking at the broader cultural context,[18] it is first of all relevant that China is a 'single-party authoritarian state', which is led by the communist party.[19] China has "[e]xtractive political institutions,", ie, "power [is concentrated] in the hands of a narrow elite and [...] few constraints [are placed] on the exercise of this power"[20]. "The Communist Party is all-powerful in China and controls the entire state bureaucracy, the armed forces, the media, and large parts of the economy. Chinese people have few political freedoms and very little participation in the political process"[21]. The restriction of free speech and censorship are common.[22] However, this also applies in a similar way to Russia, for example. But, unlike the other countries, surveillance measures by the government are particularly common and pervasive in China, and the Chinese are used to them and have no other option but to accept them. It comes as no surprise then that China ranks lowest on the Internet Privacy Index: "A high privacy score means the country takes steps to protect information shared online. The higher the score, the more protected the information"[23]. Furthermore, China's social credit system, "a digital sociotechnical credit system that rewards and sanctions the economic and social behaviors of individuals and companies"[24], is still unique worldwide. It has been described as "the

17 Wawra, in this volume, at 169.

18 Cf Wawra (n 4).

19 Jaroslav Zapletal and Shane J Barter, 'China's Political System' (2021) The Newsletter 88 Spring 2021.

20 Daron Acemoglu and James A. Robinson, *Why Nations Fail: The Origins of Power, Prosperity and Poverty* (2012) 95.

21 Ibid 487.

22 Cf A. Grant, 'Internet Privacy Index' (2020) <https://bestvpn.org/privacy-index/> accessed 06/03/2022; Wang Zhicheng, 'China – Official Data on Internet Censorship' *AsiaNews* (1 September 2018) <https://www.asianews.it/news-en/Official-data-on-internet-censorship-42781.html> accessed 07.02.2023; see also Wawra, in this volume, at 169.

23 Ibid.

24 Mo Chen and Jens Grossklags, 'Social Control in the Digital Transformation of Society: A Case Study of the Chinese Social Credit System' (2022) 11(6) Social Sciences 229 <https://www.mdpi.com/2076-0760/11/6/229> accessed 07.02.2023; Wawra, in this volume, at 169.

most ambitious experiment in digital social control ever undertaken"[25]. Kisselburgh and Beever state:

> On a societal level, the use of social credit scoring systems (SCS) also carries the potential for large-scale systematic violations of privacy and human rights. In China, a government-mandated SCS was implemented to strengthen social governance and harmony [...]. Every citizen was assigned a 'trustworthiness' score, calculated from an algorithmic assessment of data from medical, insurance, bank, and school records; credit card and online transactions; satellite sensor data; mobile phone GPS data; and behavioral data from public cameras. Authorities use these data and the social credit score to evaluate and hold citizens accountable by imposing sanctions that range from restrictions on travel, bans on employment in civil service and public institutions, disqualification of children from private schools, and public disclosure of ratings on national websites [...]. Thus, the stakes of large-scale state surveillance include significant loss of freedoms of movement, employment, education, and reputation.[26]

In this system, credits can, for example, also be gained by "[p]raising the government on social media"[27]. Thus, there is an incentive to express a favorable attitude towards government measures.

The low value Chinese respondents place on their informational privacy towards their government can also be attributed to the people's general privacy orientation: In everyday life, the Chinese have been described as "less protective of [their] personal space and [their own as well as other's] privacy" than other cultures. Moreover, "quite loud public demeanors" are common and accepted: "People may openly express their emotions, carry out their conversations within earshot of others, sing or even dance with indifference for those around them"[28]. Furthermore, the philosophy of Confucianism remains a strong foundation of Chinese society. It promotes the acceptance of hierarchies, which are seen as natural and necessary for "harmonious, stable relations between individuals and [...] society" and the state. It teaches the importance of 'Li', 'social cohesiveness', and obedience to authorities. From this derives a strong "respect [for] the law and authority" in Chinese society and a desire "to maintain societal harmony. The Chinese consider na-

---

25 Bernhard Bartsch and Martin Gottske, 'China's Social Credit System' (2018) <https://www.bertelsmann-stiftung.de/fileadmin/files/aam/Asia-Book_A_03_China_Social_Credit_System.pdf> accessed 07.02.2023.

26 Lorraine Kisselburgh and Jonathan Beever, 'The Ethics of Privacy in Research and Design: Principles, Practices, and Potential' in Bart P Knijnenburg and others (eds), *Modern Socio-Technical Perspectives on Privacy* (2022) 412.

27 Bartsch and Gottske (n 25).

28 Chara Scroope and Nina Evason, 'Chinese Culture. The Cultural Atlas: Core Concepts' (2017) <https://culturalatlas.sbs.com.au/chinese-culture/chinese-culture-core-concepts#chinese-culture-core-concepts> accessed 07.02.2023.

tional unity and cooperation to be essential for society to function harmoniously"[29]. National cohesion and unity seem particularly important for a country with "the highest population of any country on Earth"[30]. The answers of the Chinese respondents in the surveys cited above must be interpreted against this background.

The following chapter discusses people's attitudes towards the collection of personal data by companies.

II General Value of Informational Privacy Vis-à-Vis Companies

In a survey by Ipsos, people were asked to what extent they agreed or disagreed that companies' use of data collected about them is something consumers should be able refuse or be paid or rewarded for.[31] The aggregated results for the response options 'strongly' and 'somewhat agree' are shown in the following diagram:

29 Ibid.

30 BBC, 'China's Political System and the Extent of Democratic Participation' (2022) <https://www.bbc.co.uk/bitesize/guides/zptxxnb/revision/2>; Statista, 'Total Population of China From 1980 to 2021 With Forecasts Until 2027' <https://www.statista.com/statistics/263765/total-population-of-china/#:~:text=As%20of%20mid%202021%2C%20China,of%20about%201.39%20billion%20people> accessed 07.02.2023.

31 Ipsos, 'Global Citizens & Data Privacy: An Ipsos-World Economic Forum Project' (2019) 12 <https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/ipsos-wef_-_global_consumer_views_on_data_privacy_-_2019-01-25-final.pptx_lecture_seule_0.pdf?mod=article_inline> accessed 07.02.2023: Switzerland was not part of the survey.

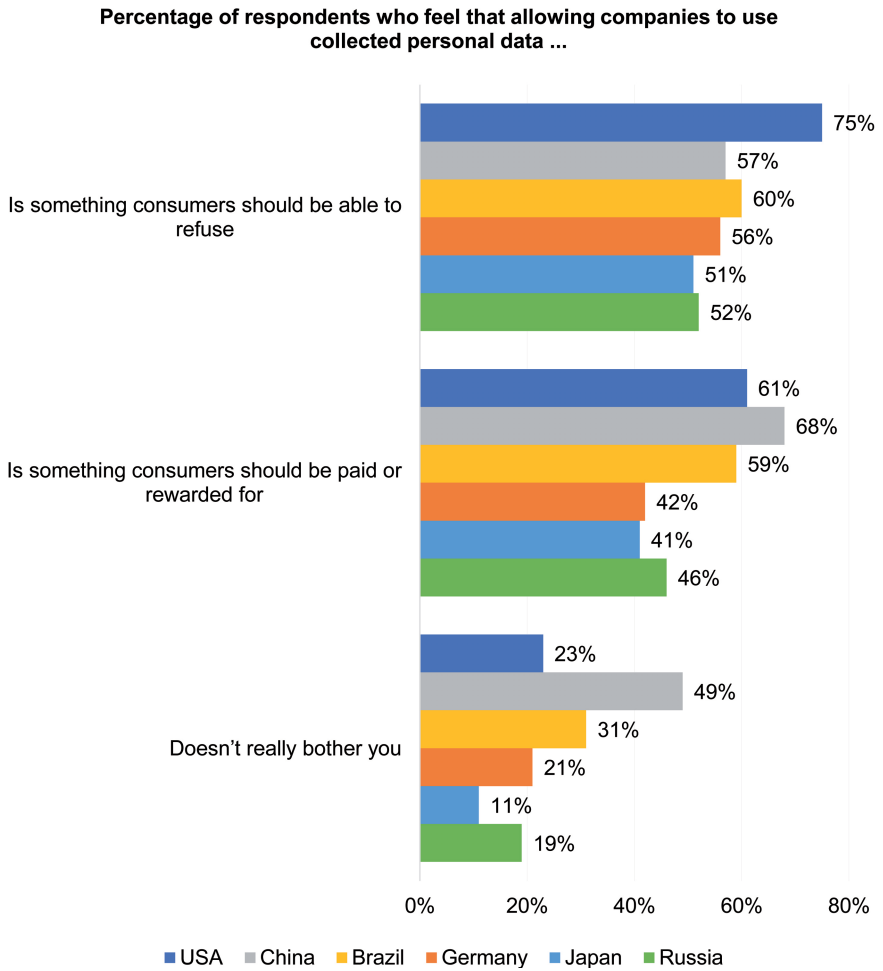

Fig. 5: Attitudes towards being able to refuse the use of collected data by companies or being paid or rewarded for it.[32]

Majorities of respondents from all countries agree that consumers should be able to refuse the collection of personal data by companies. This view is particularly common in the United States, where three quarters of respondents hold this opinion. We see here that Chinese respondents value their informational privacy higher vis-à-vis companies than towards their government (as a majority advocates that

32 Ibid.

consumers should have the right to refuse data disclosure to companies, while a majority grants their government the right to collect personal data from its citizens, even without their knowledge.[33] When it comes to the question of whether consumers should be paid or otherwise rewarded for the collection of their personal data, major cultural differences can be observed. Majorities of respondents from China, the United States, and Brazil are in favor, but only minorities in Russia, Germany, and Japan. It is therefore to be expected that – in principle – incentives for data disclosure are a more effective means of increasing the willingness of Chinese, Brazilians and US-Americans to share their personal data with companies. China again draws attention as almost half of the respondents (49 %) state that the collection of personal data by companies does not bother them. In all other countries, it is not even a third of respondents, and with the exception of Brazil, even always less than a quarter who express this attitude.

We can conclude that the majorities of respondents from all countries included want to decide for themselves whether or not to share data with companies. This indicates that they value their informational privacy in this context. It is most valued in the United States, Brazil, and China, as the results of the first survey item show. This is further underlined by the fact that it is precisely these three countries in which majorities believe that they should be paid or rewarded for disclosing their data to companies.

C Benefits Associated with Data Disclosure

What are people's assessments of the potential benefits of data disclosure to companies?[34] The following figure shows the results of a survey by Ipsos:[35]

33 See *supra,* B.I.

34 People were asked "To what extent do you agree or disagree that allowing companies to use data they collect about you" "a) Is a good thing, because it helps me find/discover products, services and information that are relevant to me," "b) Is a good thing, because it helps them to provide products, services, and information that better meet my needs," "c) Helps you save time," "d) Helps you save money", Ipsos (n 31) 12.

35 Ibid: Switzerland was not part of the survey.

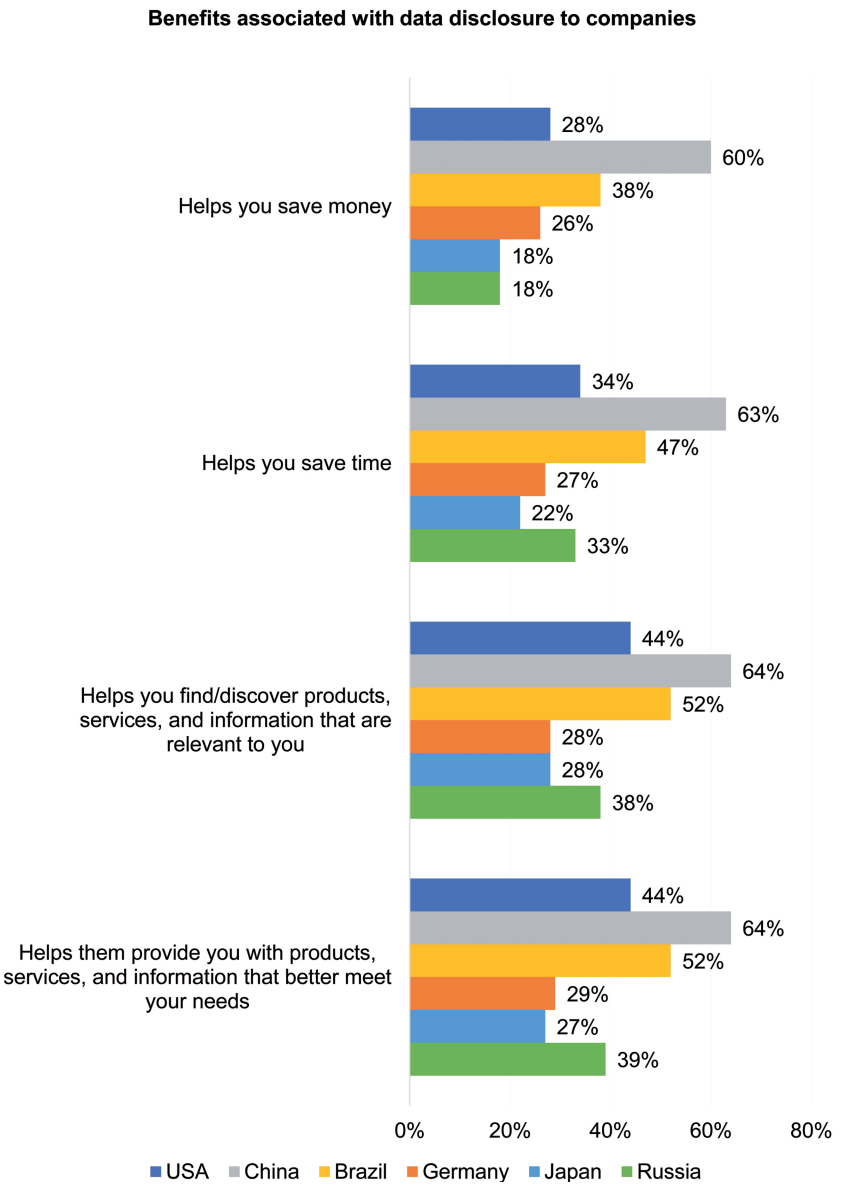

Fig. 6: Benefits associated with data disclosure in cross-cultural comparison.[36]

36 Ibid 12.

Saving money and time are seen as benefits of data disclosure only by the majority of Chinese respondents. Majorities of respondents from China and Brazil associate data disclosure with the easier discovery of relevant products, services and information, and their better provision by companies. While the majorities in Brazil are small, they are solid in China. Based on this survey, it can therefore be expected that – as a general tendency – the promotion and communication of such potential benefits of data disclosure is more effective in China and Brazil than in the other countries.

When respondents are asked directly whether they would be "willing to share [...] personal data (health, financial, driving records, energy use, etc.) in exchange for benefits or rewards like lower costs or personalized service"[37], on a seven-point Likert scale (1 meaning they do not agree at all, 7 they agree completely), 6- or 7-point agreement is found only among small minorities across all cultures included. Agreement is highest in China at 38 %,[38] followed by Russia at 29 %,[39] Brazil at 26 %,[40] the United States with 25 %,[41] Germany with only 12 %,[42] and the lowest agreement is expressed by Japanese respondents with 8 %.[43] According to the surveys above, respondents from China, Brazil and the United States were the most supportive of payments and rewards for data disclosure (see B. II) and the most convinced of benefits of data disclosure compared to the other surveyed countries (see above). Together with respondents from Russia, they are also the ones that show the highest percentages in terms of agreement on the effectiveness of incentives for data disclosure. However, the percentages are rather low (between 25 % and 38 %), so that – according to this survey – benefits and rewards are not seen as incentives to share their data by majorities across these cultures. This is somewhat contrary to the results of the Ipsos[44] survey in B. II. The differences could be attributed to the fact that, in contrast to the GfK survey[45], the Ipsos survey does not ask directly about the influence of payments or rewards on the willingness to disclose. Moreover, the GfK survey mentions highly sensitive information as examples of data that should potentially be disclosed, namely 'health' and 'fi-

37 Gfk, 'Willingness to Share Personal Data in Exchange for Benefits or Rewards' (Global Gfk Survey, 2017) <https://cdn2.hubspot.net/hubfs/2405078/cms-pdfs/fileadmin/user_upload/country_one_pager/nl/images/global-gfk_onderzoek_-_delen_van_persoonlijke_data.pdf> accessed 07.02.2023.
38 Cf ibid 74.
39 Ibid 35.
40 Cf ibid 61.
41 Ibid 52.
42 Ibid 23.
43 Ibid 78.
44 Ipsos (n 31).
45 Gfk (n 37).

nancial' data (see above, and see also in this volume on the sensitivity of personal data[46]). This could explain why people indicate that they would not share their data despite the incentives. As Ackermann and others state in their meta-study on data disclosure research:

> [C]onsumers will be very unlikely to share private data that they perceive as very sensitive, irrespective of what type of compensation they are offered in return or the degree of anonymity that is granted to them.[47]

D Privacy Concerns and Risks

Which significance does data security have in different cultures? The following chapters first discuss concerns about data security (cf D. I.), followed by concerns about data control (cf D. II.).

I Concerns about Data Security

The following figure shows how concerned or relaxed people are when it comes to the security of their data. They were asked about their agreement or disagreement with various statements on data storage and transnational data transfer.[48] Figure 7 summarizes the results:

46 Wawra, in this volume, at 169.

47 Kurt Alexander Ackermann and others, 'Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies' (2021) 21(2) Journal of Consumer Behaviour; cf also Wawra, in this volume, at 169.

48 The survey did not include Switzerland and this item was not surveyed in China.

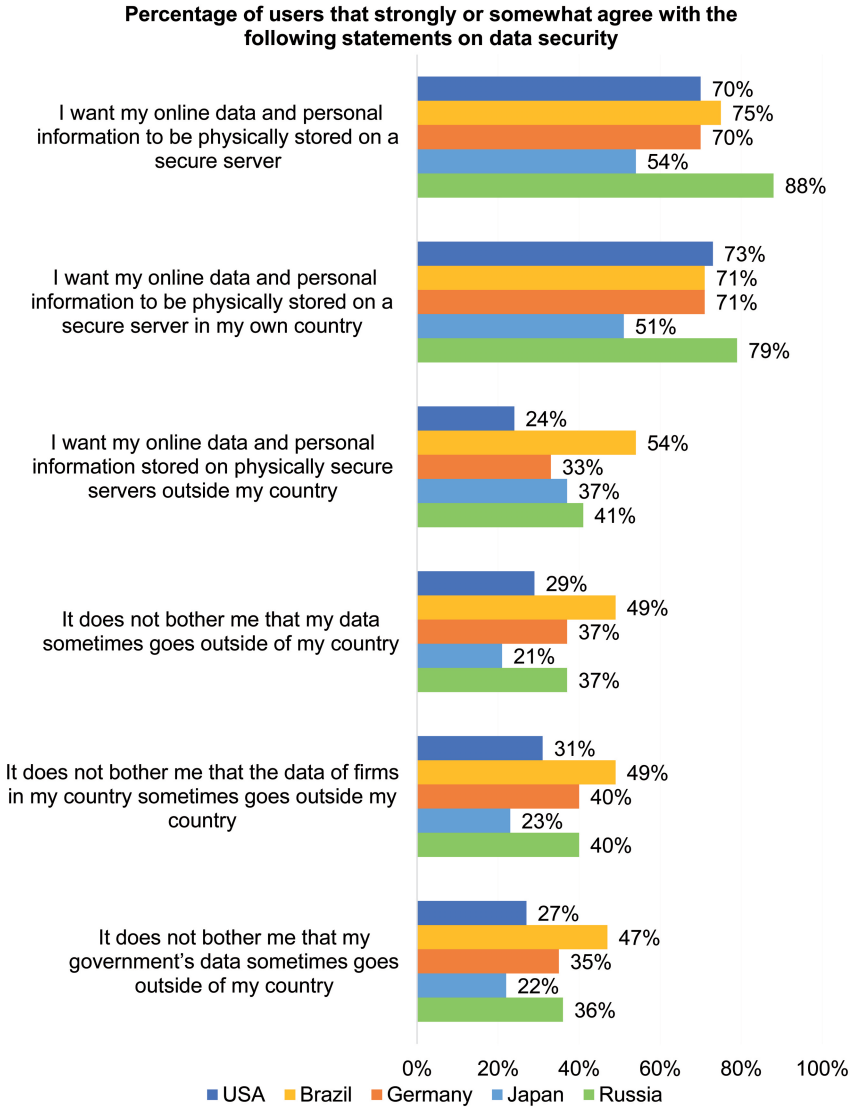

Fig. 7: Percentage of users that strongly or somewhat agree with the respective statements on data security.[49]

49 CIGI-Ipsos, 'CIGI-Ipsos Global Survey on Internet Security and Trust: Detailed Results Tables' (2019) 283 <https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/> accessed 07.02.2023.

For the majorities of respondents from all countries surveyed here, data security is important. They want their data to be stored on secure servers, preferably in their own country. This is most important for Russians and least important for respondents from Japan. Brazilian respondents are more open to having their data stored on a secure server abroad than respondents from the other countries. And although all countries have in common that it is always only minorities that are not concerned about their companies' or their government's data sometimes going outside of their country, it is again Brazilians who are clearly the least troubled by this. The survey results for Brazil can be explained by a prevailing strong distrust of the country's government and political institutions (see E.).

II Concerns about Data Control

What are the cultural trends in disclosure behavior as a consequence of concerns about data control? The following figure provides an overview:

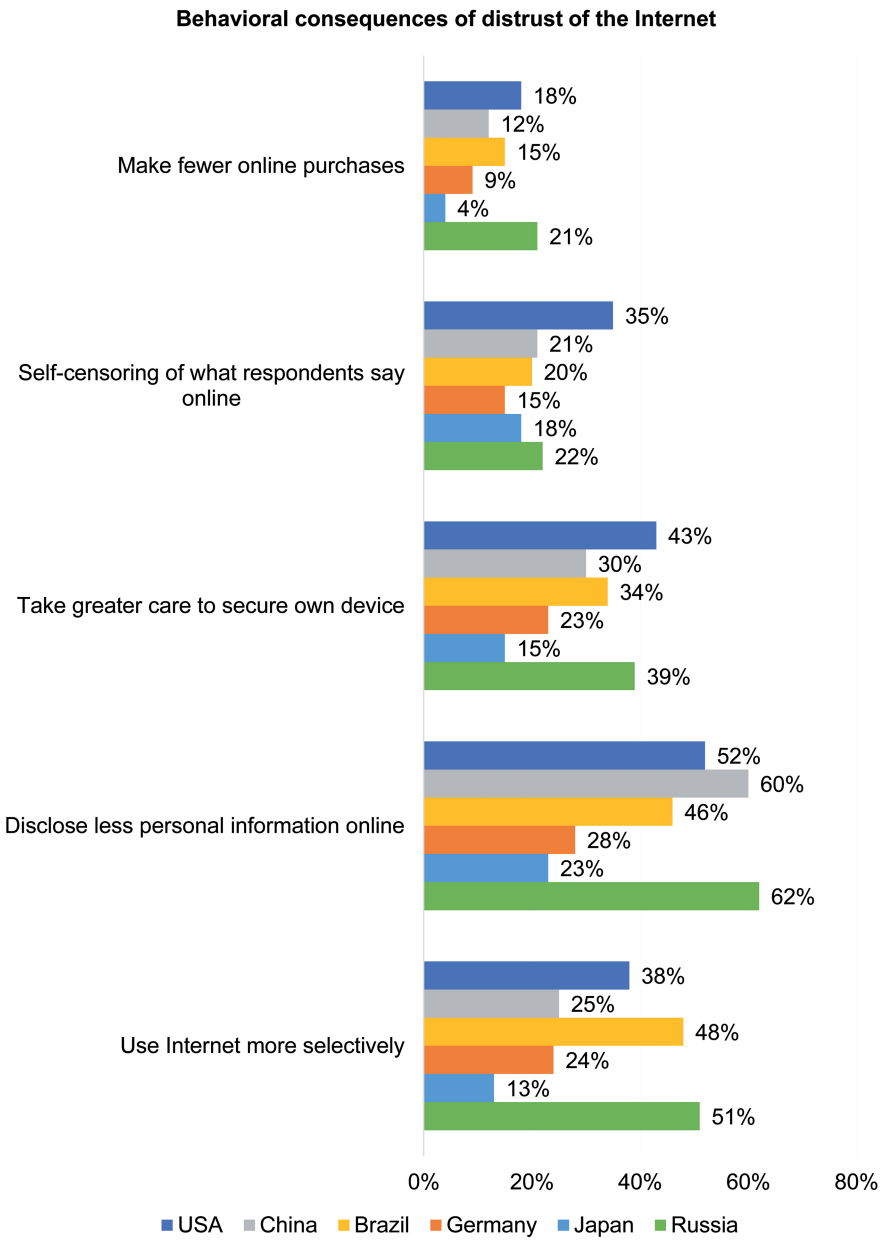

Fig. 8: Behavioral consequences of distrust of the Internet.[50]

50 Ibid 24. Switzerland was not part of the survey.

As a behavioral consequence of their distrust of the Internet, only majorities from Russia, China, and the United States report that they disclose less personal information online. The Russians surveyed are also the only ones who predominantly say they use the Internet more selectively. Minorities in all countries indicate they make fewer online purchases, self-censor online, or make more of an effort to secure their own device. It is notable that respondents from the United States (before respondents from Russia) are the ones that most frequently state that they self-censor online and take greater care to secure their device. This most likely reflects the growing political polarization in the United States: A study by Gibson and Sutherland concludes that:

> [o]ver the course of the period from the heyday of McCarthyism to the present, the percentage of the American people not feeling free to express their views has tripled. In 2019, fully four in ten Americans engaged in self-censorship.[51]

Gibson and Sutherland establish the following links: The "[l]evels of self-censorship are related to affective polarization among the mass public, [...] greater polarization is associated with more self-censorship." The authors identify "micro-environment sentiments" as the drivers of self-censorship, ie, "worrying that expressing unpopular views will isolate and alienate people from their friends, family, and neighbors." Gibson and Sutherland comment:

> [...] unless one can completely isolate oneself from the toxic political environment of contemporary America, it is perhaps prudent to withhold one's views, at least in certain contexts. Free speech has never been free; but the cost of such speech today seems to have skyrocketed – and, to some, the cost may have become exorbitant and out-of-reach.[52]

According to this study, those with the most to lose are most likely to report self-censorship, ie, mainly people with more resources, including a higher level of education.[53]

51 James L Gibson and Joseph L Sutherland, 'Keeping Your Mouth Shut: Spiraling Self-Censorship in the United States' [2020] SSRN Journal.

52 Ibid.

53 Cf ibid.

E Trust in Data Recipients

An important dimension that can have a great impact on the willingness to share personal data is trust. In general, the more people trust a data recipient, the more willing they are to disclose data. In the following, we therefore examine people's basic trust in frequent data recipients on an aggregated cultural level.

We will begin by looking at the wider cultural contexts and here at people's general levels of trust (Fig. 9). In an /WVS survey[54], people were asked whether they thought that most people could be trusted or that one needed to be careful when dealing with people.

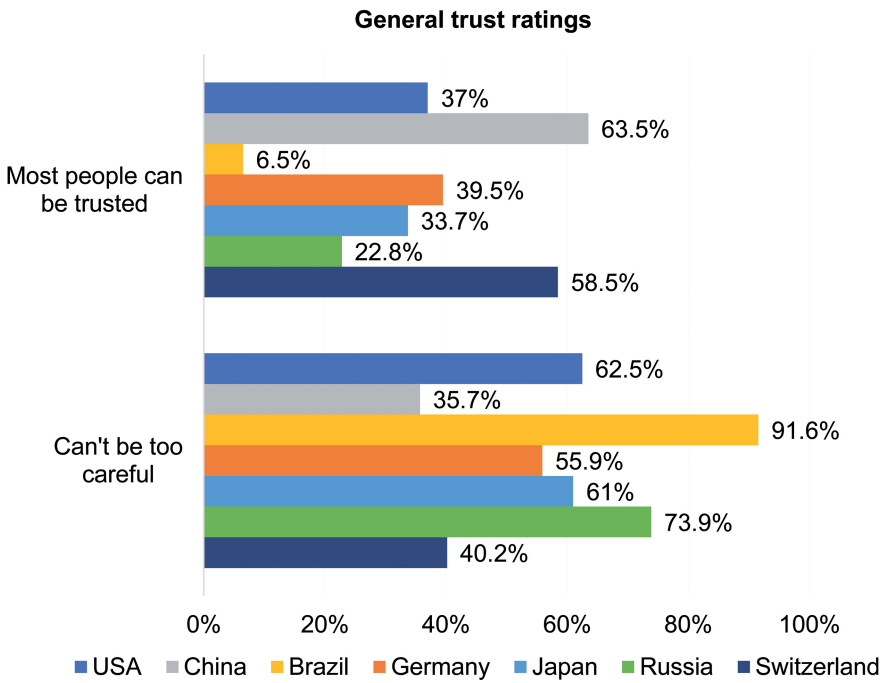

Fig. 9: Trust towards others in cross-cultural comparison.[55]

According to this survey, the Chinese are by far the most trusting people, at least according to their self-report (which, along with other results for China, could be

54 EVS/WVS (n 12).
55 Ibid 180, 181.

biased for the reasons discussed above, see B. I.). Switzerland is the only other country included where a large majority of respondents also say they trust most people. In all other cultures, distrust predominates. Brazilians are the most skeptical.

What picture emerges regarding people's trust in their own government?

I Trust in Governments

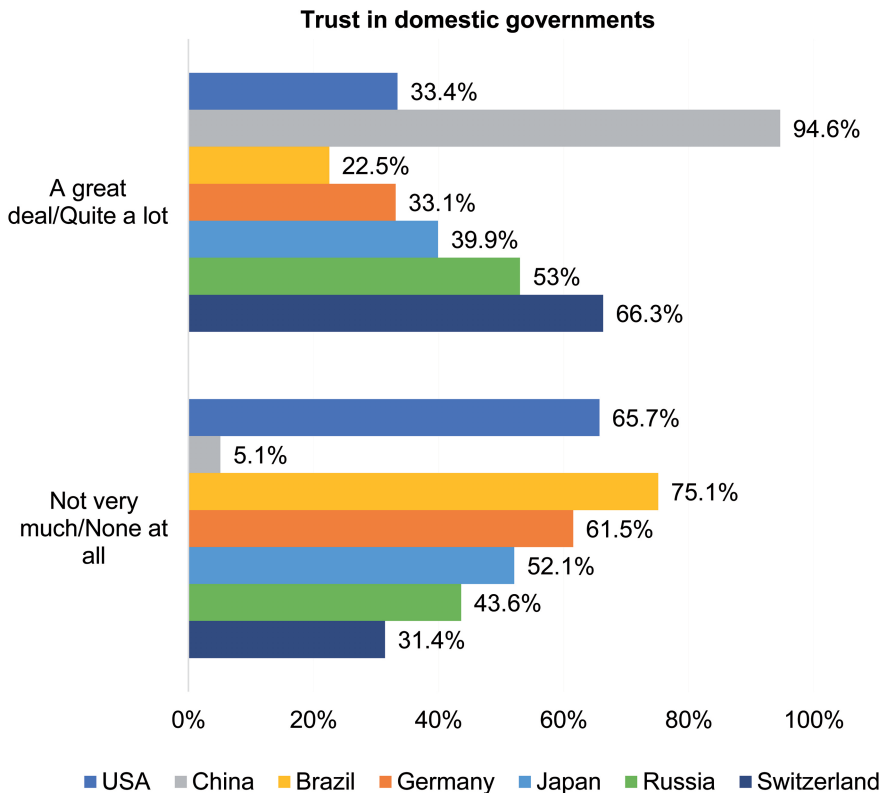

Fig. 10: Trust in domestic governments.[56]

Chinese respondents overwhelmingly express trust in their government (see B. I. for an explanation). Majorities in Switzerland and Russia also trust their governments. Brazil leads the list of countries where people mostly distrust their govern-

56 Ibid 279, 280.

ments, followed by the United States, and Germany. Brazilians' particularly pronounced distrust of their government coincides with the frequently stated cultural observation that "skeptical attitudes towards political institutions prevail in Brazilian civil society," and that "there is a widely held belief that the government and law enforcement bodies are corrupt"[57].

Looking at the narrower cultural context of data disclosure, trust in domestic governments to use collected personal data correctly[58] (cf Fig. 11 below) is considerably higher at 41% than general trust in the government in Brazil at 22.5%; respondents in Germany and the United States express slightly more confidence in this respect (37% compared to 33.1% general trust for Germany, 34% and 33.4% general trust for the United States). In Russia, trust in the correct handling of personal data by the government is significantly lower at 36% than the reported general trust in the government at 53%.[59]

In none of the countries surveyed does a majority report having trust in their domestic government to use personal data in the right way. Even fewer people trust foreign governments. Respondents from China are the ones who trust foreign governments the most, but they are still a minority (at 44%). The following chapter discusses people's trust in companies.

57 Chara Scroope, 'Brazilian Culture. The Cultural Atlas: Core Concepts' (2018) <https://culturalatlas.sbs.com.au/brazilian-culture/brazilian-culture-core-concepts> accessed 07.02.2023.

58 Ipsos (n 31) 20: People were asked "To what extent, if at all, do you personally trust the following institutions to use the information they have about you in the right way?".

59 There are no survey data from China and Switzerland regarding this item.

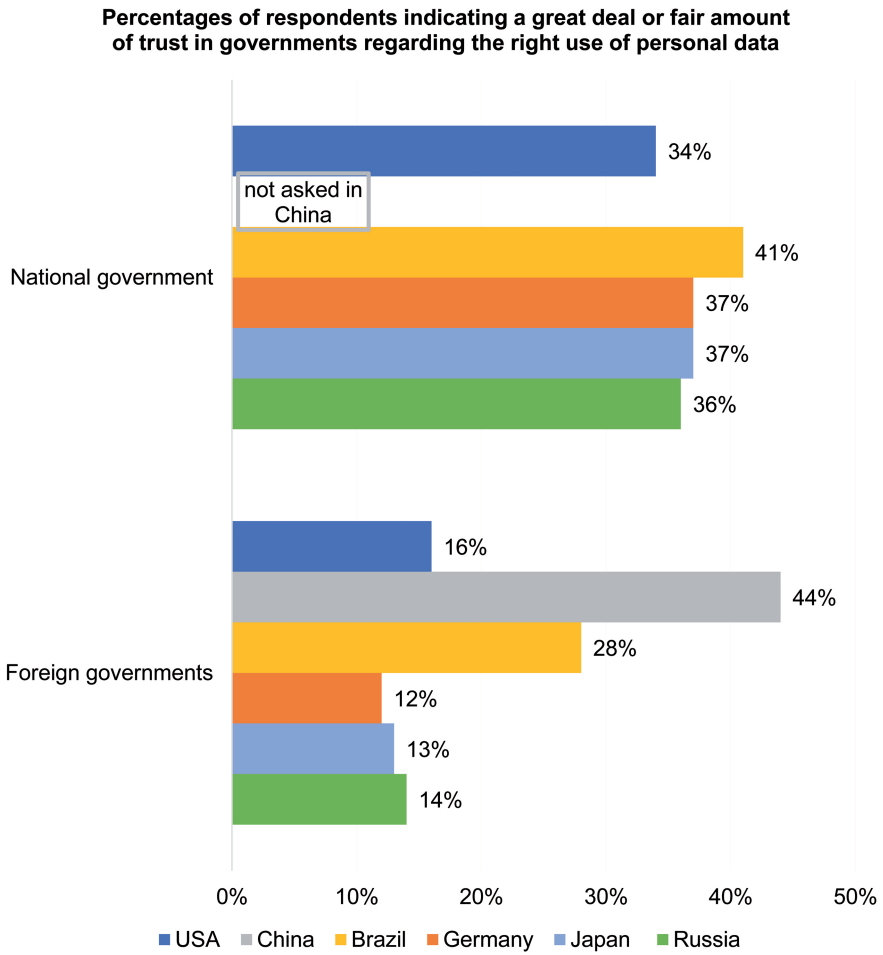

Fig. 11: Percentages of respondents indicating a great deal or fair amount of trust in governments regarding the right use of personal data.[60]

60 Ipsos (n 31) 20.

II Trust in Companies

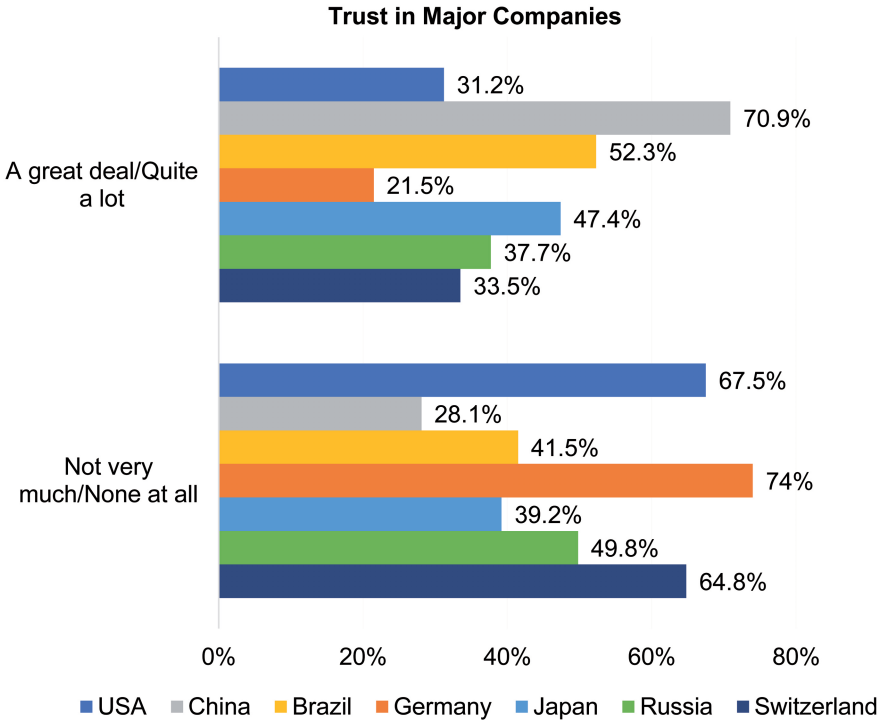

Fig. 12: Trust in major companies in cross-cultural comparison.[61]

Overall, well over 50 % (70.9 %) of respondents from China express their general trust in major companies. Still more than half of the respondents from Brazil trust companies. Distrust is by far most common among respondents from Germany, followed by respondents from the United States and Switzerland. In all three countries, significantly more than half of the respondents express their distrust of major companies.

If we compare people's trust in their domestic governments' efforts to protect their data with that of companies (see Fig. 13 below), respondents across all cultures clearly trust the companies[62] they use more than their governments. Trust in companies in this regard is expressed by 66 % of Brazilian respondents, followed by Russians at 60 %, Germans at 55 %, and US Americans at 50 %. Japan is

61 EVS/WVS (n 12) 283, 284.

62 The item was not surveyed in China and Switzerland.

the only country where only a minority of respondents have confidence in the data protection efforts of companies. Apart from Japan, respondents from all other countries express more trust in the companies they use when it comes to data protection than in companies in general (cf Figs. 12 and 13). One reason for this is likely to be that they select companies they consider to be trustworthy in this respect.

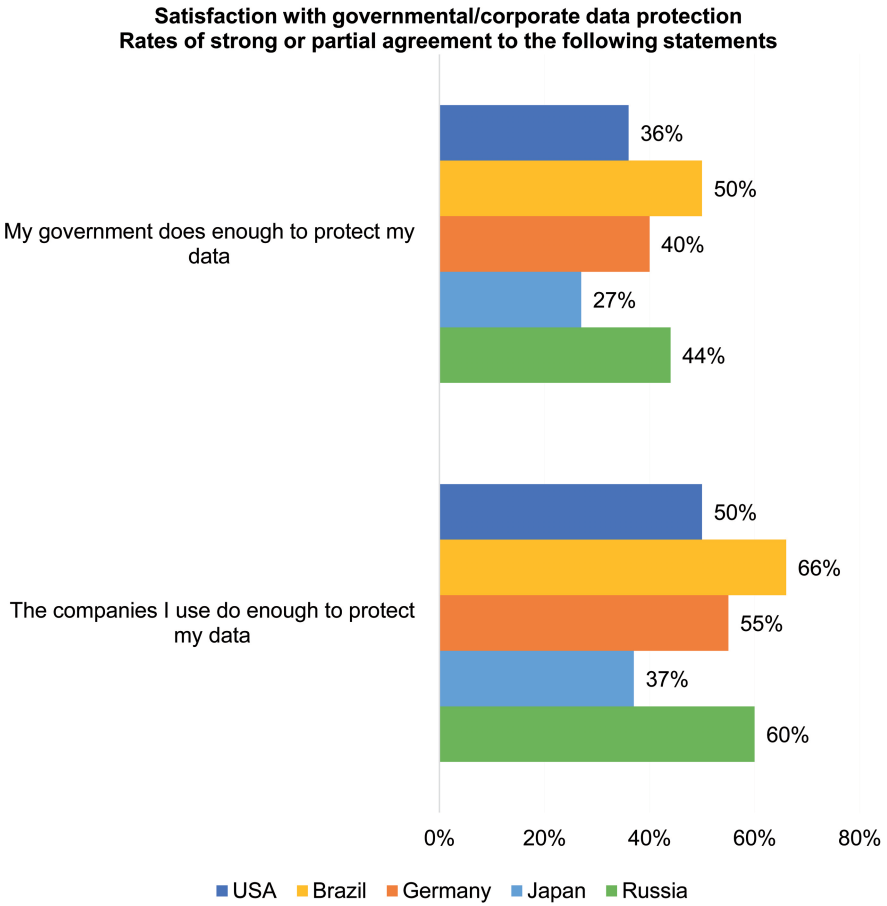

Fig. 13: Satisfaction with data protection by the government and by companies in cross-cultural comparison.[63]

63 CIGI-Ipsos (n 48) 283.

A closer cross-cultural look at people's trust in different industries regarding the correct use of personal data yields the following results:[64]

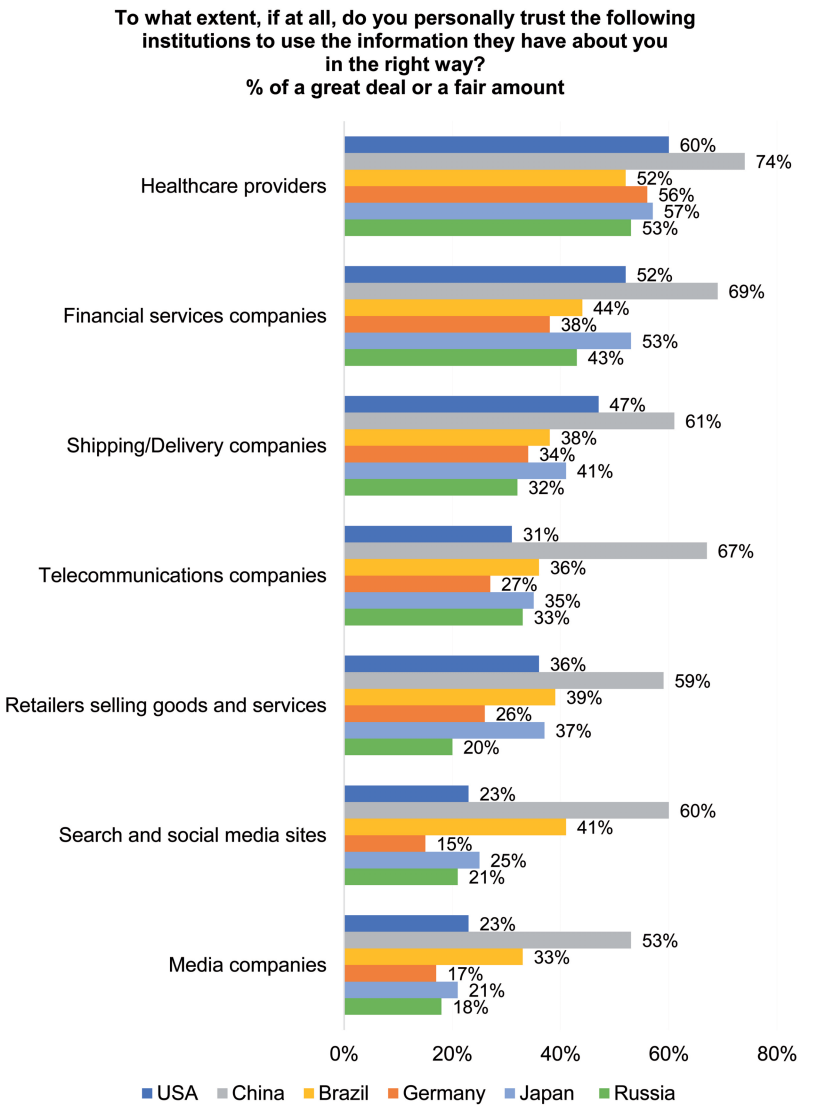

Fig. 14: Trust in different industries to use collected data correctly in cross-cultural comparison.[65]

64 Switzerland was not part of the survey.

65 Ipsos (n 31) 18, 19, 20.

In all countries, healthcare providers enjoy the highest level of trust regarding the correct handling of personal data. Across all countries, more than 50 % of respondents express their trust in this respect. Chinese respondents lead not only with regard to trust in healthcare providers, but regarding all industries mentioned in the survey. It is always a majority of respondents from China who express their trust in the data protection measures of the various industries. Japan and the United States are the only other countries with trust rates above 50 % for financial services companies. Regarding all other industries, only minorities in all countries (with the exception of China) have confidence that their data is handled correctly. In Germany and Russia, trust in this regard is lowest for all sectors surveyed with the exception of healthcare. We can conclude from this that healthcare providers have by far the best reputation for personal data protection in all countries surveyed. Financial services companies are in second place, while media companies have the worst reputation.

Majorities of respondents from all cultures, with the exception of Japan, are more willing to share their data with companies that do not have a history of data misuse and with which they have a lot of experience (cf Fig. 15 below). Both obviously increase their trust in them. This mindset is most widespread in Russia, followed by the United States. One reason for the relaxed attitude of Japanese respondents in this regard stems from their pragmatic approach to privacy.[66]

66 For more details, cf Wawra, in this volume, at 169.

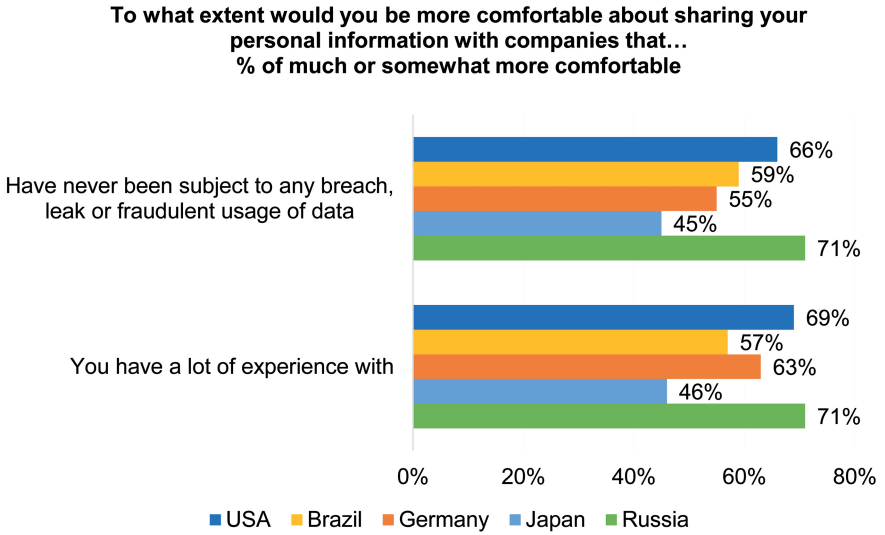

Fig. 15: Willingness to share data with frequently used companies with no history of data misuse.[67]

F Transparency / Communication on Data Use

Finally, can communication increase the willingness to share data in different cultures? Majorities in all cultures report that they would be more comfortable sharing their data if companies communicated the use of the data transparently (cf Fig. 16).[68] Most Russian respondents, followed by US respondents, indicate this, with the majority among Japanese respondents being the smallest. It can therefore be assumed that transparent communication in this respect increases the basic willingness to disclose personal data in all cultures included, particularly in Russia and the United States.

67 Ipsos (n 31) 14.

68 China and Switzerland were not part of the survey.

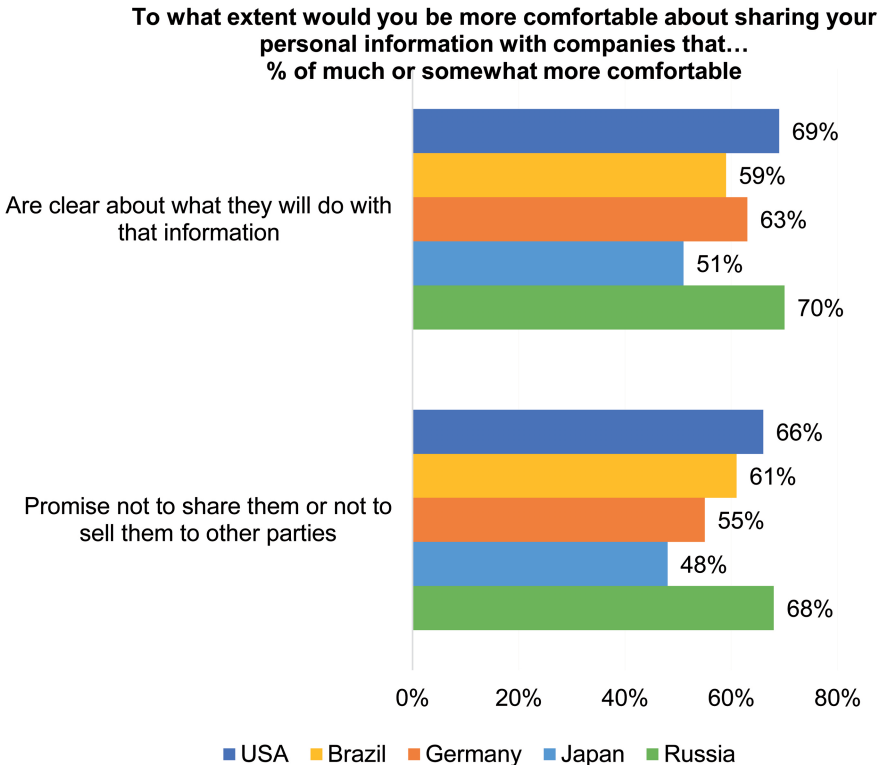

Fig. 16: Attitudes towards communication on data use in cross-cultural comparison.[69]

If companies promise not to share collected data with third parties, this will also mostly increase people's willingness to disclose personal data across all cultures, except in Japan[70], where only a minority of respondents say they would be more comfortable about sharing their data under these circumstances (see Fig. 16 above). According to these survey results, it would again generally be most promising to make such a commitment to Russian and US customers.

69 Ipsos (n 31) 14.

70 This could again be due to the general tendency in Japan to take a pragmatic and relaxed approach to privacy (see above and Wawra, in this volume, at 169).

G Discussion of the Explanatory Potential of Cultural Dimension Models

The cross-cultural comparison of the survey results has shown that there is cultural variation with regard to key parameters that can influence the willingness to share data. Some explanatory cultural factors for noticeable findings have already been included in the chapters above. Can we also attribute these differences to cross-cultural variation in general cultural dimensions that are often used to capture countries' prevailing value orientations and practices? Cultural dimensions are mainly used to compare the wider cultural contexts that might have an impact on the value people place on informational privacy in particular, but also on other parameters of data disclosure. At country level, cultures have mostly been compared using Hofstede's dimensions[71], another established model is Globe's[72].

Li's meta-study[73], for example, refers to Hofstede's dimensions when discussing "major cross-cultural differences that have been reported in privacy research." In relation to privacy, according to Li, the *Individualism-Collectivism dimension*[74] plays an important role.[75] In contexts of data disclosure where the data recipient is an organization, Li claims that "individualism has a positive association with information privacy concerns,", ie, individualistic cultures would be characterized by higher perceptions of privacy risks when sharing personal data.[76] This would also result in "more protective behaviors, such as securing sen-

71 Geert Hofstede, 'The Dimensions of National Culture' (2022) <https://hi.hofstede-insights.com/national-culture> accessed 07.02.2023; Geert Hofstede, 'Country Comparison Graphs' (2022) <https://geerthofstede.com/country-comparison-graphs/> accessed 07.02.2023.

72 Globe, 'Country List' (2020) <https://globeproject.com/results/countries/BRA?menu=country#list>, <https://globeproject.com/results/countries/CHN?menu=list#list>, <https://globeproject.com/results/countries/DEU?menu=country#country>, <https://globeproject.com/results/countries/JPN?menu=list#list>, <https://globeproject.com/results/countries/RUS?menu=list#list>, <https://globeproject.com/results/countries/CHE?menu=list#list>, <https://globeproject.com/results/countries/USA?menu=list#list> accessed 07.02.2023.

73 Li (n 1).

74 Hofstede, 'The Dimensions of National Culture' (n 70) defines this dimension as follows: "Individualism [...] can be defined as a preference for a loosely-knit social framework in which individuals are expected to take care of only themselves and their immediate families. Its opposite, Collectivism, represents a preference for a tightly-knit framework in society in which individuals can expect their relatives or members of a particular ingroup to look after them in exchange for unquestioning loyalty. A society's position on this dimension is reflected in whether people's self-image is defined in terms of 'I' or 'we'".

75 Li (n 1).

76 Ibid.

sitive personal information"[77]. Collectivist cultures, on the other hand, would "tend to be less sensitive to privacy concerns," and "appear to trust data collection entities more and are more willing to share information with these entities"[78].

Furthermore, Li and others[79] claim that online users in both individualist and collectivist countries respond positively to customization, time or money savings, and benefits from disclosing personal data. Customers from individualistic cultures would be more likely to share their data with paid services and organizations with which they already have a relationship. Customers from collectivist countries would be more likely to share their data with their government and their employers:

> People in collectivistic cultures such as China and India are relatively more accepting of data collection performed by the government than people in individualist cultures such as the USA and Canada. Data collection by users' employers is also better accepted in collectivistic cultures. People in individualist cultures are relatively more accepting of data collection when they either pay for or already have an existing relationship with the service provider.[80]

Li claims that "[v]alue exchange,", ie, "what value users can obtain from personal data sharing," such as saving time and money or getting a recompense "are appealing values from data collection in both individualistic and collectivistic countries." Altruistic value, ie, benefits for the community, are "more acceptable in collectivistic countries and less acceptable in individualistic countries. This indicates that users in individualistic countries cannot be swayed by benefits to the community"[81].

Do the survey data presented above support such claims? In the following, data disclosure to the government is used as an example. If we rank the countries included here on an individualism-collectivism continuum according to their score on Hofstede's cultural dimension[82], we obtain the following results: Countries with a predominant individualistic orientation (IDV above 50) are the United States (IDV 91), Switzerland (IDV 68) and Germany (IDV 67); countries with a predominant collectivistic orientation (IDV below 50) are Japan (IDV 46), Russia (IDV 39), Brazil (IDV 38), and China (IDV 20). With regard to data disclosure to the government, for ex-

---

77 Ibid.

78 Li (n 1).

79 Yao Li and others, 'Cross-Cultural Privacy Prediction' (2017) 2017(2) Proceedings on Privacy Enhancing Technologies 113.

80 Li (n 1).

81 Ibid.

82 Hofstede, 'The Dimensions of National Culture' (n 55); Hofstede, 'Country Comparison Graphs' (n 70).

ample, we would therefore expect – relating the Hofstede scores to the results of the surveys discussed above – that respondents from the collectivistic oriented countries would be more willing to share data with their government than respondents from individualistic countries. This association can be confirmed for China: according to Hofstede, it is the most collectivistic oriented culture,[83] and in the surveys the largest majorities of respondents who are open to data sharing and in favor of governmental data collection rights could be found among the Chinese. Brazil and Russia, however, do not rank second and third in this regard, as would be expected given their low scores on individualism. In fact, Brazilian respondents were the least open to governmental video surveillance in public spaces, with Russians in 5th place. In terms of accepting the collection of information without their knowledge on anyone living in the country, Brazilians rank 4th, Russia ranks 3rd, but the most individualistically oriented country, the United States, ranks 2nd here, after China. In terms of approval of online monitoring, Russia ranks 2nd, Brazil only 6th, while Switzerland (3rd) and Germany (4th) are placed before it as more individualistically oriented countries. So summing up, if we only look at the general tendencies provided by the Hofstede scores for the countries and check whether the hypotheses can be confirmed that the three more individualistic countries are less open to data sharing than the three collectivistic oriented countries, we would expect the United States, Switzerland and Germany (individualistic countries) to occupy between 5th and 7th place, and China, Brazil, Russia, and Japan to occupy ranks one to four, yet these predictions do not hold either.

Is Hofstede's *Power Distance* dimension[84] a better predictor of cross-cultural differences in people's attitudes towards data collection by their government? The hypothesis would be that the higher a country's score on this dimension, the less the members of this culture value their informational privacy towards governments and corporations, because they are more accepting of authority. We would therefore expect that the higher a country's Power Distance score, the higher the percentage of respondents who say that surveillance measures do not bother them and that governments should have the right to collect their data, regardless of the context. Can this hypothesis be confirmed?

The countries with a predominantly high power distance orientation (PDI above 50) are Russia (PDI 93), followed by China (PDI 80), Brazil (PDI 69), and Japan (PDI 54). Countries with a rather low power distance orientation (PDI

83 Hofstede, 'Country Comparison Graphs' (n 70).

84 Hofstede defines Power Distance as the "degree to which the less powerful members of a society accept and expect that power is distributed unequally." A high score on the PDI means that "people accept a hierarchical order in which everybody has a place and which needs no further justification", Hofstede, 'The Dimensions of National Culture' (n 70).

below 50) are the United States (PDI 40), Germany (PDI 35), and Switzerland (PDI 34). However, Russian respondents are not the most open to sharing data with their government in the three contexts surveyed (as would be expected according to the hypothesis formulated above): They rank 5th (relating to openness to video surveillance), 3rd (with regard to information collection), and 2nd (with regard to information collection online). Swiss respondents would be expected to be the least open to data collection (because of the country's low PDI), but they rank 4th, 5th, and 3rd in these contexts of disclosure.

Are Globe's cultural dimensions[85], rather than Hofstede's[86], consistent with the survey results presented above? The low value Chinese respondents place in their informational privacy in relation to their government is consistent with China having the highest country value score (3.1) on Globe's Power Distance (PD) dimension[87] among the seven countries included here. However, the relation does not hold for the survey results in the other countries: Japan, for example, has the second highest Power Distance value score at 2.86 and Brazil the lowest at 2.35, according to Globe. However, Japanese respondents do not rank second after China with regard to a low value for informational privacy vis-à-vis their government, nor do Brazilian respondents express the highest value for their informational privacy vis-á-vis their government of all the countries included here.

Another cultural dimension that could help explain survey results is *Uncertainty Avoidance.* Wawra discusses it in this volume in connection with perceived data sensitivity and also concludes that it cannot be linked directly to the survey results.

These examples demonstrate how problematic it is to try to link survey results in a specific area such as data disclosure directly to general cultural dimensions such as those established by Hofstede[88] and the Globe study[89].[90] This is evident from the very fact that the countries are ranked differently according to Globe's in comparison to Hofstede's[91] Power Distance dimension, for example, although

85 Globe, (n 71).

86 Hofstede, 'The Dimensions of National Culture' (n 70); Hofstede, 'Country Comparison Graphs' (n 70).

87 According to Globe (n 71), Power Distance (PD) is defined as the "extent to which the community accepts and endorses authority, power differences, and status privileges". The Globe study usually differentiates between country practice (what is) and country value scores (what should be); for PD, only a value score is provided.

88 Hofstede, 'The Dimensions of National Culture' (n 70); Hofstede, 'Country Comparison Graphs' (n 70).

89 Globe (n 71).

90 Cf also Wawra, in this volume, at 169, for a critical discussion of this practice.

91 Hofstede, 'The Dimensions of National Culture' (n 71).

they are supposed to capture essentially the same thing.[92] Neither with any of Hofstede's dimensions[93], nor with those of the Globe study could a solid and consistent connection be established with the survey results. One major reason for this is that the cultural dimensions comprise a variety of aspects that are summarized under one dimension, as shown not least by the breadth of the survey questions used to identify the cultural dimensions.[94] The cultural dimensions are thus too broad to have any direct explanatory power for certain areas of research, such as specific aspects of data disclosure. Furthermore, there is the question of the stability and representativity of the cultural values as expressed by the dimensions and that of the survey results.[95] As the discussions of possible cultural influences on the attitudes and views expressed by respondents in the previous chapters have shown, multiple cultural factors may influence people's decisions regarding data disclosure. Thus, one or several of these factors might have a greater impact in certain contexts of data disclosure, and they might even work in different directions – like vectors. Nevertheless, all of them should be considered as potential influences on data disclosure.

H Conclusion and Outlook

Influences on a person's willingness to share data in concrete disclosure scenarios are multifaceted and their interplay is complex. In this comparative cross-cultural study, a macro-perspective was adopted, ie, people's attitudes in areas that may influence their willingness to share data were compared across nations, we abstracted from details and aggregated individual and contextual data.[96] Masur and others attribute to such an approach a value in its "own right, given the inherent tension between global information infrastructures and localized user experiences"[97]. Individual and socio-demographic factors (such as age, education, ethnicity, gender,

92 Cf previous footnotes.

93 Hofstede, 'The Dimensions of National Culture' (n 70); Hofstede, 'Country Comparison Graphs' (n 70).

94 Cf Globe (n 70) and Geert Hofstede, 'Values Survey Module' (2013) <http://geerthofstede.com/wp-content/uploads/2016/07/VSM-2013-English-2013-08-25.pdf>, respectively; for criticism see also Philipp Gerlach and Kimmo Eriksson, 'Measuring Cultural Dimensions: External Validity and Internal Consistency of Hofstede's VSM 2013 Scales' (2021) 12 Frontiers in psychology 662604.

95 Cf Wawra, in this volume, at 169.

96 Cf Philipp K Masur and others, *A Comparative Privacy Research Framework* (2021) 12; Kurt Dopfer, John Foster and Jason Potts, 'Micro-Meso-Macro' (2004) 14(3) Journal of Evolutionary Economics 263, 267.

97 Ibid 12.

income, political orientation, rural or urban neighborhood) were thus not taken into account here. Such data are difficult to compare, not least because they have not been surveyed systematically across all cultures within our research context. The data situation in this respect is poor in most of the countries we included in our study. The data basis is broadest for the United States and Germany, and we included socio-demographic details, where possible, in the individual country reports that were compiled in our project. The results show that there can be considerable intra-cultural variation for different parameters of data disclosure.[98] More cross-cultural studies are needed that explicitly include and evaluate personality traits and socio-demographic factors and their influence on data disclosure, especially ones that compare more than two and further countries than Germany and the United States.

Another caveat is that the surveys sometimes ask for personal data in general, or include personal data with very different levels of sensitivity as examples. This may, however, influence the responses of the respondents. In their meta-study of data disclosure literature, Ackermann and others, for example, conclude that the more sensitive the data are rated by respondents, the less other variables (such as benefits of disclosure) influence people's willingness to share personal data:

98 Cf Howe (n 7); Kessel (n 7); see also Drew DeSilver, 'Young Americans and Privacy: It's Complicated' (2013) <https://www.pewresearch.org/fact-tank/2013/06/20/young-americans-and-privacy-its-complicated/> accessed 07.02.2023; Mary Madden, 'Privacy and Security Experiences of Low-Socioeconomic Status Populations' (2015) <https://datasociety.net/library/privacy-security-and-digital-inequality/> accessed 07.02.2023; Mary Madden, 'Privacy, Security, and Digital Inequality' (27 September 2017) <https://datasociety.net/library/privacy-security-and-digital-inequality/> accessed 07.02.2023; Sabine Trepte and Philipp K Masur, *Privacy Attitudes, Perceptions, and Behaviors of the German Population* (2017) <https://www.philippmasur.de/documents/pubs/Trepte_Masur_2017_Research_Report_Hohenheim.pdf> accessed 07.02.2023; Brooke Auxier and others, 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information' (19 November 2019) <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/> accessed 07.02.2023; Brooke Auxier, 'How Americans See Digital Privacy Issues Amid the COVID-19 Outbreak' (2020) <https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/>; Franziska Herbert, Gina M Schmidbauer-Wolf and Christian Reuter, *Differences in IT Security Behavior and Knowledge of Private Users in Germany* (2020) <https://library.gito.de/wp-content/uploads/2021/08/V3_Herbert-Differences_in_IT_Security_Behavior_and_Knowledge-541_c.pdf> accessed 07.02.2023.

> In other words, consumers will be very unlikely to share private data that they perceive as very sensitive, irrespective of what type of compensation they are offered in return or the degree of anonymity that is granted to them.[99]

Previous research[100] also indicates that people's willingness to share data can be improved by giving them a sense of control over their data. This can be achieved by offering an option to delete data and/or by granting anonymity. Ackermann and others even rate the guarantee of anonymity as "the most effective single factor for evoking WTS [willingness to share]"[101]. However, this does not seem to apply to the case of very sensitive data.[102] In general, disclosure of data is also more likely when the requested data are consistent with a recipient's mission and responsibilities.[103]

This shows that actual data disclosure behavior is difficult to predict. It depends on the concrete data disclosure situation, which potentially influential factors of data disclosure play a more or less prominent role, and also on whether individuals make a conscious choice or disclose their data rather thoughtlessly.[104] There are therefore still many research desiderata in the broad field of data disclosure.

---

99 Ackermann and others (n 46).

100 Cf eg Donna L Hoffmann, Thomas P Novak and Marcos P Peralta, 'Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web' (1999) 15(2) The Information Society 129; Bjoern Roeber and others, 'Personal data: how context shapes consumers' data sharing with organizations from various sectors' (2015) 25(2) Electron Markets 95; Ackermann and others (n 46).

101 Ackermann and others (n 46).

102 Cf ibid.

103 Cf ibid.

104 Melanie Kim, Kim Ly and Dilip Soman, *A Behavioural Lens on Consumer Privacy: Behavioural Economics in Action Research Report Series* (Rotman School of Management, University of Toronto 2015); Ackermann and others (n 46); Wawra, 'The Cultural Context of Personal Data Disclosure Decisions' (n 4) 6.

Jana Dombrowski

What Does It Take? Factors Determining Individual Privacy Regulation

A Individual Privacy Regulation Behavior

The internet is bursting with tips on how to protect privacy on social media by using privacy settings.[1] Restricting access to one's profile, removing users from the contact lists, and prohibiting direct messages from strangers are just a few examples of what media outlets and official institutions recommend; all of them come with some form of restriction or withdrawal. But social media is an integral part of individuals' social routines.[2] Social media helps them, for example, to communicate and coordinate meetings with close peers, to manage their image and reputation, and to acquire new contacts. Thus, from an individual's perspective, restricting their online experience thus is not always a sufficient option to manage privacy.

Jana Dombrowski is an academic research assistant at the Chair of Media Psychology (Prof. Dr. Sabine Trepte) at the University of Hohenheim, jana.dombrowski@uni-hohenheim.de.

1 Eg Europol, 'How to set your privacy settings on social media' (2021) <https://www.europol.europa.eu/how-to-set-your-privacy-settings-social-media> accessed 07.02.2023; T. Klosowski, 'How to protect your digital privacy' (31 August 2022) <https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy> accessed 07.02.2023.

2 Michael A Jenkins-Guarnieri, Stephen L Wright and Brian Johnson, 'Development and validation of a social media use integration scale' (2013) 2(1) Psychology of Popular Media Culture 38; Charles Steinfield, Nicole B Ellison and Cliff Lampe, 'Social capital, self-esteem, and use of online social network sites: A longitudinal analysis' (2008) 29(6) Journal Of Applied Developmental Psychology 434.

https://doi.org/10.1515/9783111010601-006

In general, privacy regulation behavior is defined as the management of interpersonal boundaries.[3] According to the latest Eurobarometer on privacy, European social media users are very concerned about their privacy.[4] However, only half tried to change default privacy settings because they trust companies to provide appropriate settings.[5] Insights from a panel study conducted in the Netherlands show that individuals protect their online privacy rarely to occasionally.[6] The most common privacy behaviors are the deletion of cookies and browser histories.[7] Research confirms that this behavior is, unlike previously claimed, not paradox at all.[8] Rather, the process of privacy regulation is more complex as it is characterized by a continuous act of balancing opposing forces.[9] Similarly, privacy behaviors are manifold and range from corrective to preventive, from individual to collaborative, and from behavioral to mental tactics.[10]

This highlights a critical question: What does it really take for individual privacy regulation? The aim of this paper is to give an overview of theoretical and empirical contributions from communication science and media psychology to understand the process and predictors of individual privacy regulation. First, I outline the understanding of privacy in the disciplines of communication science and psychology. Next, I highlight the most important theories explaining (privacy) regulation behavior and summarize empirical evidence on privacy regulation by mainly focusing on social media privacy. Lastly, I emphasize important theoretical and empirical implications for the understanding of individual privacy regulation.

---

3 Irwin Altman, 'Privacy: A conceptual analysis' in Stephen T Margulis (ed), *Man-environment interactions: Evaluations and applications* (Dowden, Hutchinson & Ross 1974).

4 European Commission, 'Special Eurobarometer 499: Europeans' attitudes towards cyber security' (2020).

5 Ibid.

6 Sophie C Boerman, Sanne Kruikemeier and Frederik J Zuiderveen Borgesius, 'Exploring motivations for online privacy protection behavior: Insights from panel data' (2018) 25 Communication Research <https://journals.sagepub.com/doi/abs/10.1177/0093650218800915> accessed 07.02.2023

7 Ibid.

8 Tobias Dienlin and Miriam J Metzger, 'An extended privacy calculus model for SNSs—Analyzing self-disclosure and self-withdrawal in a US representative sample' (2016) 21(5) Journal of Computer-Mediated Communication 368; Hanna Krasnova and others, 'Online social networks: Why we disclose' (2010) 25(2) Journal of Information Technology 109.

9 Nicole C Krämer and Nina Haferkamp, 'Online self-presentation: Balancing privacy concerns and impression construction on social networking sites' in Sabine Trepte and Leonard Reinecke (eds), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (Springer 2011).

10 Airi Lampinen and others, 'We're in it together: Interpersonal management of disclosure in social network services' (Vancouver, BC, Canada).

B Theoretical Perspectives on Individual Privacy Regulation

I A Communication Science Perspective on Privacy (Regulation)

Numerous disciplines are engaged in the discourse on privacy such as legal science, business informatics, sociology, and philosophy.[11] Since I specifically focus on a communicational and psychological perspective, the following section traces the history of privacy conceptualizations that are relevant to this particular line of research.

Westin's conceptualization of privacy is commonly seen as a starting point for research on privacy.[12] In his book called "Privacy and freedom" Westin defines privacy as an individual's claim "when, how, and to what extent information about them is communicated to others".[13] One important contribution of Westin's definition is characterizing privacy as the freedom of choice to withdraw from interactions. Thus, forms of forced isolation (eg, prison) cannot be referred to as privacy. Moreover, Westin links an individual's perceived level of privacy to well-being. According to Westin,[14] imbalanced levels of privacy lead to, for example, emotional pressure or neurotics. Contrasting, maintaining privacy is essential for personal autonomy, being able to seek emotional release from fulfilling social expectations, the integration of experiences in meaningful patterns, and being able to share intimacy with close peers in protected social spaces.

Shortly after Westin's had published "Privacy and freedom", another privacy theory was introduced by Johnson.[15] Johnson emphasized the behavioral components of privacy by describing privacy as an equivalent to control behavior.[16] Further, privacy is understood as a form of secondary control because individuals aim to "enhance and maintain one's control over outcomes indirectly by controlling in-

11 Philipp K Masur, *Situational privacy and self-disclosure: Communication processes in online environments* (Springer International Publishing 2019).

12 Stephen T Margulis, 'On the status and contribution of Westin's and Altman's theories of privacy' (2003) 59(2) Journal of Social Issues 411 <https://doi.org/10.1111/1540-4560.00071>.

13 Alan F Westin, *Privacy and freedom* (Atheneum 1970) 7.

14 Ibid.

15 Carl A Johnson, 'Privacy as personal control' in Stephen T Margulis (ed), *Man-environment interactions: Evaluations and applications* (Dowden, Hutchinson & Ross 1974).

16 Ibid.

teractions with others".[17] The term "secondary control behavior" describes behavior that increases the chances of primary control (ie, behavior that directly influences outcomes) to succeed. Interestingly, Johnson highlights that the selection between various behavioral strategies, might be perceived as a burden and therefore decrease an individual's perceived level of control. In absence of clear criteria for identifying superordinate strategies, the psychological costs are high.

Almost simultaneously to Johnson's conceptualization, Altman described privacy as "the selective control over access to the self or to one's group".[18] Until now, this definition remains one of the most influential.[19] Privacy regulation, according to Altman, is an "interpersonal boundary control process, designed to pace and regulate interactions with others".[20] Altman steps out of Westin's conceptualization by understanding privacy as an ongoing process instead of a subjective state. Defining privacy as a state implies that an individual either has privacy or has no privacy at all. The procedural perspective of Altman complements Johnson's stance on privacy as control behavior, which is described above. However, Altman concludes that not behavior itself defines privacy but the mere ability to exercise control and regulate access. Consequently, individuals can feel private even if they disclose information about themselves. Only if the achieved level of privacy equals the desired level of privacy, individuals perceive an optimal level of privacy. Imbalances between achieved and desired levels result in either too low or too high privacy levels, which are both perceived as unpleasant.[21]

The following years of privacy research resulted in several definitions and typologies of privacy that "tend[ed] to overlap without being exhaustive".[22] Burgoon suggested a typology of different privacy dimensions that closes this gap by highlighting the multidimensional nature of privacy. In particular, Burgoon describes four dimensions of privacy: physical, social, psychological, and informational privacy.[23] The physical dimension defines privacy in terms of being physically accessible or inaccessible to others. This is a rather intuitive view on privacy, as the dimension includes thoughts on territory, personal space, or visual and auditory seclusion that are also central to traditional privacy theorists like Westin or Altman. The social dimension refers to the ability to withdraw from or take part in

17 Ibid, 90.
18 Altman (n 3) 6.
19 Margulis (n 12).
20 Ibid, 3.
21 Altman (n 3).
22 Judee K Burgoon, 'Privacy and communication' (1982) 6(1) Annals of the International Communication Association 206, 210.
23 Ibid.

social interaction. Burgoon denotes that social privacy is closely related to norms that help to maintain meaningful social interactions while minimizing conflicts. For example, individuals seek a more intimate conversation with close peers while creating distance to an extended group of friends. Thirdly, Burgoon defines the psychological dimension of privacy as the ability to control cognitive in- and outputs. For example, an individual may not want to disclose her or his election decision and at the same time feels overwhelmed when others do so. Lastly, the informational dimension refers to the ability to determine which, how, when, and to what extent information is released. Interestingly, Burgoon mentions that this dimension goes beyond personal control because "information about a person, group, or organization can be gathered and disseminated without their knowledge".[24] This is of particular relevance for more recent topics like online privacy, as the collection of personal information and its dissemination is becoming increasingly difficult to trace.

Retrieved from this timeline of seminal conceptualizations of privacy (regulation), several key characteristics of privacy can be identified: (i) *Complexity:* First and overall, scholars agree that privacy is a complex, multi-dimensional concept involving a wide variety of variables that have to be considered.[25] (ii) *Universality:* Privacy is a universal concept. As Altman puts it: "mechanisms for separating the self and nonself and for regulating interpersonal boundaries to achieve a desired level of privacy are universal and present in all societies".[26] Although existing research denotes that privacy is shaped by culture,[27] privacy is a key issue in all cultures. (iii) *Dialectic:* One of the central characteristics of privacy – and also the main assumption in the privacy calculus[28] – is the balancing act between opposing forces. Both withdrawal (eg, personal autonomy, emotional release, intimacy, creativity) and self-disclosure (eg, meaningful social contacts, social support, appreciation) fulfill important psychological functions for individuals. "Either too much or too little privacy can create imbalances, which seriously jeopardize the individual's well-being".[29] This rationale also implies that there never is complete privacy but

24 Ibid 229.

25 Ibid; Altman (n 3).

26 Altman (n 3) 19.

27 Eg Sabine Trepte and others, 'A cross-cultural perspective on the privacy calculus' (2017) 3(1) Social Media + Society 1–13.

28 Tamara Dinev and Paul Hart, 'An extended privacy calculus model for e-commerce transactions' (2006) 17(1) Information Systems Research 61; Sabine Trepte, Michael Scharkow and Tobias Dienlin, 'The privacy calculus contextualized: The influence of affordances' (2020) 104 Computers in Human Behavior 106115.

29 Westin, (n 13) 40.

an optimal level of access an individual strives for.[30] (iv) *Dynamic:* The nature of privacy is commonly described as dynamic rather than static because its meaning shifts, for example, within an individual's life-cycle, between different situations, and even within ongoing events.[31] Consequently, privacy is characterized as a continuous adjustment and readjustment caused by changing contexts.[32] (v) *Procedural:* Therefore, scholars agree on the assumption that privacy is a process. It manifests in different stages of privacy regulation, it is structured in action-reaction chains, and it is oriented towards achieving an optimal level of privacy.[33]

II Theories Predicting Individual Privacy Regulation Behavior

Most studies from the disciplines of communication science and psychology, are based on one of the following five theories: Protection Motivation Theory, Theory of Planned Behavior, Privacy Calculus Theory, Communication Privacy Management Theory, or the Social Media Privacy Model. I will shortly introduce them in the next section.

Rogers developed the so-called *Protection Motivation Theory.*[34] Initially, it focused on describing the effectiveness of fear appeals in health contexts.[35] However, a growing body of research shows its applicability in contexts beyond such as online privacy.[36] The theory proposes two appraisal processes – threat and coping appraisal – that can result in attitude and behavior change[37]. Rogers explains that individuals continue to behave risky when they experience the behaviors as overall beneficial after threat and coping appraisal.[38] Protection Motivation Theory is

30 Altman (n 3); Burgoon (n 22); Westin (n 13).

31 Altman (n 3); Burgoon (n 22).

32 Altman (n 3).

33 Burgoon (n 22); Johnson (n 15).

34 Ronald W Rogers, 'A protection motivation theory of fear appeals and attitude change' (1975) 91(1) The Journal of Psychology 93.

35 Ibid; Steven Prentice-Dunn and Ronald W Rogers, 'Protection motivation theory and preventive health: Beyond the health belief model' (1986) 1(3) Health Education Research 153.

36 Eg Yannic Meier and others, 'Applying Protection Motivation Theory to Predict Facebook Users' Withdrawal and Disclosure Intentions' [2020] SMSociety'20: International Conference on Social Media and Society 21; Muliati Sedek, Rabiah Ahmad and Nur F Othman, 'Motivational factors in privacy protection behaviour model for social networking' (2018) 150 MATEC Web of Conferences 5014.

37 Prentice-Dunn and Rogers (n 35).

38 Ibid; Meier and others (n 36).

mostly used to research the effectiveness of privacy interventions[39] because it focuses on explaining stimulus appraisal. However, it cannot trace a continuous process of privacy regulation.

The *Privacy Calculus Theory* is based on similar assumptions as the Protection Motivation Theory but is specifically developed to explain privacy behavior. The Privacy Calculus represents the further development of the so-called Privacy Paradox.[40] Studies observed that individuals self-disclose personal information despite privacy concerns.[41] However, scholars highlight that concerns alone do not sufficiently predict online privacy behavior.[42] The Privacy Calculus proposes that individuals weigh benefits of self-disclosure, eg, relationship building, self-presentation, or enjoyment[43] against its risks, eg, data leakages. If benefits outweigh the risks, individuals will show self-disclosure despite their concerns for privacy.[44] The comprehensibility of the Privacy Calculus is a flexible theory suiting many research designs. However, it again may simplify the complexity of privacy regulation. It is questionable whether individuals rationally decide on how to manage privacy.

Another important theory in the context of online privacy regulation behavior is the *Theory of Planned Behavior* initially developed by Ajzen.[45] The theory includes three predictors of behavioral intentions: the attitude towards the behavior, subjective norm, and perceived behavioral control. All three variables already have been shown to predict online privacy regulation behavior.[46] However, the Theory of

39 Meier and others (n 36).

40 Krasnova and others (n 8).

41 Susan B Barnes, 'A privacy paradox: Social networking in the United States' (2006) 11(9) First Monday; Monica Taddicken, 'The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure' (2014) 19(2) Journal of Computer-Mediated Communication 248.

42 Tobias Dienlin and Sabine Trepte, 'Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors' (2015) 45(3) European Journal of Social Psychology 285.

43 Christy Cheung, Zach W Y Lee, and Tommy K H Chan, 'Self-disclosure in social networking sites' (2015) 25(2) Internet Research 279.

44 Dienlin and Metzger (n 8); Dinev and Hart (n 28).

45 Icek Ajzen, 'The theory of planned behavior' (1991) 50(2) Organizational Behavior and Human Decision Processes 179.

46 Eg C. Bryan Foltz, Henry E Newkirk and Paul H Schwager, 'An empirical investigation of factors that influence individual behavior toward changing social networking security settings' (2016) 11(2) Journal of theoretical and applied electronic commerce research 2; A K M Nuhil Mehdy and others, 'Privacy as a planned behavior: Effects of situational factors on privacy perceptions and plans' (Proceedings of the 29th ACM Conference on User Modeling, Adaption and Personalization (UMAP'21), ACM, Utrecht, Netherlands, 21 June 2021–25 June 2021) <http://arxiv.org/pdf/2104.

Planned Behavior is hard to apply in some research contexts. Studies either need to focus on one specific behavioral tactic or on regulation behavior in general.

For the last decade, privacy research has increasingly described privacy regulation as a cooperative behavior.[47] The *Communication Privacy Management Theory* developed by Petronio[48] has been one of the first theories accounting for this social nature of privacy. Petronio describes individuals as autonomous, as well as social actors. The regulation of privacy thus is a dialectical issue. These considerations have already been mentioned in Altman's conceptualization of privacy.[49]Additionally, Communication Privacy Management Theory acknowledges that the process of privacy regulation includes, for example, the creation of shared boundaries, the coordination of these boundaries, and coping with consequences of privacy turbulences.[50] The theory has already been applied in the contexts of family, health communication, but also social media.[51] Although Communication Privacy Management Theory includes privacy mechanisms and behaviors, ie, creating boundaries, coordinating boundaries, and turbulence coping, Petronio does not explain how these behaviors manifest. Consequently, operationalizations of CMP considerably differ from one another, resulting in a lack of comparability of results.[52]

11847v1>; Alexander K Saeri and others, 'Predicting facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior' (2014) 154(4) The Journal of Social Psychology 352; Mike Z Yao and Daniel G Linz, 'Predicting self-protections of online privacy' (2008) 11(5) CyberPsychology & Behavior 615.

47 Eg Hichang Cho and Anna Filippova, 'Networked privacy management in Facebook' (CSCW '16: Computer Supported Cooperative Work and Social Computing, San Francisco California USA, 27.02. 2016–02. 03. 2016); Lampinen and others (n 10); Alice E Marwick and Danah Boyd, 'Networked privacy: How teenagers negotiate context in social media' (2014) 16(7) New Media & Society 1051.

48 See Sandra Petronio, *Boundaries of privacy* (State University of New York Press 2002); Sandra Petronio, 'Road to developing communication privacy management theory: Narrative in progress, please stand by' (2004) 4(3–4) Journal of Family Communication 193; Sandra Petronio, 'Communication privacy management theory' in Charles R Berger and Michael E Roloff (eds), *The international encyclopedia of interpersonal communication* (ICA international encyclopedias of communication. Wiley Blackwell 2016).

49 Altman (n 3).

50 Sandra Petronio and Wesley T Durham, 'Communication privacy management theory.' in Leslie A Baxter and Dawn O Braithwaite (eds), *Engaging Theories in Interpersonal Communication: Multiple Perspectives* (Sage 2008).

51 Sandra Petronio, 'Brief status report on communication privacy management theory' (2013) 13(1) Journal of Family Communication 6.

52 Eg Cho and Filippova (n 47); Haiyan Jia and Heng Xu, 'Measuring individuals' concerns over collective privacy on social networking sites' (2016) 10(1) CP; Miriam J Metzger, 'Communication privacy management in electronic commerce' (2007) 12 Journal of Computer-Mediated Communication 335.

One of the latest theories on online privacy is the *Social Media Privacy Model* suggested by Trepte.[53] It proposes a complex process of privacy management that accounts for the special characteristics of social media and the social nature of privacy. Trepte defines social media privacy regulation as

> an individual's assessments of (a) the level of access to this person in an interaction or relationship with others (people, companies, institutions) and (b) the availability of the mechanisms of control, interpersonal communication, trust, and norms for shaping this level of access through (c) self-disclosure as (almost intuitive) behavioral privacy regulation and (d) control, interpersonal communication, and deliberation as means for ensuring (a somewhat more elaborated) regulation of privacy. In social media, then, the availability of the mechanisms that can be applied to ensure privacy are crucially influenced by the content that is being shared and the social media affordances that determine how this content is further used.[54]

The following section explains the various dimensions of the Social Media Privacy Model in detail. Furthermore, I will present selected empirical findings on predictors and determinants of individual privacy regulation behavior on social media.

C Determinants of Individual Privacy Regulation – The Example of Social Media

The first stage of the Social Media Privacy Model is the so-called *initial assessment*. It describes that users have different demands for privacy according to individual characteristics. First, this stage includes an individual's ideal – or adequate – *level of access*. Individuals are expected to differ regarding their general need for privacy. People with a high need for privacy also disclose less and protect their data more.[55] Moreover, studies show that cultures come with different privacy expectations, laws, and habits influencing an individual's privacy behavior[56] and that females disclose less information than males as they generally have more concerns

53 Sabine Trepte, 'The Social Media Privacy Model: Privacy and communication in the light of social media affordances' (2021) 31(4) Communication Theory 549.
54 Ibid 561.
55 Regina Frener, Jana Wagner and Sabine Trepte, 'Development and Validation of the Need for Privacy Scale (NFP-S)' forthcoming.
56 Zilong Liu and Xuequn Wang, 'How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison' (2018) 55(8) Information & Management 1005; Trepte and others (n 27).

regarding their privacy.[57] Second, the Social Media Privacy Model proposes that individuals use social media to fulfil different *communication goals.* These goals are accompanied by a certain demands for privacy. A study conducted by Cheung, Lee and Chan[58] shows that individuals tend to disclose more when they use social media to maintain existing or build new relationships. Further, self-representation and entertainment goals are associated with more self-disclosure.[59]

The second dimension of the Social Media Privacy Model is called *boundary conditions.* Individual privacy regulation differs according to the specific *social media content*, the *flow of content* ie, where and how the information is forwarded, archived, or sold, and the social media *affordances.* Individuals perceive, eg, fears or financial information as very private, whereas information on, eg, favorite books or geo-location data is categorized as less private.[60] Consequently, privacy threats directed at more sensitive information are also very likely to be considered more severe and important. Trepte points to four affordances that are especially relevant in the context of social media privacy management: *anonymity* ie, not being able to identify a messenger, *association* ie, the interconnectedness between social media users, *editability* ie, the ability to select, package, change, and craft a message, and *persistence* ie, the durability of disclosed content.[61] Snapchat is, for example, ranked lower in persistence than instant messengers (eg, WhatsApp) or other social networks (eg, Facebook, Instagram) because posts can only be viewed once by their recipients. Contrasting, Facebook is ranked higher in association than instant messenger services or Snapchat because it is used for network building[62]. Further, affordances have been shown to influence depth, breadth, and sensitivity of disclosures. For example, higher anonymity and stronger associations lead to more in-depth disclosure.[63]

---

57 Sigal Tifferet, 'Gender differences in privacy tendencies on social network sites: A meta-analysis' (2019) 93 Computers in Human Behavior 1.

58 Cheung, Lee, and Chan (n 43).

59 Ibid.

60 Stanislav Mamonov and Raquel Benbunan-Fich, 'An empirical investigation of privacy breach perceptions among smartphone application users' (2015) 49 Computers in Human Behavior 427; Philipp K Masur and Michael Scharkow, 'Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies' (2016) 2(1) Social Media + Society.

61 Trepte (n 53).

62 Jesse Fox and Bree McEwan, 'Distinguishing technologies for social interaction: The perceived social affordances of communication channels scale' (2017) 84(3) Communication Monographs 298.

63 Renwen Zhang, Natalya Bazarova and Madhu Reddy, 'Distress Disclosure across Social Media Platforms during the COVID-19 Pandemic: Untangling the Effects of Platforms, Affordances, and Audiences' (2021) <http://dx.doi.org/10.1145/3411764.3445134>.

According to the Social Media Privacy Model the interaction between the initial assessment and the boundary conditions determines the *availability of privacy mechanisms.* Trepte refers to the mechanisms of *control*, *norms*, *trust*, and – largely new to the landscape of privacy research – *interpersonal communication.*[64] Control is one of the most frequently researched concepts because it is closely related to seminal definitions of privacy. Altman, Johnson, as well as Westin, and Burgoon defined privacy by using the term control, ie, the ability to determine which, how, and to whom personal information is released.[65] Social media users perceiving high levels of control are less concerned regarding their online privacy.[66] Moreover, users perceiving control tend to self-disclose more[67] and tend to protect their privacy less[68]. Next, the Social Media Privacy Model includes norms as a mechanism, ie, relying on sanctionable legislative or social rules.[69] These rules are known to guide regulation behavior.[70] Several studies demonstrate that users' self-disclosure or privacy protection behavior is strongly influenced by the behavior of other social actors.[71] Trust is described as an individual's expectation about the extent to which others will actually adhere to existing norms.[72] Research reveals that the mechanism of trust mitigates existing privacy concerns.[73] When trust in institutions, organizations, platforms, and peers is high, individuals stop protecting their privacy.[74] Further, experiencing privacy violations significantly decreases

64 Trepte (n 53).

65 Altman (n 3); Johnson (n 15); Westin (n 13); Burgoon (n 22).

66 Cheung, Lee and Chan (n 43); Nick Hajli and Xiaolin Lin, 'Exploring the security of information sharing on social networking sites: The role of perceived control of information' (2016) 133(1) Journal of Business Ethics 111; Lili N Zlatolas and others, 'Privacy antecedents for SNS self-disclosure: The case of Facebook' (2015) 45 Computers in Human Behavior 158.

67 Cheung, Lee and Chan (n 43); Liu and Wang (n 56); Jill Mosteller and Amit Poddar, 'To share and protect: Using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors' (2017) 39 Journal of Interactive Marketing 27; Zlatolas and others (n 66).

68 Mosteller and Poddar (n 67).

69 Trepte (n 53).

70 Sandra Petronio, 'Communication privacy management theory' in Charles R Berger and Michael E Roloff (eds), *The international encyclopedia of interpersonal communication* (ICA international encyclopedias of communication. Wiley Blackwell 2016).

71 Cheung, Lee and Chan (n 43); Liu and Wang (n 56); Lili Zlatolas and others (n 66).

72 Ari E Waldman, *Privacy as trust* (Cambridge University Press 2018).

73 Cheung, Lee and Chan (n 43); Mosteller and Poddar (n 67).

74 Nancy K Lankton, D Harrison McKnight and Jason B Thatcher, 'The moderating effects of privacy restrictiveness and experience on trusting beliefs and habit: An empirical test of intention to continue Using a Social Networking Website' (2012) 59(4) IEEE Transactions on Engineering Management 654; Liu and Wang (n 56); Mosteller and Poddar (n 67); Saeri and others (n 46).

the trust in entities that caused the violation.[75] Although interpersonal communication has been mentioned in privacy theorizing before, the Social Media Privacy Model is the first theory that explicitly conceptualizes communication as a separate mechanism and behavioral tactic. Although qualitative studies highlight that individuals use a variety of communication-based mechanisms and tactics to protect their privacy (eg, rule negotiation, relationship management, message encoding), research on interpersonal communication is scarce.[76]

This result also affects the next stages of the Social Media Privacy Model: *subjective experience of privacy* and *privacy behavior.* First, the subjective experience of privacy includes a collection of unsorted stimuli resulting from all of the stages mentioned before ie, the *experienced level of access.* These unsorted stimuli shape an individual's *privacy perception* that results from elaboration. Individuals weigh desired against perceived levels of privacy and benefits of using social media against its risks. An unbalanced level of privacy then motivates an individual's privacy regulation behavior. According to the Social Media Privacy Model, this can result in either of the two following behaviors: *ego-centric regulation* (ie, control, self-disclosure) and *interdependent regulation* (ie, deliberation, interpersonal communication). The concept of ego-centric regulation behavior includes tactics an individual can use independent of other actors. Control behaviors include technological measures helping to reclaim privacy, for example, users can change their password or can use browser plug-ins to protect their privacy. The second type of ego-centric regulation behavior is self-disclosure ie, conscious decisions on which information is released or not released. In its most extreme form, restricting self-disclosure can mean that individuals stop using social media applications. In contrast, the concept of interdependent regulation includes social-centered tactics exerted through interpersonal communication.[77] For example, individuals complain or exchange experiences through interpersonal communication helping them to deal with issues regarding privacy.[78] Deliberation behavior is more formal and involves rational-critical decision-making. Individuals, for example, aim to

75 Bryan Hammer and others, 'Psychological contract violation and sharing intention on Facebook' (Hawaii International Conference on System Sciences 2019, Hawaii, 2019) <http://hdl.handle.net/10125/59715>.

76 Eszter Hargittai and Alice E Marwick, '"What can I really do?" Explaining the privacy paradox with online apathy' (2016) 10 International Journal of Communication 3737; Marwick and Boyd (n 47).

77 Trepte (n 53).

78 Hichang Cho, Pengxiang Li and Zhang H Goh, 'Privacy risks, emotions, and social media: A coping model of online privacy' (2020) 27(6) ACM Trans Comput-Hum Interact 1.

find solutions and negotiate rules.[79] Interdependent regulation tactics can, according to Trepte,[80] crystallize in trust or norms because communication can help individuals build trust and develop liable social norms. Scholars have demonstrated that perceived risks or threats do not necessarily result in privacy behavior.[81] Individuals disclose less and protect more only if severe privacy threats occur.[82] Individuals change their informational privacy behavior when their privacy has been violated. However, they do not change their social or psychological privacy behavior.[83] Privacy issues that provoke negative affects (eg, fear, anger) lead to the use of distributive tactics (eg, yelling, criticizing, or venting), as individuals try to restore social damage.[84]

D Learnings from Research on Individual Privacy Regulation

This review on empirical and theoretical contributions highlights three important points that contribute to the understanding of individual privacy management. First, *it is not high privacy that matters, it is optimal privacy that matters.* The societal and academic dialogue on privacy is focused on privacy threats and thus low levels of privacy. Withdrawal and access restriction are discussed as the main tactics to prevent and tackle online threats. However, self-disclosure comes with risks as well as benefits. Using social media, for example, helps individuals to engage in self-presentation or relationship management and thus has the potential to improve an individual's overall well-being.[85] This highlights two points regarding individual privacy regulation: First, we know from Privacy Calculus Theory that benefits can outweigh the risks of self-disclosure. Since social media is a vital part in

79 Stephanie Burkhalter, John Gastil and Todd Kelshaw, 'A conceptual definition and theoretical model of public deliberation in small face-to-face groups' (2002) 12(4) Communication Theory 398.
80 Trepte (n 53).
81 Cheung, Lee and Chan (n 43); Liu and Wang (n 56); Saeri and others (n 46).
82 Hsin H Chang, Kit H Wong and Ho C Lee, 'Peer privacy protection motivation and action on social networking sites: Privacy self-efficacy and information security as moderators' (2022) 54 Electronic Commerce Research and Applications 101176.
83 Philipp K Masur and Sabine Trepte, 'Transformative or not? How privacy violation experiences influence online privacy concerns and online information disclosure' (2021) 47(1) Human Communication Research 49.
84 Lindsey S Aloia, 'The emotional, behavioral, and cognitive experience of boundary turbulence' (2018) 69(2) Communication Studies 180; Cho, Li and Goh (n 78).
85 Arnold Buss, *Psychological dimensions of the self* (Sage 2001); Margulis (n 12); Westin (n 13).

the lives of most individuals, they will continue to self-disclose despite their concerns. Second, individuals will only engage in regulation behavior if the actual level of privacy differs from the desired level of privacy. Both too low and too high levels of privacy lead to turbulences that threaten the psychological balance of individuals. Instead of limiting online experiences through, eg, over-regulation, public discourse should focus on ways to limit potential threats of social media without diminishing its positive effects. It is important to create a conducive environment for privacy (eg, through norms, trust, or communication) and empower individual behavior that goes far beyond access restriction and withdrawal.

This leads to my second point: *Privacy (regulation) is a social matter.* The so-called privacy as control paradigm[86] has been dominating the social sciences for a long time[87]. Altman, Johnson, as well as Westin and Burgoon defined privacy along the term control.[88] On the one hand, this perspective implies that individuals can disclose every personal detail and would still consider their situation private as long as they perceive being in control about whether to disclose or not.[89] On the other hand, this paradigm excludes that there can be private situations in which individuals have no control at all.[90] Consequently, control should be understood as one privacy mechanism among others. Privacy theorizing increasingly acknowledges the social nature of privacy.[91] Especially in online environments like social media users are co-manager of information and privacy regulation which also includes managing shared boundaries.[92] Users already take their opportunities to engage in collective privacy management, for example, through sanctioning violations of norms on social media.[93] Consequently, interpersonal communication and – in its crystallized form – social norms and trust need to be recognized as equally important mechanisms and tools for individual privacy regulation.

---

86 Robert S Laufer and Maxine Wolfe, 'Privacy as a concept and a social issue: A multidimensional developmental theory' (1977) 33(3) Journal of Social Issues 22; Herman T Tavani, 'Philosophical theories of privacy: Implications for an adequate online privacy policy' (2007) 38(1) Metaphilosophy 1; Trepte (n 53).

87 H Jeff Smith, Tamara Dinev and Heng Xu, 'Information privacy research: An interdisciplinary review' (2011) 35(4) Mis Quarterly 989.

88 Altman (n 3); Johnson (n 15); Westin (n 13); Burgoon (n 22).

89 Tavani (n 86).

90 Herman T Tavani and James H Moor, 'Privacy protection, control of information, and privacy-enhancing technologies' (2001) 31(1) SIGCAS Comput Soc 6.

91 Petronio, Boundaries of privacy (n 48); Trepte (n 53).

92 Petronio, 'Road to developing communication privacy management theory: Narrative in progress, please stand by' (n 48).

93 Yasmeen Rashidi and others, '"It's easier than causing confrontation": Sanctioning strategies to maintain social norms and privacy on social media' (2020) 4(1) Proc ACM Hum-Comput Interact 1.

A last important point is the role of context-dependency. *Privacy regulation needs to be contextualized, not generalized.* As we continually learn from theorists and empirical studies, individual regulation of privacy evolves entirely different when the context changes.[94] The process of privacy regulation includes a variety of variables, mechanisms, and effects that influence the way privacy is experienced and managed.[95] This leads to the conclusion that we need to understand the context first before we can understand or empower individual privacy regulation. Creating the right conditions on different applications, for different users, and different contexts is thus an ongoing task for scholars and practitioners.

94 Helen Nissenbaum, 'A contextual approach to privacy online' (2011) 140(4) Daedalus 32.
95 Trepte (n 53).

Lemi Baruh

One Calculus to Rule it All? The Need for New Analytical Tools and Comparative Approaches to Fine-tune the Privacy Calculus

The notion of the privacy paradox, which typically refers to a discrepancy between professed privacy concerns or attitudes and intents or actions, has been a significant topic of discussion in the literature on privacy self-management (eg, disclose personal information, engage in online commerce, adopt privacy protecting measures).[1] The concept of privacy paradox stands in contrast to the premises of the Privacy Calculus Model,[2] according to which the decision to disclose information,

Lemi Baruh is an Associate Professor at Koç University, Department of Media and Visual Arts, Istanbul, lbaruh@ku.edu.tr.

Acknowledgement: The author would like to thank the whole Vectors of Data Disclosure project team for organizing the conference and inviting him to the conference. Special thanks to Prof. Dr. Daniela Wawra and Peer Sonnenberg for their assistance while preparing for the conference and their patience while waiting for this conference contribution.

1 Ruwan Bandara, Mario Fernando and Shahriar Akter, 'Explicating the privacy paradox: A qualitative inquiry of online shopping consumers' (2020) 52 Journal of Retailing and Consumer Services 101947; Susan B Barnes, 'A Privacy paradox: Social networking in the United States' (2006) 11(9) First Monday 11; Lemi Baruh, Ekin Secinti and Zeynep Cemalcilar, 'Online Privacy Concerns and Privacy Management: A Meta-Analytical Review' (2017) 67(1) Journal of Communication 26; Tobias Dienlin and Sabine Trepte, 'Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviours: The relation between privacy attitudes and privacy behaviours' (2015) 45(3) European Journal of Social Psychology 285.

2 Mary J Culnan and Pamela K Armstrong, 'Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation' (1999) 10(1) Organization Science 104.

https://doi.org/10.1515/9783111010601-007

as well as related decisions related to privacy regulation / management behavior, is a function of two sets of considerations: our expectations about benefits from sharing and the risks we associate with sharing information (Fig. 1).

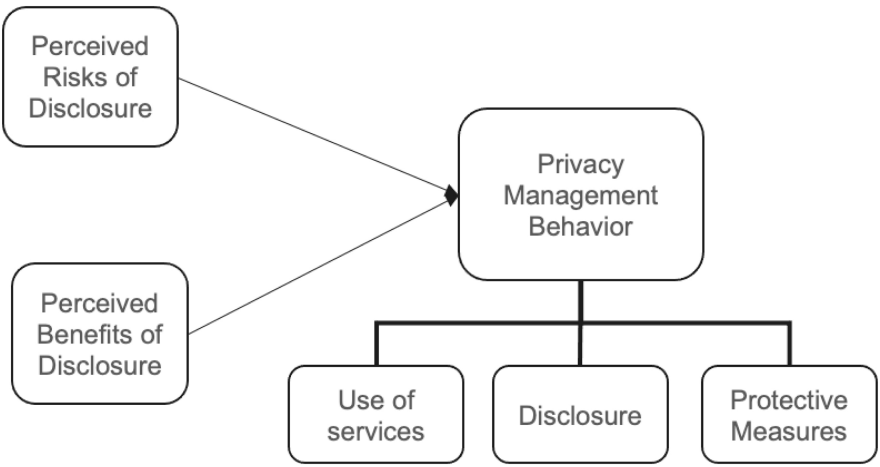

Fig. 1: The Privacy Calculus Model.

While empirical studies provide evidence against the privacy paradox in that we consistently observe a weak but significant relationship between privacy concerns and disclosure behavior,[3] there are some key reasons why the relationship is weak at best.

First, privacy calculus is based on a rational decision-making model where individuals are assumed to carefully evaluate the risks and benefits before engaging in self-disclosure.[4] However, research suggests there are several reasons why individuals often cannot engage in a rational deliberation of risks and benefits. These reasons include lack of available information about risks and benefits, low motivation to engage in the deliberation of respective risks and benefits, reliance on emotions, and cognitive biases that result in discounting of long-term risks.[5] It is

3 Baruh, Secinti and Cemalcilar (n 1).

4 Maxine Wolfe and Richard S Laufer, 'The concept of privacy in childhood and adolescence' in Daniel H Carson (ed), *Man-environment interactions* (Environmental Design Research Association 1974).

5 Alessandro Acquisti and others (2017) 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' 50(3) ACM Computing Surveys 1; Susanne Barth and Menno D T de Jong, 'The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behaviour – A systematic literature review' (2017) 34(7) Telematics and Informat-

also worth noting that, particularly in the context of social media use, expected (and concrete) benefits like social validation and connectivity may override considerations of long-term (and relatively more abstract) risks.[6]

Second, increasingly more research underscores how the decision to engage in privacy-related behavior is influenced by contextual (eg, affordances of a platform)[7] and situational[8] factors that may influence not only our risk and benefit perceptions but also the respective weight we assign to them. For example, Barth and De Jong (2017)[9] assert that users end up acting online in a way that contradicts their privacy attitudes because there are circumstances in which users do not weigh the risks associated with their privacy concerns in favor of the expected advantages. For instance, this would be the case when the need for a given service (eg, using credit cards) is so high that privacy risks will not be considered. In such a context, we may fail to find a statistically significant relationship between privacy concerns and disclosure because the behavior occurs despite concerns. Conversely, there may be contexts where the expected benefits are so low that disclosure does not happen even when the risk perceptions are low.

The recent emphasis on situational and contextual factors indicates the need for a more nuanced approach to studying how individuals engage in privacy calculus. Namely, it underscores the possibility that we are not talking about a single privacy calculus because contexts or situations will affect risk and benefit considerations' respective (and often conjoint) influence. In this light, the aim of this conribution is two-fold. First, following the footsteps of a recent article that we authored,[10] I will outline how a novel analytical technique called Response Surface Analysis (RSA)[11] can be used to account for conjoint effects of risk and benefit con-

---

ics 1038; Aaron Brough and Kelly D Martin, 'Critical roles of knowledge and motivation in privacy research' (2020) 31 Current Opinion in Psychology 11; Philipp K Masur, *Situational Privacy and Self-Disclosure* (Springer International Publishing 2019); Renwen Zhang and Sophia Fu, 'Privacy Management and Self-Disclosure on Social Network Sites: The Moderating Effects of Stress and Gender' (2020) 25(3) Journal of Computer-Mediated Communication zmaa004.

6 Bernhard Debatin and others, 'Facebook and Online Privacy: Attitudes, Behaviours, and Unintended Consequences' (2009) 15(1) Journal of Computer-Mediated Communication 83.

7 Sabine Trepte, Michael Scharkow and Tobias Dienlin, 'The privacy calculus contextualized: The influence of affordances' (2020) 104 Computers in Human Behaviour 106115.

8 Masur (n 5).

9 Barth and De Jong (n 5).

10 Murat Kezer, Tobias Dienlin and Lemi Baruh, 'Getting the Privacy Calculus Right: Analyzing the Relations between Privacy Concerns, Expected Benefits, and Self-disclosure Using Response Surface Analysis' (2022) 16(4) Cyberpsychology: Journal of Psychosocial Research on Cyberspace 1.

11 Jeffrey R Edwards, 'Alternatives to difference scores: Polynomial regression analysis and response surface methodology' in Fritz Drasgow and Neil Schmitt (eds), *Measuring and analyzing be-*

siderations. Using secondary analysis of a dataset, I will show how RSA can be conducted and interpreted. What is important to note about this dataset is that if we were to use conventional linear methods (eg, linear regression), we would have failed to find a statistically significant relationship between privacy concerns and disclosure (a conclusion that would be in line with the premise of the privacy paradox). Yet, the RSA will help us reveal important insights that indicate that risk perceptions were not inconsequential. Second, I will summarize the ongoing works of a new network called the *Comparative Privacy Research Network*[12] (CPRN). After introducing the members of the network, I will briefly outline the conceptual approach of CPRN[13] and how this approach may help more systematically study contextual and situational factors that may influence privacy-related behavior.

A Studying Privacy Calculus Using Response Surface Analysis

A closer look at current findings supporting the privacy paradox paradigm points to two problems regarding how the relationship between concerns and disclosure behavior is modelled. First, many studies reporting the privacy paradox focus only on the concern / risk dimension without taking into account perceived benefits.[14] This will not be the focus of this section. Second, when studies investigate both risks and benefits, they often employ analytical approaches, like regression or structural equation modelling, that model the isolated linear influence of benefit and risk perceptions on privacy behavior after controlling for each other.[15]

Such models would allow us to test the linear effects of each variable on self-disclosure. Additionally, we can reach conclusions about the respective magnitude

haviour in organizations: Advances in measurement and data analysis (The Jossey-Bass business & management series 2002).

12 <https://comparativeprivacy.org/> accessed 07.02.2023.

13 Philipp K Masur and others, *A Comparative Privacy Research Framework* (Reprint, SocArXiv 2021).

14 Eg Joshua Fogel and Elham Nehmad, 'Internet social network communities: Risk taking, trust, and privacy concerns' (2009) 25(1) Computers in Human Behaviour 153; Wonsun Shin and Hyunjin Kang, 'Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet' (2016) 54 Computers in Human Behaviour 114.

15 Eg Sabine Trepte and others 'A Cross-Cultural Perspective on the Privacy Calculus' (2017) 3(1) Social Media + Society; Hanna Krasnova, Natasha F Veltri and Oliver Günther, 'Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus' (2012) 4(3) Business & Information Systems Engineering 127.

of risk and benefit perceptions. However, a significant drawback of such conventional methods is that they do not honor the privacy calculus model's assumption, which states that disclosure will occur when the perceived advantages of doing so outweigh its dangers. This means that we may disclose information even when risk perceptions are very high if the benefits are higher. Similarly, above, I discussed how risk concerns could be disregarded when people think the advantage of sharing information is too great or when there is no way to think of an alternative to sharing information since one cannot live without a convenience like a smartphone. Barth and De Jong[16] describe such situations as "value of desired goal outweighs risk assessment". Or conversely, individuals may not even think about risks if the benefits are so low that it is not even worth considering the risks.

In short, to achieve a more nuanced understanding of the privacy calculus model, we need an analytical approach that allows us to model how two predictors (benefit and risk perceptions) of calculus are related to disclosure (or other privacy-related behavior) when one exceeds the other (eg, benefits > risks; risks > benefits) and at what levels (eg, both risk and benefit considerations are high, both risk and benefit considerations are low, perceived risk is high but perceived benefits is low, perceived benefits are high but perceived risk is low). RSA is a fine-grained approach that can address these considerations.

I What is Response Surface Analysis?

In Kezer and others,[17] we provide a summary of how RSA can be conducted for studying privacy calculus.[18] Edwards and Parry[19] also provide a handy tutorial. In this section, I will briefly summarize how RSA is conducted and how the output is interpreted for perceived benefits and perceived risks as predictors of disclosure.

RSA starts with a polynomial regression containing two independent variables, their quadratic transformations to test the nonlinear effects, and the interaction

16 Barth and De Jong (n 5) 1048.

17 Kezer, Dienlin and Baruh (n 10).

18 Also, please see Edwards (n 11) and Jeffrey R Edwards and Mark E Parry, 'On the use of polynomial regression equations as an alternative to difference scores in organizational research' (1993) 36(6) Academy of Management Journal 1577 for a detailed description of the methodology and why RSA should be preferred over approaches where difference scores between two independent variables are computed to predict a dependent variable.

19 Ibid.

between the independent variables. For the privacy calculus model, the polynomial regression would be as follows:

$$\text{Disclosure}_i = b_0 + b_1\text{Benefits}_i + b_2\text{Risks}_i + b_3\text{Benefits}_i^2 + b_4\text{Benefits}_i{*}\text{Risks}_i + b_5\text{Risks}_i^2$$

Next, the polynomial regression coefficients are used to construct a three-dimensional plot of the relationship between disclosure and the independent variables (benefit perceptions and risk perceptions). RSA also computes the surface values of the three-dimensional plot. Table 1 summarizes how RSA coefficients are calculated and what they imply for privacy calculus.

The RSA coefficients summarized in Table 1 can be used to infer the conjoint effects of benefit and risk perceptions. First, coefficients a_1 ($b_1 + b_2$) and a_2 ($b_3 + b_4 +$ b a_2) represent what is called the *line of congruence* (see the blue line in Figure 2, next section), the line where both benefit and risk perceptions have the same values. When a_1 is significant and positive, disclosure is higher when both benefit and risk perceptions are higher. When a_1 is significant and negative, this would mean disclosure is higher when both benefit and risk perceptions are on lower levels. Coefficient a_2 concerns whether the relationship observed in a_1 is linear or curvilinear. That is, a significant a_2 should be interpreted as meaning that the line of congruence is not linear but instead produces a parabolic shape.

Coefficients a_3 ($b_1 - b_2$) and a_4 ($b_3 - b_4 + b_5$) represent the *line of incongruence* (LOIC; red line in Figure 2, next section), which pertains to situations when perceived benefits and perceived risks have opposite values (ie, Perceived Benefits = -Perceived Risks). A significant and positive a_3 would indicate that disclosure increases when perceived benefits are higher than perceived risks. A negative a_3 would suggest that disclosure is higher when perceived risks exceed perceived benefits. Coefficient a_4 is about whether the LOIC is linear or curvilinear. That is, a significant a_4 should be interpreted as meaning that the line of incongruence is not linear but instead produces a parabolic shape.

Tab. 1: Meaning of polynomial regression and RSA coefficients

Coefficient	Calculation	Meaning
Polynomial Regression		
b_1		Linear effect of predictor perceived benefits.
b_2		Linear effect of predictor perceived risks.
b_3		Curvilinear effect of perceived benefits.

Tab. 1: Meaning of polynomial regression and RSA coefficients *(Continued)*

Coefficient	Calculation	Meaning
b_4		Interaction between perceived benefits and perceived risks.
b_5		Curvilinear effect of perceived risks.
Response Surface		
a_1	$b_1 + b_2$	Higher disclosure when both risk and benefit are at higher ($+a_1$) or lower ($-a_1$) levels
a_2	$b_3 + b_4 + b_5$	Line of congruence is curvilinear
a_3	$b_1 - b_2$	Disclosure is higher when benefits are higher ($+a_3$) or lower ($-a_3$) than risks.
a_4	$b_3 - b_4 + b_5$	Line of incongruence is curvilinear

II Illustration of Response Surface Analysis for Privacy Calculus

1 Procedure & Participants

The data for this example comes from a cross-sectional survey about Facebook use and privacy attitudes. The sample comprised a convenience sample of adult online panel members provided by Qualtrics Panel. Out of the 384 respondents who completed the survey, 341 completed all the questions related to Facebook uses and gratifications, disclosure on Facebook, and privacy concerns (general). The mean age of the respondents was 44.6 (*SD* = 14.5); 49 % of the respondents were female; majority of the respondents either had a college degree (32.4 %) or had some college education (30.2 %), followed by high school degree (20.1 %), master's degree (6.9 %), and technical school degree (5.8 %).

2 Measures

Perceived benefits of using Facebook were captured with *uses and gratifications*[20] of Facebook. The survey asked respondents to rate, using a five-point scale (1 =

20 Lemi Baruh, 'Mediated Voyeurism and the Guilty Pleasure of Consuming Reality Television'

strongly disagree to 5 = strongly agree), their agreement with statements describing why they use Facebook (eg, "to keep in contact with family and friends", "to meet new people", "because it helps me understand what people are really like"). The reliability of the items was high (ω = .91). The resulting scale had a mean score of 2.98 (*SD* = 0.79).

Perceived risks of sharing personal information were operationalized as *concerns about privacy*, measured with four items which asked respondents to rate, using a five-point scale (1 = strongly disagree to 5 = strongly agree), their agreement with statements about privacy concerns (eg, "I am concerned that people around me know too much about me"). The reliability of the items was good (ω = .84). The resulting scale had a mean score of 3.31 (*SD* = 0.90).

The dependent variable, sharing personal information on Facebook, was measured using eight items adapted for Facebook from the *self-disclosure index*.[21] Each item asked the respondents to indicate, using a six-point scale (never = 1 to more than once a day = 6), the frequency with which they shared different information on Facebook (eg, religious beliefs, work, political views, feelings). The reliability of the items was high (ω = .95). The resulting scale had a mean score of 2.02 (*SD* = 1.13).

3 Results

The RSA analysis was conducted in R (R Core Team, 2020)[22] using the package RSA.[23] RSA requires that there is a sufficient number of cases for each possible combination of the value of the two independent variables (ie, there should be a sufficient number of cases where perceived risks are higher than perceived benefits, perceived benefits are higher than perceived risks, and perceived benefits and perceived risks are approximately equal to each other). For this dataset, this requirement was satisfied: for 33 % of the cases, privacy concerns were lower than Facebook uses and gratifications, and for 29 % of the cases, privacy concerns

(2010) 13(3) Media Psychology 201; Gina M Chen, 'Tweet this: A uses and gratifications perspective on how active Twitter use gratifies a need to connect with others' (2011) 27(2) Computers in Human Behaviour, 755; Nicole B Ellison, Charles Steinfield and Cliff Lampe, 'The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites' (2007) 12(4) Journal of Computer-Mediated Communication 1134.

21 Lynn C Miller, John H Berg and Richard L Archer, 'Openers: Individuals who elicit intimate self-disclosure' (1983) 44(6) Journal of Personality and Social Psychology 1234.

22 R Core Team, 'R: A language and environment for statistical computing' (2020) <https://www.R-project.org/> accessed 07.02.2023.

23 Felix D Schönbrodt, 'RSA: An R package for response surface analysis' (version 0.9.11, 2017) <https://cran.r-project.org/package=RSA> accessed 07.02.2023.

were higher than Facebook uses and gratifications. Table 2 presents the polynomial regression coefficients and surface parameters.

In the polynomial regressions, uses and gratifications of Facebook (perceived benefits) were positively related to sharing personal information on Facebook (b_1 = .85, p <.001). This relationship was a curvilinear relationship (b_3 = .32, p <.001). More importantly, for our purposes, privacy concerns (risks) were not a significant predictor of sharing personal information on Facebook. Hence, if we were to solely rely on a regression, our conclusion would be in line with the notion of a privacy paradox: privacy risk perceptions are not related to disclosure behavior. However, RSA results qualify this finding. First, the a_1 parameter, which is about the line of congruence, is statistically significant and positive. This implies that sharing information on Facebook is highest when both benefits and risk perceptions are high. While a cross-sectional survey is not sufficient to articulate why this may be the case, it is possible that given the importance of Facebook in users' social lives, they share information on it despite being concerned about the consequences of sharing that information (or, alternatively, users who share too much information become concerned about their privacy). Second, the a_2 parameter, which is about the curvilinearity of the line of congruence, is significant, implying that the congruent relationship observed becomes stronger as perceived benefits and perceived risks increase. Third, the a_3 parameter, which pertains to the line of incongruence, is significant and positive. This implies that, in line with the premise of the privacy calculus model, sharing information on Facebook increases when perceived benefits are higher than perceived risks.

Tab. 2: Polynomial regression coefficients and surface parameters

Coefficient	Description	*b*	*se*	*p*
Polynomial Regression				
b_1	U&G of Facebook (Benefits)	.85	.08	< .001
b_2	Privacy Concerns (Risks)	.01	.07	.834
b_3	U&G of Facebook^2	.32	.06	< .001
b_4	Privacy Concerns * U&G of Facebook	.14	.08	.075
b_5	Privacy Concerns^2	.02	.04	.598
Response Surface				
a_1	$b_1 + b_2$	.87	.08	< .001
a_2	$b_3 + b_4 + b_5$	.48	.07	< .001

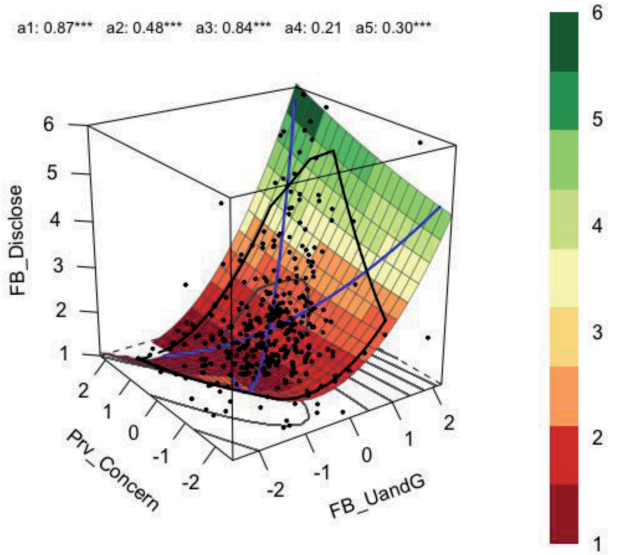

Fig. 2: RSA Predicting Disclosure on Facebook.

Tab. 2: Polynomial regression coefficients and surface parameters *(Continued)*

Coefficient	Description	*b*	*se*	*p*
a_3	$b_1 - b_2$	.84	.12	< .001
a_4	$b_3 - b_4 + b_5$	.21	.13	.110

The illustration provided above underscores how RSA can help offer new insights into the privacy calculus that individuals engage in under different circumstances. Specifically, the illustration showed that even when we do not observe a direct, linear relationship between privacy risk perceptions (privacy concerns) and privacy management behavior (disclosure on Facebook), risk perceptions still matter for the balance individuals seek between risks and benefits.

It is important to note that there is a multitude of such contexts / circumstances that RSA could help identify. Let me give two examples that only focus on the linear relationship between risk and benefit perceptions and self-disclosure. The first one would be when users underestimate risks because they do not have sufficient information about them. When individuals underestimate risks, we would expect a positive relationship between the size of the difference between benefits (high) and risks (suppressed, low) and disclosure behavior. Within the RSA framework, we would observe that while benefits have a positive and linear main effect,

concerns do not have a main effect (non-significant b_2); furthermore, the line of incongruence would be positive (significant a_3). As discussed in the previous sections, the second example would be one where users suppress concerns about risks either because there are no options for protecting privacy without giving up an important service or product or because the benefits are perceived to be too high. In such a context, we can expect high-risk perceptions, but risk perceptions would not have a direct, linear impact on behavior (non-significant b_2). Hence, what can be expected in RSA results is that disclosure behavior will be positively associated with a congruent increase in both benefit and risk perceptions (significant a_1) with again a non-significant main effect of risk considerations (non-significant b_2).

It should also be noted that RSA would also be useful in understanding individuals' privacy management behavior in response to varying levels of risk and efficacy perceptions or varying levels of declarative ("knowing that") and procedural dimensions ("knowing how") of privacy literacy.[24] For example, RSA would allow us to investigate generational differences regarding the extent to which general awareness of risks may translate into protective behavior as a function of procedural knowledge about how to protect oneself from privacy intrusions. Given these considerations, in addition to proper analytical approaches (such as the RSA introduced in this section), what is needed is a framework that can allow us to more systematically study contexts and circumstances such as the ones described hereinabove. In the next section, I will shortly summarize a new framework developed by the CPRN.

B A Primer on a Framework for Studying Privacy Comparatively

The development of a comparative understanding of privacy and surveillance is of special importance given the rise in the cross-border flow of digital services and data. In a similar vein, a comparative approach to privacy is required due to the continuous conflict between national and international regulatory frameworks, global platforms, and micro-level individual experiences. However, much recent research on privacy and surveillance has a single-nation focus, frequently looking at

24 Sabine Trepte and others 'Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS)' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law* (Vol 20, Springer Netherlands 2015).

privacy through the lens of Western, educated, industrialized, affluent, and democratic (WEIRD) societies.[25]

A few years ago, the CPRN was founded by (in alphabetical order) Dmitry Epstein (Department of Communication and the School of Public Policy, Hebrew University of Jerusalem, Jerusalem, Israel), Philip Masur (Vrije Universiteit Amsterdam, Amsterdam, The Netherlands), Kelly Quinn (Department of Communication, the University of Illinois at Chicago, Chicago, USA), and Carsten Wilhelm (Center for Research on Economies, Societies, Arts and Techniques, Université de Haute Alsace, Mulhouse, France) to advance comparative research in privacy. Recently, the network expanded with the inclusion of Christoph Lutz (Department of Communication and Culture, BI Norwegian Business School, Oslo, Norway) and me (Koç University, Istanbul, Turkey).

One of the preliminary purposes of the CPRN is to create a conceptual and methodological framework for investigating the antecedents, potential mediators, and effects of privacy-related decision-making and behavior. Comparative studies are frequently viewed as contrasting several macro-level units such as countries and regions. However, while previous research[26] highlights the potential benefit of employing macro-level units such as nation-states as indicators of cultural differences,[27] the global flow of digital services and data has undermined the utility of such containers.[28] Given these factors, the comparative privacy research framework will prioritize comparative research along five axes:[29]

A cultural axis that includes a comparison of regional or national factors along with the comparison of subcultures that may share characteristics across the more macro level cultures.

A social axis pertaining to clusters that people are grouped into as a function of socio-demographic factors. Additionally, this axis would take into consideration organizational structure characteristics that are necessarily interwoven with power and control.

A political axis that would pay attention to how political and regulatory systems may influence how privacy is protected and experienced.

---

25 Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008); Philip F Wu, Jessica Vitak and Michael T Zimmer, 'A contextual approach to information privacy research' (2020) 71(4) Journal of the Association for Information Science and Technology 485.

26 Baruh, Secinti and Cemalcilar (n 1), cf also Daniela Wawra, in this volume, at 51.

27 Geert Hofstede, 'Dimensionalizing Cultures: The Hofstede Model in Context' (2011) 2(1) Online Readings in Psychology and Culture.

28 Frank Esser, 'The emerging paradigm of comparative communication enquiry: Advancing cross-national research in times of globalization' (2013) 7(1) International Journal of Communication 113.

29 Masur and others (n 13).

An economic layer that is related, among others, to the level of competition within a market and / or the level of openness of a given market.

A technological axis regarding technological environments in which people communicate and enact their lives, affordances of specific technologies and platforms, and communication modalities (eg, face-to-face vs. teleconferencing).

In this regard, comparative privacy research may frequently focus on macro-level units (eg, cultures, nations, political systems), but it should also engage in comparisons at the meso- (eg, different organizations) and micro-levels (eg, different interactional contexts like face-to-face interactions vs. mediated interactions). It is important to note that the framework put forward by the CPRN is not merely about disclosure and privacy calculus. However, with regard to the focus of this volume, let us give three examples that can help explain how this framework would be useful for studying disclosure.

First, we focus on questions about privacy literacy, discussed in the previous section. A potentially paradoxical outcome of privacy literacy is that higher literacy may result in higher self-disclosure. On the one hand, this may be due to a "control paradox"[30], whereby users with higher literacy feel more confident about their ability to protect their privacy and consequently share more information.[31] On the other hand, this may be the result of what has been called as *privacy fatigue*[32], *online apathy*[33] or *privacy cynicism*[34]*:* The more online users learn about how data is collected, collated and shared among institutions, the less efficacious they feel about the prospects of having a meaningful way of protecting their privacy. These possibilities underscore the contingent nature of the relationship between literacy and privacy management. For example, one pertinent question that comparative approaches are better equipped to address would concern how differences in economic and regulatory environments may be related to the trust that users place in themselves and in institutions as a predictor of self-disclosure. Relatedly, a comparison of socio-demographic factors like age or gender would be key in the

30 Laura Brandimarte, Alessandro Acquisti and George Loewenstein, 'Misplaced confidences: Privacy and the control paradox' (2013) 4(3) Social psychological and personality science 340.

31 Joseph Turow and Michael Hennessy, 'Internet privacy and institutional trust: Insights from a national survey' (2007) 9(2) New Media & Society 300.

32 Hanbyul Choi, Jonghwa Park and Yoonhyuk Jung, 'The role of privacy fatigue in online privacy behaviour' (2018) 81 Computers in Human Behavior 42.

33 Eszter Hargittai and Alice Marwick, 'What Can I Really Do? Explaining the Privacy Paradox with Online Apathy' (2016) 10 International Journal of Communication 3737.

34 Christoph Lutz, Christian P Hoffmann and Giulia Ranzini, 'Data capitalism and the user: An exploration of privacy cynicism in Germany' (2020) 22(7) New Media & Society 1168.

identification of risk groups that need to be targeted with different types of literacy interventions.

As a second example, let us turn to the question of whether focusing on individuals as the unit of analysis is sufficient for understanding privacy management behavior. Growing number of studies[35] and theoretical frameworks like the communication privacy management theory[36] underscore the interconnectedness of individuals in managing and handling their privacy. From the standpoint of privacy management, a turn toward groups and networks raises important theoretical and empirical questions, including but not limited to understanding 1) the impact of decisions made by individuals on the larger network, 2) the extent to which assemblages can be the basis for raising collective claims of harm on behalf of its members, and relatedly, 3) how the networked nature of privacy harms can be used to inform privacy impact analyses that are conducted at an institutional level.

As a third example, we consider how technological and political axes may influence what types of privacy- related concerns are important in terms of the use of a messaging application such as WhatsApp. In the context of Turkey, for example, fears of authoritarian pressure have made WhatsApp's end-to-end encryption an important benefit for users. In this context, vertical privacy concerns related to government surveillance, as opposed to vertical privacy concerns about a corporation's (ie, Meta) data practices, may possibly predict the uptake of the application. Another relevant question would be the extent to which Turkish users suppress horizontal privacy concerns because of the expected social benefits of using WhatsApp. Among parents in Turkey, for example, each parent is part of multiple (and many times large) WhatsApp groups related to one's child, school, and sports teams. Most members of the group are not individuals they have met in person. Yet, issues including COVID diagnosis, emotional breakdown of a child, and even marital problems are discussed in the groups (and interestingly, sometimes spillover from one group to the other without much consideration of contextual norms of sharing). These considerations underscore how cultural norms interact

35 Lemi Baruh and Zeynep Cemalcilar, 'It is more than personal: Development and validation of a multidimensional privacy orientation scale' (2014) 70 Personality and Individual Differences 165; Alice E Marwick and Danah Boyd, 'Networked privacy: How teenagers negotiate context in social media' (2014) 16(7) New Media & Society 1051; Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 475; Ralf de Wolf, Koen Willaert and Jo Pierson, 'Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook' (2014) 35(8) Computers in Human Behavior 444.

36 Sandra Petronio, *Boundaries of privacy: Dialectics of disclosure* (State University of New York Press 2002); Sandra Petronio and Jeffrey T Child, 'Conceptualization and operationalization: Utility of communication privacy management theory' (2020) 31 Current Opinion in Psychology 76.

with technological affordances (the end-to-end encryption along with network effects making WhatsApp the default messaging app), the political environment (an authoritarian political system where fears of government surveillance is high) and social factors (dual income, white-collar families in a city like Istanbul where parents and children have very long commutes) and encourage public intimacies[37] on WhatsApp. From a comparative perspective, a crucial question concerns how differences in these axes translate into differences in information-sharing behavior.

C Conclusion

My aim in the presentation that I made during the *Vectors of Data Disclosure Conference*, and in this short contribution summarizing the presentation, was two-fold. First, building on a recent article illustrating the use of response surface analysis for addressing questions about privacy calculus,[38] I aimed to introduce RSA as a tool that can be utilized to understand the impact of variations in contextual elements in terms of how they influence the conjoint effects of risk and benefit perceptions as components of the calculus. Second, through several examples, I tried to underscore the importance of understanding privacy calculus contexts with the comparative framework that the CPRN has developed.[39]

It should be noted that the examples I showed during the presentation and in this short contribution present a very limited overview of the possibilities offered by RSA and the comparative privacy research framework. For example, as mentioned above, from an analytical point of view, RSA can be applied to other privacy-related variables, such as the balance between risk and efficacy perceptions. Relatedly, Trepte and colleagues[40] make an important distinction between declarative vs procedural knowledge when it comes to privacy-management behavior. The balance between these two types of knowledge may be critical in terms of identifying when literacy translates into a willingness to protect one's privacy vs the perception that no matter what one does, one cannot protect their privacy. Also, for the comparative perspective, the examples that I gave focused on the five axes of comparison in relation to self-disclosure. However, the comparative privacy framework

37 Lemi Baruh and Levent Soysal, 'Public Intimacy and the New Face (Book) of Surveillance The Role of Social Media in Shaping' in Tatyana Dumava and Richard Fiordo (eds), *Handbook of Research on Social Interaction Technologies and Collaboration Software: Concepts and Trends* (IGI Global 2010).

38 Kezer, Dienlin and Baruh (n 10).

39 Masur and others (n 13).

40 Trepte and others (n 24).

also works with individual-level differences such as psychological traits, or within-person processes, such as comparing different situations or motivations across time. Second, the comparative privacy framework is not only about disclosure but more generally about privacy. For example, a comparative privacy framework will be particularly useful in addressing questions related to how differences in the ways in which we conceptualize privacy (as an individual right vs. as a collective good; as control over communication intimacy vs. control over data) may be crucial in terms of how we approach privacy protection, what practices we find acceptable, and who, we think, should be responsible for protecting privacy.

Lothar Determann

California Privacy Law Vectors for Data Disclosures

Lothar Determann teaches computer, internet and data privacy law at the Free University of Berlin, University of California, Berkeley School of Law and Hastings College of the Law, San Francisco, and he practices technology law as a partner at Baker McKenzie LLP in Palo Alto. This contribution reflects views the author shared in presentations at the Conference on 'Vectors of Data Disclosure' hosted by the Bavarian Institute for Digital Transformation in Munich in June 2022, <www.bidt.digital/event/conference-vectors-of-data-disclosure/> and at the US Federal Trade Commission privacy hearings in April 2019 and contains excerpts of prior articles, including Lothar Determann, 'Data Privacy and Data Security Legislation: Policy focus on data processing regulation v. specific individual harms' in David A. Marcello (ed), *International Legislative Drafting Guidebook: 25th Anniversary Celebration* (Carolina Academic Press 2020) 189; Lothar Determann, 'Privacy and Data Protection' (2019) 1 Moscow Journal of International Law 18; Lothar Determann, 'La normativa de protección de datos en la encrucijada' [Data Privacy Legislation at Crossroads] (2019) almacen de derecho <https://almacendederecho.org/la-normativa-de-proteccion-de-datos-en-la-encrucijada> accessed 07.02.2023.

https://doi.org/10.1515/9783111010601-008

At the conference on 'Vectors of Data Disclosure' in June 2022, scholars from several disciplines came together to examine when and why persons or organizations share information. This depends on numerous vectors, ie, directional forces[1] that drive if, when, where, to whom and under what conditions data is disclosed. Humans disclose personal information about themselves based on individual inclinations, socialization, cultural norms, power dynamics, technological necessities and economic considerations, such as perceived benefits.

Lawmakers also provide vectors for data disclosures, directly and indirectly. For example, under tax laws, tax payers must disclose very sensitive and detailed data to authorities in tax returns.[2] Under national security laws, citizens must not disclose state secrets.[3] Beyond such direct legal vectors, various laws drive data disclosures indirectly and in different directions. For example, businesses are enabled and encouraged to restrict disclosures of business secrets under trade secret laws.[4] Under competition laws, on the other hand, competitors are able to demand access to data.[5] Whistleblowers are exempt from secrecy obligations to encourage disclosures of information concerning misconduct, wrongdoing and illegal activity.[6]

Privacy and data protection laws contain vectors in different directions concerning data disclosures. One key policy objective of the European Union (EU) General Data Protection Regulation (GDPR) is to remove obstacles to data disclosures within the common market, as evidenced in the title of the 'regulation [...] on the protection of natural persons with regard to the processing of personal data **and on the free movement of such data'** (emphasis added).[7] Also, organizations must disclose data to individual data subjects, data protection officers, and supervisory authorities on request under the GDPR.[8] But, for the most part, the GDPR points vectors for data disclosures in the other direction, namely against disclosure. Under the GDPR, individuals have rights to prohibit businesses from disclosing or even collecting their personal data[9] and from transferring personal data across

1 Vector means 'a quantity that has magnitude and direction' <www.merriam-webster.com/dictionary/vector> accessed 07.02.2023.

2 Eg German Income Tax Code (EStG) Section 25(3).

3 German Penal Code (StGB) Section 95.

4 Lothar Determann, Luisa Schmaus und Jonathan Tam, 'Trade Secret Protection Measures and New Harmonized Laws' (2016) CRi 179 and (2017) Computer & Internet Lawyer 1.

5 Eg <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077> accessed 07.02.2023.

6 Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] L 157/1, Art. 5(b) and Recital 20.

7 Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] L 119/1.

8 Art. 15(4) GDPR.

9 Eg Art. 18 GDPR.

borders.[10] Also, an individual can demand that organizations delete personal data about them.[11] More broadly, the GDPR prohibits any processing of personal data, unless individual data subjects consent or other statutory justifications are available,[12] and then only subject to minimization requirements[13] and extremely broad definitions of what constitutes 'personal data', roping in nearly all types of data that humans tend to be interested in.[14] These forceful vectors against data disclosures have increasingly hindered scientific and academic collaboration, information technology development, medical research, precision medicine, public health measures and free exercise of information and communication rights in the EU.[15] As a countermeasure, with vectors encouraging data disclosures, the EU is now debating an EU Data Act 'for a fair and innovative data economy'[16] instead of modernizing and deregulating its privacy law framework, leaving businesses and individuals in a confusing crossfire of vectors, requirements and prohibitions for and against disclosures.

United States and California privacy lawmakers have traditionally taken a more nuanced approach and mostly focused on ensuring that individual data subjects can make an informed decision about disclosures of personal data, but not outright prohibited or regulated personal data processing.[17] After expressly recognizing a right to privacy in the California Constitution in 1972 pursuant to a popular ballot initiative, California has enacted myriad sector-, harm- and situation-specific privacy law statutes nearly every year.[18] California enacted the first laws worldwide requiring companies to notify individuals of data security breaches (in 2002) and to post website privacy policies (in 2004).[19] More recently, California citizens pushed privacy legislation according to which businesses must specifically

10 Eg Art. 44–49 GDPR.

11 Eg Art. 17 GDPR.

12 Art. 6(1) GDPR.

13 Art. 5(1)(c) GDPR.

14 Art. 4(1) GDPR.

15 Winfried Veil, 'The GDPR: The Emperor's New Clothes – On the Structural Shortcomings of Both the Old and the New Data Protection Law' (2018) NVwZ 686.

16 <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113> accessed 07.02.2023.

17 Paul M Schwartz, 'Preemption and Privacy' (2008) 118 Yale Law Journal 902, 910916; Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 116 The Georgetown Law Journal 115, 138 et seq.

18 More generally on the adequacy of US privacy laws, see Lothar Determann, 'Adequacy of data protection in the USA: myths and facts' (2016) International Data Privacy Law 2016; Lothar Determann, 'US-Datenschutzrecht – Dichtung und Wahrheit' [US Data Protection Law – Myths and Facts] (2016) NvWZ 561.

19 Lothar Determann, *California Privacy Law, Practical Guide and Commentary* (4th edn, The Recorder 2020) Ch 1 and Ch 2(N) and (O).

notify Californians about sales of personal information, rights to object to the sale, the right not to be discriminated against in case of opt-out choices, and the value of personal information to the business.[20] These novel vectors for data disclosure are far more specifically tailored and suited to protect individual privacy rights than the somewhat outdated concept of a general prohibition with limited exceptions in the GDPR.[21]

This contribution is based on my presentation at said conference and introduces novel vectors for personal data disclosures under California privacy law in Part A, discusses fundamental differences in privacy legislation and data processing regulations in Part B, examines options for lawmakers in Part C, explores policy choices and tradeoffs for lawmakers in other countries in Part D and concludes with a summary and outlook in Part E.

A Data Monetization Trends and Consumer Information Requirements in California

Internet users have to share IP addresses of their devices in order to access websites, location information to see their position on online maps or automatically receive local weather updates, and mobile phone numbers to receive text messages. This is due to technical requirements that Sun Microsystem's CEO famously summed up in 1999 with 'You have zero privacy anyway. Get over it.'[22] Internet users may be willing to share additional personal information – which is not strictly required for technical reasons – as consideration for valuable services, in lieu of subscription fees or other payments. For example, companies offer discounts or opportunities to win a prize to consumers who are willing to register for loyalty programs, online accounts, or product trials, or to respond to surveys. Free from the shackles and chains of legacy broadcasting laws, individuals and businesses around the world developed the Internet as a free marketplace for ideas, goods and services.[23] Start-up companies were able to gain critical mass of users for

20 Lothar Determann and Jonathan Tam, 'The California Privacy Rights Act of 2020: A broad and complex data processing regulation that applies to businesses worldwide' (2021) 4 Journal of Data Protection & Privacy 7.

21 Art. 6(1) GDPR provides that '[p]rocessing shall be lawful only if and to the extent that at least one of the following applies:' and then lists individual consent and 5 other very limited exceptions that individual persons or organizations must claim to justify any processing of personal data.

22 <www.wired.com/1999/01/sun-on-privacy-get-over-it/>.

23 Lothar Determann, *Kommunikationsfreiheit im Internet* (Nomos 1999).

new innovative services like online maps, social media networks and user-generated content platforms by offering their services free of charge. To fund their operations, businesses sold advertising space and increasingly also personal data of users. Consumers traded data for online services that could never have been established with paid subscription models and mostly felt they received a fair bargain.[24]

Businesses consider data a valuable asset even if they cannot legally own data.[25] In recent years, companies in California and elsewhere have been strategic about collecting personal information for various purposes, including targeting advertisements, generating market insights, improving communications with consumers, developing products, and creating marketable consumer profiles that other companies are willing to pay for.[26] As companies have refined their data collection and monetizing methods, consumers have found it increasingly difficult to understand how their data is used, monetized and valued. Consumers and lawmakers have been growing concerned that consumers may be unable to make informed decisions and obtain fair compensation for disclosures of their data. They started questioning the fairness of the data-for-services bargain.[27]

To empower consumers and strengthen their ability to drive a fair bargain, California lawmakers have insisted on accurate and comprehensible disclosures. In 2004, California enacted the first law worldwide specifically requiring companies to publish website privacy policies.[28] Companies are required to inform consumers about their data processing practices under myriad other laws, from Art. 1 of the California Constitution to special rules for Supermarket Club Cards.[29] Yet, some consumer and privacy advocates felt that the incremental changes brought by routine advancements of sector-, harm- and situation-specific California privacy laws were not enough.[30]

In 2018 and 2020, privacy advocates brought about the California Consumer Privacy Act (CCPA) by way of a ballot initiative that also triggered an avalanche of additional legislation and regulations as well as the creation of a California Pri-

24 Lothar Determann, 'Social Media Privacy – 12 Myths and Facts' (2012) Stanford Technology Law Review 7.

25 Lothar Determann, 'No One Owns Data' (2018) 70 Hastings Law Journal 1.

26 Lothar Determann, 'California data broker registrations: Who made the list on Jan. 31?' (*IAPP Privacy Advisor*, 11 February 2020) <https://iapp.org/news/a/california-data-broker-registrations-who-made-the-list-on-jan-31/> accessed 07.02.2023.

27 Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).

28 California Online Privacy Protection Act (CalOPPA), California Bus & Prof Code paras 22575–22579.

29 See Determann (n 19) ch 2.

30 See Californians for Privacy <www.caprivacy.org/>.

vacy Protection Agency, the first agency specifically dedicated to privacy protection in the United States.[31]

Under CCPA, businesses must not discriminate against consumers who exercise their rights to information deletion or object to the selling or sharing of their personal information. At the same time, businesses shall not be prohibited under the CCPA from 'charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data' or 'from offering loyalty, rewards, premium features, discounts, or club card programs.' The California Attorney General promulgated in 2020 regulations that a business that offers a financial incentive or price or service difference shall provide a 'notice of financial incentive' with prescribed disclosures, in addition to 'at collection notices', which businesses must generally provide at or before the time they collect personal information from consumers. In the 'notice of financial incentive', businesses must disclose material terms of incentive programs, including the value of the consumer's information.

In enforcement actions concerning failures to provide notices of financial incentive, the California Attorney General offered the businesses 30 days to come into compliance with the CCPA before further enforcement actions would be commenced (as is currently required under the CCPA). In a press release issued by the office of the Attorney General, Bonta 'urge[d] all business[es] in California to take note and be transparent about how you are using your customer's data', signaling an intent to prioritize enforcement of loyalty and other similar consumer programs moving forward.

In notices of financial incentives, businesses must clearly describe the material terms of their financial incentive program. Businesses must include the following information in the notice:

- A succinct summary of the financial incentive or price or service difference offered.
- A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data.
- How the consumer can opt-in to the financial incentive or price or service difference.

31 Lothar Determann, 'Kaliforniens erste Datenschutzbehörde – dank Volksentscheid. California Privacy Rights Act (CPRA) verschärft California Consumer Privacy Act (CCPA) und gilt auch für deutsche Unternehmen' (2021) ZD 69; Determann and Tam (n 20).

- A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right.
- An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:
- A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference.
- A description of the method the business used to calculate the value of the consumer's data.

A notice of financial incentive must clarify how a consumer can 'opt in' (a term not defined in the CCPA), which should not be conflated with a requirement under the CCPA to obtain consent (a defined term in the CCPA). Many financial incentive programs require terms of use and thus a need for an agreement involving some form of consent, anyhow (and in such cases, a separate consent could be added), but there are contexts where companies ask for personal information that may trigger a requirement for a financial incentive notice where terms and conditions may not be required. Per California Civil Code Section 1798.125, a business may enter a consumer into a financial incentive program only if the consumer gives the business prior 'opt-in consent' pursuant to Cal. Civ. Code Section 1798.130. But the reference to 1798.130 is confusing because 1798.130 does not provide for how to obtain opt-in consent and, as amended, Section 1798.130 has a heading of 'notice, disclosure, correction, and deletion requirements'. If the reference is to be given any meaning, it supports that consent is not required before first enrolling a consumer in a financial incentive program because 1798.130(a)(5)(A) requires that businesses include in their CCPA online policy a description of a consumer's rights pursuant to 1798.125 and methods for submitting requests. There are other possible readings of the CCPA on this point. But the CCPA generally does not require opt-in consent for data collection and has an opt-out structure with regards to selling personal information. It would seem logical that the drafters of the CCPA meant for a similar opt-out regime with respect to financial incentive programs to apply (where opt-in consent and waiting 12 months is only required after someone first opts out). And the title of 1798.125 has been amended to say 'consumer's right of no retaliation following opt-out or exercise of other rights', which would seem supportive of such interpretation.

Businesses now face the difficult task to estimate the value of consumers' personal information. They should carefully consider all implications from an accounting, tax and litigation perspective. For example, once a business publishes a value pertaining to personal information, the stated value will likely be considered in unrelated contexts and disputes such as data security breaches, trade secret misappropriation, breaches of marketing collaboration contracts with busi-

ness partners, unclaimed property compliance (escheat), or transfer pricing arrangements in multinational groups. Courts will not be bound by the business's valuation, of course, but adversaries may hold a published valuation number against a business as an admission of value and make it difficult to argue for a different valuation.

Consumers may find the additional information helpful to make more informed decisions on how much personal information they want to disclose to a particular business or in the context of a specific service or incentive programs. Also, academics, journalists, privacy advocates, consumer protection association and other information intermediaries will likely conduct studies on value disclosures regarding personal information to help consumers compare offerings and make more informed decisions. At the same time, businesses face skyrocketing costs and challenges in adjusting their privacy law compliance programs to the myriad new and highly prescriptive privacy laws in California and elsewhere.[32] Compliance costs are enormous[33] and favor larger and mature organizations, thus raising market entry barriers for start-up companies and reducing competition as well as innovation. With the antidiscrimination provisions in CCPA,[34] businesses are vectored to move away from charge-free services models that made the Internet so successful in the first place. Businesses must offer the same level of services to consumers who opt out of personal information selling or exercise other rights under CCPA. It remains to be seen whether consumers will benefit from a fairer bargain, or whether the return to pre-Internet paid subscription business models ultimately drives a reduction in available services, consumer choice, innovation and competition.

B Privacy and Data Protection Legislation

The United States are at a crucial turning point with respect to the protection of individual privacy and regulation of data processing more broadly on a state and federal level. Several states have followed California in enacting comprehensive consumer privacy laws, including Nevada, Virginia, Colorado, Utah and Con-

32 See <www.uschamber.com/major-initiative/data-privacy>.

33 The California Attorney General's office estimated a $55 billion cost (approximately 1.8 % of California Gross State Product) for initial compliance with the original CCPA, not including costs of ongoing compliance, responses to data subject requests, litigation, and adjusting to the many amendments, see Berkeley Economic Advising and Research, LLC, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations (2019) 19.

34 California Civil Code para 1798.125.

necticut by June 2022, with many more bills pending at the state and federal level. Businesses have been pushing for decades for laws at the federal level to preempt the proliferation of diverging US state laws that hamper interstate commerce and innovation.[35] Lawmakers and regulators are debating multiple controversial questions, including the following: Should laws governing data processing impose data minimization and prohibitions as a default or continue to focus on individual privacy harms? How should laws reconcile free speech and access to information with the privacy-based 'right to be left alone'? Should anyone own data? How can governments ensure access to data for law enforcement, national security and governance purposes?

Answers to these questions and corresponding legislative measures are likely to impact the willingness of individuals to disclose personal data and the consideration they expect in return. But, the vectors of personal data disclosures also depend on cultural norms, habits and history, which vary from country to country and state to state within the USA.

I Privacy

Privacy is a sphere that a person controls regarding his mind, thoughts, decisions, communications, body, dignity, home and personal effects, such as papers and smart phones.[36] The right to privacy is the right of an individual to be let alone.[37] It is a right against other people and legal entities, including family members, neighbors, company representatives and government agents, who may invade a person's privacy by trespassing, entering a person's home without permission, accessing personal files on a computer or forcing a person to reveal sensitive personal information about herself.

One can find privacy best where no other people are, in solitude, furthest away from other humans. In civilization, one trades privacy for benefits of living and interacting with others. One lets other people into one's life to learn, communicate, collaborate, trade, socialize and seek help. One individual's right to privacy can become an intrusion into another person's rights to information, free speech or security.

35 See <www.uschamber.com/major-initiative/data-privacy>.

36 Lothar Determann, 'Privacy Please' (YouTube, 28 June 2021) <www.youtube.com/watch?v=7u0XNVHXzus>.

37 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

With respect to information specifically, privacy means control over the dissemination of personal information, discretion regarding who may know what about one's body and mind, the choice to remain anonymous, the ability to keep thoughts and communications confidential, and the power to avoid being photographed, filmed or audiotaped.

Individuals feel different needs for data privacy depending on their personal circumstances. A child prodigy living in a large city may physically suffer from excessive invasions into privacy by journalists while a reality television star may welcome any publicity she can get. A dissident may depend on data privacy for his life while an established politician may depend on publicity for his livelihood.

Also, people in different cultures, societies and political systems feel differently about privacy. Americans care deeply about individual freedom, property and privacy in their homes and personal effects, but tend to be less concerned about data collected on public spaces or the Internet.

Germans have created the world's first and strictest regulation of data processing, but they have not coined an exact equivalent of 'privacy' in the German language. In everyday language, Germans may occasionally refer to 'Privatsphäre' (literally translated: 'private sphere') as an abstract sphere and aspect of the general right of personality ('Allgemeines Persönlichkeitsrecht') in which the state and other persons should not interfere. Unlike the US concept of 'privacy', German 'Privatsphäre' is not directly linked to one's home or property. German courts and lawyers additionally use terms like 'informationelle Sebstbestimmung' (information self-determination) and 'Datenschutz' (data protection) with respect to the regulation of data processing, which exists separately from civil law claims pertaining to violations of one's rights to private sphere and personality. The General Data Protection Regulation (GDPR), which is ultimately modelled after German data protection laws, does not mention the term 'privacy' even once.

In Russia, views and terminology regarding privacy have been evolving, particularly since the end of the Soviet Union and communism, which prioritized collective objectives over individual privacy. A direct equivalent of 'privacy' has not yet evolved in the Russian language. 'Приватность' is a modern borrowed term derived from the English term 'private.' 'Конфиденциальность' means literally 'confidentiality' but has been used to translate 'privacy' in the past; for example, 'Privacy Policy' has commonly been translated as 'Политика конфиденциальности.' More recently, 'приватность' is used to translate 'privacy.' The closest equivalent to 'private sphere' is 'Неприкосновенность частной жизни,' which means literally the 'sanctuary of private life' and is used in literature and legislation but not in everyday language. 'Информационная приватность' means 'information privacy' and 'data protection' means 'Защита персональных данных' and is common-

ly found in Russian legislation. For example, the Russian Data Protection Law is called 'Закон о защите персональных данных'.

In China, the word '隐私' is commonly used to refer to privacy. '隐' means hidden, and '私' means personal, private, and secret. '隐私' commonly refers to private and personal information that an individual prefers to keep secret. One potential difference between the word 'privacy' and the word '隐私' is that '隐私' focuses more on the subjective intent of an individual to keep things from other people while 'privacy' often refers to the objective state or condition of being free from observation or disturbance by other people. The word '隐私' first appeared in the Zhou Dynasty (1046–256 BCE). Back then, '隐私' meant 'clothes'; having it or not was thought to be one of the most obvious differences between civilized people and barbarians or beasts.

Around the world, data privacy needs have changed over time and increased exponentially with the development of information technologies. In the 18th century, citizens were most concerned about physical privacy intrusions in the form of arrests, searches and seizures by government agents. In the 19th century, as photography developed, privacy invasion by the press became more noticeable. In the 20th century, computers, data bases and the Internet started to provoke fears of glass citizens, repressive surveillance states and intrusive business practices. Today, mobile phones, connected cars, planes, trains, industrial machines, toys and other devices on the Internet of Things (IoT) generate vast amounts of data and information and the total amount of stored data worldwide is expected to double every two years.

II Privacy Law and Data Processing Regulation

As individuals have felt an increasing need for data privacy over time, states enacted laws protecting privacy. Express references to privacy can be found increasingly in constitutions, international treaties and statutes since the second half of the last century.[38]

38 David Banisar and Simon Davies, 'Global Trends in Privacy Protection' (1999) 8 Journal of Computer and Information Law 1 et seq; Lee A Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1999) 6 International Journal of Law and Information Technology 247 et seq; Bert-Jaap Koops and others, 'A Typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483.

1 Constitutional Safeguards

The United States maintain the oldest written constitution. Its bill of rights dates back to 1791 and does not contain an express right to privacy, only a limited prohibition of unreasonable searches and seizures in its fourth amendment. The citizens of the State of California added an express right to privacy to the California Constitution in 1972 by way of a ballot measure in a general election, but there has not been enough consensus in the United States to add such a right to the federal constitution.

Germany enacted its current constitution in 1949 as its 'basic law' without expressly referring to 'privacy', but protecting human dignity in Art. 1(1), a right to 'unfold one's personality' in Art. 2(1), the confidentiality of mail and telecommunications in Art. 10(1) and the sanctity of one's home in Art. 13(1). In December 1983, weeks before the turn to the year for which George Orwell had predicted grave intrusions on individual privacy in his novel '1984', the German Constitutional Court recognized an implied right to information self-determination emanating from the express rights to dignity and personality in Art. 1(1) and 2(1) when German citizens challenged an expansive federal census measure.[39]

Newer constitutions tend to expressly protect a right to privacy, including, for example, the constitutions of Russia (Articles 23, 24 and 25) and South Africa (Section 14).

2 International Treaties

The Universal Declaration of Human Rights of 1948 refers to privacy expressly in Art. 12, as do the subsequently adopted International Covenant on Civil and Political Rights (Art. 17), UN Convention on Migrant Workers (Art. 14), UN Convention of the Rights of the Child (Art. 16), European Convention for the Protection of Human Rights and Fundamental Freedoms (Art. 8) and the American Convention on Human Rights (Art. 11). The Charter of Fundamental Rights of the European Union does not refer to privacy, but protects a right to 'private life' in Art. 7 and the 'protection of personal data' in Art. 8.

---

39 German Constitutional Court, 65 BVerfGE 1 English translation <https://freiheitsfoo.de//files/2013/10/Census-Act.pdf> accessed 07.02.2023.

3 Statutes

National statutes protecting privacy have become more common since in 1970 the state Hessen in Germany enacted the first data protection law worldwide. When Governor Oswald signed the Hessian data protection law into force, he referred to George Orwell's novel '1984' and declared that the Hessian data protection law was intended to prevent the surveillance state forecasted by Orwell. Other countries in Europe followed. The European Community then harmonized national data protection laws in Directive 95/46/EC (the 'Data Protection Directive'), which the European Union replaced effective 2018 by a General Data Protection Regulation (GDPR).

More and more countries have followed Europe and also regulated the processing of personal data with general data protection regulations. In August 2018, Brazil enacted a GDPR-like data protection law and India published a GDPR-like bill which has been heavily debated since, but still not been enacted in June 2022.[40]

The United States, on the other hand, had opted against broad omnibus data processing regulation until recently. Since the early 1970s, Congress and state legislatures have been enacting hundreds of sector-, situation- and harm- specific data privacy laws.[41] When California privacy advocates pushed for data processing regulation in the form of CCPA in 2018, the California legislature followed only reluctantly, provoking a second ballot initiative in 2020, which Californians passed with a resounding majority. In other US states, legislatures followed the trend with statutes modelled after CCPA, but this does not change the vector for omnibus data processing regulation in the United States did not originate from parliaments, but rather from privacy advocates and ultimately popular majorities with voters.

III Policy Reasons for Privacy Protections and Limitations

Governments typically protect privacy to safeguard individual human dignity and freedom. Under the shield of data privacy protection, citizens are more empowered to exercise civil rights, such as the freedom of speech, religion and assembly. This in turn helps secure the functioning of the democratic process. Also, citizens need protection from psychological, economic and other privacy harms that states, businesses, criminals and others cause, for example by identity theft; blackmail; bully-

40 See Lothar Determann and Chetan Gupta, 'Indian Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018' (2018) Berkeley Journal of International Law.

41 Schwartz (n 17).

ing; stalking; revelation of secret location or identities of spies, domestic abuse victims or persons in witness protection programs; stigmatization based on addictions, diseases, political opinions, religion, race or sexual preferences; computer hacking; irritating direct marketing methods; unfair business practices based on surreptitious data collection; and discrimination by employers, banks and insurance companies based on information about pre-existing health conditions.[42]

There are also reasons why – and situations when – governments do not protect, but rather invade privacy. The executive branch of governments fulfils many functions, most importantly law enforcement, that necessitate data processing and tend to collide with privacy protection agendas. Additionally, legislatures and courts also safeguard interests and policy objectives that conflict with data privacy, such as freedom of information and commercial enterprise. One person's right to gather and share information on another person can intrude on the other person's interest in data privacy. Different jurisdictions balance these conflicting policy goals differently.

The U.S., for example, tends to hold freedom of speech, information and commercial enterprise in relatively high regard and therefore decided against enacting the kind of omnibus data protection laws that are prevalent in Europe. Also, after the terrorist attacks of September 11, 2001, the United States has been very focused on national security and ramping up government surveillance programs. In Europe, on the other hand, people still remember what surveillance by totalitarian regimes has done to them. European lawmakers have decisively acted to limit the automated processing of personal data and carved out narrowly defined exceptions for press, media and non-commercial activities. Anyone trying to understand, interpret and apply data privacy laws has to consider the various conflicting interests and their relative status in the applicable legal system.

Without security, there can be no privacy; criminals, companies and foreign governments will invade individual privacy if security is not safeguarded. There can be security without any privacy, though. A totalitarian state focused on absolute security will monitor all individuals at the expense of their privacy. But, this is not necessary and reasonable degrees of security and privacy can co-exist. There

42 Danielle K Citron, 'Sexual Privacy' (2019) Yale Law Review; Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087; Daniel J Solove and Danielle K Citron, 'Risk and Anxiety: A Theory of Data-Breach Harms' (2018) Texas Law Review; Ryan Calo, 'Privacy Harm Exceptionalism' 12 Colorado Tech Law Journal 361 (2018); Amit Datta and others, 'Automated Experiments on Ad Privacy Settings' (2015) De Gruyter Open; Margaret Hu, 'Big Data Blacklisting' (2015) 67 Florida Law Review 1735, 1809; Mikella Hurley and Julius Adebayo, 'Credit scoring in the era of big data' (2016) 18 Yale Journal of Law & Tech 148, 151; Danielle K Citron and Frank Pasquale, 'The Scored Society: Due Process For Automated Predictions' 89 (2014) Washington Law Review 15.

cannot be free speech and democracy without privacy or security. Societies have to strike a balance with respect to privacy and security.

C Legislative Approaches

The terms 'data privacy' and 'data protection' are often used interchangeably, in particular in the context of comparisons of Anglo-Saxon data privacy laws and continental European data protection laws. Also, data security, data residency, data retention, data ownership and trade secret requirements are often thrown into the mix. But, the approaches, purposes and effects are quite different.

I Privacy Protection

The individual person and her autonomy is the central focus of privacy laws. Data privacy laws are intended to protect individuals from intrusion into reasonable privacy expectations, interception of confidential communications and other specific privacy harms.

Data privacy laws typically contain requirements regarding notice, choice, data security and sanctions. Individuals must be notified about how their data is handled so they can decide how much information they share, with whom and for what consideration. If they have access to sufficient information in privacy policies and other notices, they can adjust their conduct or privacy expectations. In particularly sensitive scenarios, companies may need to obtain express and informed consent. If companies fail to live up to their commitments in privacy policies or apply reasonable security safeguards and cause harm, then individuals can assert claims in private lawsuits including class actions. Regulators and law enforcement authorities can also sanction offenders in particularly egregious privacy law violations.

II Data Protection

The processing of personal data is the central focus of data protection laws. European legislatures have taken George Orwell's warnings to heart and view automated data processing as an inherently dangerous activity warranting strict regulation.

The GDPR, like previous EU data protection regulation, builds restrictions and limited exceptions around a fundamental prohibition of any processing of personal

data in Art. 6(1) GDPR. European data protection laws are first and foremost intended to restrict and reduce automated processing of personal data. Individual privacy expectations, harm potential, choice or consent are not predominantly relevant. Accordingly, broad definitions of 'personal data' and 'processing' prevail and even publicly available data is covered. Companies are required to minimize the amount of data they collect, the instances of processing, the people who have access and the time periods for which they retain data.

Besides basic prohibitions and minimization principles, data protection regulations typically establish data protection authorities, impose registration and approval requirements, prescribe filing fees, mandate the designation of local representatives and internal data protection officers, restrict international data transfers, mandate data protection impact assessments and require that companies maintain data inventories and accountability documentation that data protection authorities can routinely audit. Data protection authorities are also primarily tasked with enforcing data protection laws.

Data protection laws can indirectly benefit individual privacy if they cause companies and governments to process less personal data. But, protecting individual privacy is not the direct focus of the GDPR or other EU data protection laws. Individual privacy expectations, needs or harms can factor into data protection impact assessments, determinations whether security breaches have to be notified under Art. 33 or 34 GDPR, and the application of Art. 6(1)(f) GDPR, the 'legitimate interest exception' to the general prohibition of automated data processing. But, many other requirements and restrictions apply regardless of individual privacy considerations.[43]

III Information Access Blocking Prohibitions

Overly restrictive vectors against data disclosures create needs for corrections. In the EU, data processing regulation has literally become unhealthy.[44] But instead of modernizing and deregulating data processing regulations, EU lawmakers are debating corrections in the form of an EU Data Act 'for a fair and innovative data economy'.[45] At the same time, competition law authorities pressure companies

43 For a review of the GDPR as 'the law of everything', see Helen Dixon and Lothar Determann, 'International Privacy Law – Year in Review' (*Baker McKenzie*; 10 May 2022) <https://www.bakermckenzie.com/en/insight/publications/2022/06/international-privacy-year-in-review-for-us-practitioners> accessed 07.02.2023.

44 Lothar Determann, 'Healthy Data Protection' (2020) 26 Michigan Tech Law Review 229.

45 <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113> accessed 07.02.2023.

to provide access to data to competitors and refrain from implementing compliance measures that EU data processing regulations and electronic communications privacy laws seemingly require.[46]

In the United States, counter-measures to data processing regulations have largely been unnecessary, because lawmakers had narrowly tailored privacy laws to protect individual rights in sector-, harm- und situation-specific laws. But, the 'information blocking' prohibitions in the US Cures Act are a sector-specific example of countermeasures to redirect unhealthy vectors against medical data disclosures resulting from US federal health privacy laws.[47] Originally, US lawmakers sought to promote responsible medical data disclosures for treatment, research and patient access purposes in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), subject to safeguards in Privacy and Security Rules.[48] Apparently, some healthcare providers and other covered entities continued to release health information only sparingly, even where HIPAA mandated or allowed medical data disclosures, possibly due to the overwhelming complexity of HIPAA and its associated rules.[49]

More generally, companies are vectored in confusingly different directions based on privacy, competition and consumer protection policy mandates in the United States. While the FTC punishes one social media network for enabling other companies to access its publicly available data too easily with a $5bn fine, the 9th Cir. Court of Appeals prohibits another social media network from applying restrictions to data access designed to protect user privacy.[50] Businesses and individuals are caught in a confusing crossfire of vectors, requirements and prohibitions for and against disclosures.

46 Eg <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077> accessed 07.02.2023; <https://digiday.com/media/why-googles-approach-to-replacing-the-cookie-is-drawing-antitrust-scrutiny/> accessed 07.02.2023.

47 Eg <www.healthit.gov/topic/information-blocking> accessed 07.02.2023.

48 Mark A Rothstein, 'HIPAA Privacy Rule 2.0' (2013) Journal of Law, Medicine and Ethics 525.

49 See Craig Konnoth, 'Regulatory De-Arbitrage in Twenty-First Century Cures Act's Health Information Regulation' (2020) Annals of Health Law.

50 See <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook> accessed 07.02.2023 and HiQ v. LinkedIn [2022] USCOA No 17–16783.

IV Data Security Laws

Legislatures around the world have started to supplement data privacy laws with increasingly specific data security laws that aim to protect individuals from specific harms resulting from unauthorized access to personal information, in particular identity theft. Examples include data security breach notification laws: California passed the first law in 2002, with most US states and many countries following suit thereafter. Also, more and more laws prescribe encryption or other technical and organizational measures, also known as 'TOMs'. In 2018, California added a duty on manufacturers of connected devices to design products with reasonable security measures and refrain from delivering products with default passwords, for example. Data security measures limit unauthorized access to information and thus protect data and individual privacy.

V Trade Secret Laws

Businesses use contracts and tort laws to protect confidential information from misappropriation by unauthorized persons. As a condition to trade secret claims, companies have to prove that they used reasonable efforts to keep their information secret, which often includes similar measures as required by data security laws with respect to personal data. Where confidential business information pertains to persons (as opposed to technologies or manufacturing processes, for example), trade secret law can also indirectly protect individual privacy. But, the primary purpose of trade secret laws is to protect business integrity and competition from unfair misappropriation of valuable confidential information.

VI Data Ownership

With property laws, states allocate real estate, chattels, intangibles or other items to individuals with an entitlement to exclude others in the interest of incentivizing innovation, creation, maintenance and investment regarding the allocated items. Legislatures typically exclude information as such from the scope of property laws, to preserve maximum public access. Also, it seems hardly necessary or in the public interest to incentivize the creation of information. Even without rewards in the form of property rights, companies and governments hoard enough data at the expense of individual privacy.

If individuals owned personal data about themselves, they could theoretically gain additional rights to defend their privacy. In practice, however, many individ-

uals would likely be induced or compelled to sell their personal data property rights, with the undesirable effect that the buyers could exclude the data subjects from personal information about themselves. Others could use property rights to withhold information about themselves that governments, companies or individuals legitimately need for public safety, security or other purposes. Therefore, no one owns or should own data.[51]

VII Freedom of Speech and Information

Individuals and their right to communicate and inform themselves is the core function of constitutional freedoms of communication and information. Privacy rights can directly conflict with rights to free speech and information. For example, defamation claims, censorship measures and 'rights to be forgotten' can be based on privacy laws and restrict the dissemination of information or access to data. Privacy rights can also complement rights to free speech and information, because people can speak more freely when they can remain anonymous or at least hide or obscure their identities from government or private prosecution. But, freedoms of speech and information do not typically protect privacy and rather intrude.

VIII Data Residency and Retention Requirements

Governments mandate that companies and citizens maintain certain documentation, records and information locally for minimum time periods, to be available for tax audits, law enforcement investigations and national security monitoring. Russia, Kazakhstan, Indonesia and the People's Republic of China have enacted particularly broad data residency requirements that are not limited to particular types of records but all personal data.[52] Data residency and retention laws are not intended to protect privacy. To the contrary, such laws limit individual privacy. European Union laws requiring companies to store Internet meta data for minimum time periods have been successfully challenged and invalidated based on constitutional safeguards for data privacy.[53]

---

51 Determann (n 25).

52 Lothar Determann, 'Data Residency Rules Cutting Into Clouds: Impact and Options for Global Businesses and IT Architectures' (2017) Bloomberg BNA Data Privacy & Security Law Report.

53 German Constitutional Court 1 BvR 256/08, (2010) NJW 833; Case C-293/12 Digital Rights Ireland v Ireland [2014] European Court of Justice 62012CJ0293.

D International Privacy Law at Crossroads

More and more countries are enacting or updating privacy laws based on one or more of the approaches described in the preceding Part C of this contribution. Many jurisdictions enact European-style data processing legislation and few follow the United States.[54] In fact, the United States itself is currently reconsidering its own approach. International privacy laws are at crossroads.

I Privacy v. Data Protection

When Hessen and then other German states and European countries started enacting data protection laws in the 1970s, the United States also considered this option, but decided against comprehensive regulation of data processing. Congress felt it was too early to appropriately identify and address potential privacy harms and balance privacy interests with freedom of information, innovation and economic freedoms.[55] Therefore, the United States resolved to pass sector-, situation- and harm-specific privacy laws as the need arises, at the state and federal level. This allowed information technology companies in the Silicon Valley to grow and become industry leaders in semiconductor technologies, software, e-commerce, cloud computing, social media, big data and other data intensive products and services.[56] But, this also resulted in hundreds of diverging and constantly evolving privacy laws across the United States. Companies and government agencies find it increasingly difficult to navigate the maze of US privacy laws. Businesses are particularly concerned about the California Consumer Privacy Act of 2018, which adds extensive new disclosure requirements and individual rights to existing laws in order to reign in perceived risks emanating from data selling.[57]

Calls have become louder for uniform federal privacy laws in the United States. Politicians, government authorities, activists, businesses and consumers agree in principle that broad federal legislation is warranted. Disagreements prevail, however, over important questions of detail, including whether a new federal law should preempt (that is: invalidate) or merely supplement existing state laws, and whether the United States should adopt European-style data processing regulations or continue the US tradition of individual privacy protections.

---

54 See for a recent overview Dixon and Determann (n 43).

55 Schwartz (n 17).

56 Anupam Chander, 'How Law Made Silicon Valley' (2014) 63 Emory Law Journal 639.

57 Determann (n 19) Ch 2–26a.

II Adequacy of EU Regulations of Data Processing

The EU hails its GDPR as the most modern data protection law worldwide and claims authority in Art. 45 GDPR to formally decide whether the level of data protection in other countries is adequate. At the same time, critics, including in the German government, are questioning whether the GDPR itself is truly adequate.[58] The European approach from the 1970s to broadly prohibit processing of personal data, subject to a limited number of exceptions, seems even more unrealistic and impractical today where information technologies are so developed and omnipresent. European calls to elevate privacy to a fundamental human right may be merely 'rights talk.'[59]

When some refer to the GDPR as the 'gold standard for privacy laws,'[60] it seems worth asking whether a gold standard is desirable in 2022 and preferable over modern monetary policy and crypto currencies. Granted, some may be happier with owning gold than with owning bitcoin in June 2022, after spectacular devaluations in recent days. Also, some may prefer to live in a world without computers and automated processing of personal data. Yet, the GDPR seems hardly more modern or progressive than the gold standard in the currency sphere. Both seem outdated and ill-suited to safeguard competing policy interests in modern economies and information societies.

The genie is out of the bottle. Data processing technologies are here to stay. Data collection, usage and sharing will increase, in fact: must increase, to better research and cure diseases; treat patients with personalized, precision medicine; develop artificial intelligence; enable autonomous cars to recognize and protect people; support global communications; create reliable block-chains; and protect national and international security. EU-style data minimization and prohibitive regulation is counter-productive to pursuing the many opportunities of data-driven innovation. Also, vast amounts of sensitive personal data on most people is already stored in numerous legitimate and illegal data bases around the world.[61]

European companies and governments are using – and will continue to use – very similar technologies, products and services as their US counterparts. Today, most information technologies, products and services are developed by industry leaders outside of Europe, but individual data subjects in Europe are exposed to

58 Veil (n 15).

59 Schwartz (n 17); Schwartz and Peifer (n 17).

60 Alessandro Mantelero, 'The Future of Data Protection: Gold Standard vs. Global Standard' (2020) Computer Law & Security Review.

61 Robert McMillan, 'Thieves Can Now Nab Your Data in a Few Minutes for a Few Bucks' *WSJ* (Washington DC, 10 December 2018).

the same privacy harms and concerns in the EU as elsewhere. Also, omnibus data protection laws that try to regulate everything[62] are unreasonably vague and difficult to update. It took the European Union more than 20 years to replace the Data Protection Directive with the GDPR effective 2018. Moreover, the Data Protection Directive of 1995 merely constituted a harmonized version of national data protection laws from the 1970s, before private television, the Internet, mobile phones, big data, cloud computing and other technologies arrived on the scene.

III Why Then Follow Europe?

Despite the obvious shortcomings of European data protection laws, more and more countries outside Europe have enacted similar laws. One reason are benefits for cross-border trade if the EU finds data protection laws of another country 'adequate'. The procedure contemplated by the Data Protection Directive and also in the GDPR has yielded somewhat surprising results: Since 1995, only Argentina, Canada, Israel, Japan, Korea, New Zealand, Uruguay and a few smaller countries have been found to have 'adequate levels of data protection'. Another reason is that the United States approach has become unmanageable in practice. In the 1970s, the United States shied away from enacting European-style general data protection laws for fear such laws could suffocate innovation and become too difficult to update and supplement as privacy threats evolve. Since then, the United States enacted and updated hundreds of threat- or sector-specific privacy laws, each narrowly crafted, but cumulatively suffocating in their own way. The California Consumer Privacy Act of 2018 (CCPA) imposes overly complex and detailed obligations on companies that are not compatible with requirements of other jurisdictions. Businesses can no longer navigate the maze. The United States need a reform centered around federal legislation.

But, perhaps the most important reason is that crafting tailored and balanced privacy laws is very difficult. Lawmakers find it relatively easy to craft data security and data protection legislation. Anyone can agree on what good *security* looks like: unauthorized persons do not have access to confidential information. Also, if one accepts with EU lawmakers that the processing of personal data is predominantly harmful and dangerous, then one can easily agree on data minimization and the various procedural and administrative requirements contained in the GDPR.

---

62 For a review of the GDPR as "the law of everything", see Dixon and Determann (n 44).

Crafting balanced and proportionate privacy laws focused on preventing harm while protecting free speech, information and innovation, however, is much more difficult. We do not all agree on what good *privacy* looks like. A defendant who demands that the police stay out of his home or computer obstructs criminal investigations or national security measures. A patient who objects to clinical trials or research prevents medical progress and cures. An employee who objects to workplace monitoring makes it harder for employers to prevent harassment and theft of trade secrets. A politician who demands a 'right to be forgotten' intrudes on freedoms of speech and information rights of other citizens.

Data subjects are not harmed by the processing of personal data as such. Concerns pertain to particular abuses of data processing, such as discrimination by employers, health insurance companies and law enforcement. But, it is difficult for policymakers to agree on the dividing lines between legitimate use and abuses. For example, some believe that insurance companies should be permitted to consider how healthy policy holders (people) live and offer discounts to non-smokers or based on exercise and eating habits to encourage lower risk behaviors. Others see an unfair penalty for smokers or overweight people and feel violated in their privacy if insurance companies monitor their exercise levels and consumption habits.

Moreover, it is difficult to enforce laws that are narrowly focused on prohibiting certain abuses. It is much easier to just prohibit the collection of personal data in the first place, so the data cannot be abused. But, this seems like an overkill. States do not prohibit cars to reduce car accidents either and instead enact differentiated traffic rules, even if they are harder to craft and enforce than a complete prohibition of cars. Similarly, we need differentiated rules focused on privacy harms, which need to be constantly updated as technologies and threats evolve.

Policymakers should focus on particular privacy harms and craft legislation that balances privacy and other interests proportionally. Legislatures should not continue with the European approach of broadly prohibiting or regulating the processing of personal data, because this has not led to effective privacy protections in Europe in the past and only prevented scientific and commercial progress in the information technology sector, which is now globally dominated by non-European companies. Data processing as such is not harmful to individuals, but necessary and largely beneficial. Lawmakers should encourage and enable secure data sharing and direct their efforts to enforce existing laws to prevent and pursue abuses such as cybercrime, fraud and harmful discrimination. If lawmakers enact broadly applicable general privacy laws to define baselines, they must be careful to prevent ossification and leave room for updates and upgrades as technologies and business practices evolve and new threats emerge.

E Conclusion and Outlook

The United States and other countries find themselves at crossroads with respect to data-related policies. The rigid regulatory and prohibitive approach in Europe has hindered the development of information technologies in Europe. The GDPR repeats and doubles down on regulatory concepts of the 1970s by broadly restricting data collection, retention, transfers and other processing. In the 2020s, this blunt vector hardly promises adequate answers for today's or tomorrow's data-related challenges. Countering harmful effects of restricting data sharing with an even more complex regime requiring data sharing under the EU Data Act proposal threatens further confusion and misdirection through inconsistent and incomprehensive vectoring.

Technology companies have fared better in the United States under narrowly crafted privacy laws, but evolving technologies and privacy threats have triggered so many specific laws that the legal environment has become unmanageably complex. Data privacy law reform should focus on actual harms and remain flexible to allow frequent updates and adjustments as technologies and threats evolve. Yet, California voters have decided in the 2020 general election by way of popular ballot measure to abandon the United States' historic approach of sector-, harm- and situation-specific privacy laws in favor of omnibus data processing regulation adopting elements found in the GDPR. The people have spoken.

Aside from being overbroad and overly complex, however, California privacy laws also contain novel and interestingly nuanced vectors: By requiring businesses to inform consumers specifically regarding the value of personal information in 'notices of financial incentives', providing detailed disclosures regarding information processing practices, and offering opt-out rights concerning selling and sharing of personal information, California has fortified existing consumer rights. Consequently, consumers may become able to better understand and exercise their rights and bargaining powers concerning personal information in online and offline market places. This should allow lawmakers to peel back other laws and regulations to positively and consistently shape policy-focused vectors for personal data disclosures in California and elsewhere.

More broadly, lawmakers should address data policy holistically within coherent and understandable legislative frameworks instead of unleashing confusingly complex and disparate vectors concerning data disclosures on businesses and individuals – as in the GDPR and the EU Data Act in Europe or in the United States in the HIPAA Privacy Rule and information blocking prohibitions in the U.S. Cures Act. Precisely aimed, modern vectors for thoughtful data disclosures as in the CCPA can be effective only if businesses and consumers are enabled to understand

and follow them. Lawmakers have to repeal, simplify and realign the thicket of existing data-related legislation in Europe and in the United States.

Normann Witzleb

Responding to Global Trends? Privacy Law Reform in Australia

A Introduction

This contribution explores the extent to which Australian privacy law reform in the early 2020s engages with, and is influenced by, global developments and trends. It has a particular focus on the major (and at the timing of writing ongoing) review of the Australian *Privacy Act 1998* and also considers the newly enacted *Data Availability and Transparency Act 2022.* The contribution demonstrates that Australia is committed to regulating the disclosure of personal data in a way that balances personal privacy and competing public interests. The review process seeks to modernize Australia's data protection regime and maintain its global interoperability in the digital era. In doing so, Australia's privacy laws are likely to maintain many of their distinctive characteristics that reflect Australia's cultural, economic and legal preferences.

Despite its antipodean location, Australia's legal system appears in many ways quite familiar to European observers. Australia follows the common law tradition,

Normann Witzleb is an Associate Professor at the Chinese University of Hong Kong, faculty of law, and maintains an adjunct position at the Monash University Australia, Melbourne, n.witzleb@cuhk.edu.hk.

https://doi.org/10.1515/9783111010601-009

it is a federal state and a modern liberal democracy. Although Australia's most important trading partners are in Asia and most of its recent migrants also hail from the region, its legal traditions remain still very much aligned with the West. Taking account of its regional connections, Australia has engaged with its Asian neighbors more readily and more extensively in recent decades than in previous times. Australia is a member of Asia-Pacific Economic Cooperation, an inter-governmental forum for 21 economies in the Pacific Rim that seek to promote free trade throughout the Asia-Pacific region. This membership also has importance for privacy protection because the APEC Privacy Framework of 2004 provides an important point of orientation for Australia's privacy regulation. However, as will be further discussed below, the global influence of the EU General Data Protection Regulation (GDPR)[1] can also be felt in Australia's current law reform debates.

B Human Rights Protection of Privacy

Australia has rarely been in the vanguard of protecting privacy interests, but equally it seeks to ensure that it does not stray too far off the mainstream. When describing a country's approach to privacy and data protection, especially to a European audience, it is convenient to start with the applicable human rights framework. The European Union has a rights-based approach to the protection of privacy and data protection, which is evident not least in the separate protection of both these rights in Articles 7 and 8 of the Charter of Fundamental Rights. This double anchoring is, of course, unique to the EU, and a world away from the position in Australia. Australia does not even have a bill of rights or similar human rights catalogue in its federal law. It still follows the traditional position that the common law provides sufficient protection of human rights. There are, however, now an increasing number of states and territories within Australia that do have human rights legislation,[2] although this has so far not had significant effect on privacy protection.[3]

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.

2 These are the Human Rights Act 2004 (ACT); Human Rights Act 2019 (Qld); Charter of Human Rights and Responsibilities Act 2006 (Vic).

3 Exceptions are cases such as Thompson v Minogue [2021] VSCA 358, in which routine strip searches of prisoners were held to be a breach of the right to privacy in s. 13(1) of the Victorian Charter of Human Rights and Responsibilities Act 2006.

The absence of a federal human rights charter does not mean, of course, that human rights are not protected in Australia. But it does make human rights protection more uncertain and the human rights discourse less explicit. Australia is a party to the International Covenant on Civil and Political Rights (ICCPR),[4] which protects against 'arbitrary or unlawful interference with [...] privacy, family, home or correspondence' in its Art. 17. It has also ratified a range of other UN treaties which protect the right to privacy for specific groups. This includes the Convention on the Rights of the Child[5] and the Convention on the Rights of Persons with Disabilities, both of which guarantee the right to privacy.[6] However, these international human rights protections are not directly applicable in Australian law. They have effect only to the extent to which they are implemented through domestic laws. These laws can be statutes, that is legislative enactments, or the common law, that is the solidified case law contained in decisions of Australian and other common law courts. While the High Court of Australia has held that statutory interpretation must 'favour construction [of legislation] which is in conformity and not in conflict with Australia's international obligations',[7] Australian courts do not acknowledge an overt influence of international human rights obligations on the Australian common law.

C Statutory Protections of Privacy

The most important statute protecting the right to privacy in Australia is the Commonwealth (or federal) Privacy Act 1988. The preamble of the Act makes explicit reference to Australia's obligations under the ICCPR and also declares the Act to be a response to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 (OECD Guidelines).[8] However, the name Privacy Act promises more than the Act in fact delivers. Instead of providing for the comprehensive protection of privacy, the Act merely protects information privacy inter-

4 International Covenant on Civil and Political Rights (1976) 999 UNTS 171.

5 UN Convention on the Rights of the Child (1990) 1577 UNTS 3.

6 UN Convention on the Rights of Persons with Disabilities and its Optional Protocol (2008) 2518 UNTS 283.

7 Minister for Immigration and Ethnic Affairs v Teoh (1995) 183 CLR 273, 287 (Mason CJ and Deane J); Plaintiff M70/2011 v Minister for Immigration and Citizenship (2011) 244 CLR 144, [2011] HCA 32, [247] (Kiefel J).

8 Organization for Economic Co-operation and Development (OECD), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, accompanied by an Explanatory Memorandum (1980).

ests. It would therefore be more accurate to describe it as a data protection statute, rather than a Privacy Act. The Act regulates how Australian Government agencies and certain private sector organizations should handle personal information.

Alongside the federal Act, there are a number of privacy statutes in the Australian states and territories. Like Germany, the Australian states have legislative powers in all areas that are not specifically transferred to, or reserved by, the federal level (called the Commonwealth of Australia, section 51 of the Australian Constitution). The majority of states and territories have their own data protection laws that are specifically directed at state government agencies[9] and, in some cases, also specialized health data laws.[10] Also important are a range of other statutory enactments that protect privacy interests from specific types of invasion, both at Commonwealth and state/territory levels. This includes the federal *Telecommunications (Interception and Access) Act 1979.* In addition, there are state and territory surveillance laws, which regulate the use of surveillance devices – and contain specific regulation for listening devices, optical devices, as well as location and computer tracking.[11]

D Common Law Protection

In line with the UK and other English-speaking countries, Australian law has never seen fit to recognize and protect privacy as a common law right. Part of the explanation for this may be that the concept of privacy is relatively abstract and elusive. It is notoriously difficult to define privacy and to explain its exact scope.[12] It is an umbrella term from which specific protections need to be developed by way of top-down reasoning, that means, from a broad concept to individual applications. This deductive approach is, in some ways, antithetical to the operation of the common

9 Information Privacy Act 2014 (ACT); Information Act 2002 (NT); Information Privacy Act 2009 (Qld); Privacy and Personal Information Protection Act 1998 (NSW); Personal Information Protection Act 2004 (Tas); Privacy and Data Protection Act 2014 (Vic).

10 Health Records and Information Privacy Act 2002 (NSW); Health Records Act 2001 (Vic).

11 Listening Devices Act 1992 (ACT); Surveillance Devices Act 2004 (Cth); Surveillance Devices Act 2007 (NSW); Surveillance Devices Act 2007 (NT); Invasion of Privacy Act 1971 (Qld); Surveillance Devices Act 2016 (SA); Listening Devices Act 1991 (Tas); Surveillance Devices Act 1998; Surveillance Devices Act 1998 (WA).

12 See eg, New Zealand Law Commission, *A conceptual approach to privacy* (Miscellaneous Paper, No 19, October 2007) ch 2.

law, which feel most comfortable when it operates from case-to-case, that is using bottom-up or inferential reasoning.[13]

However, despite this challenging starting point, many English-speaking jurisdictions have now improved their privacy protections at general law (ie, common law and equity). Often, it was human rights legislation that prompted an enhanced status of privacy also in private law. This applies most prominently to the United Kingdom, where the enactment of the *Human Rights Act 1998* triggered a revolution of common law rights protections of privacy. The UK initially provided privacy protection through an expansion of the equitable doctrine of breach of confidence.[14] However, the House of Lords soon found that it would be preferable to recognize a separate cause of action in tort law.[15] This new action has become known the tort of misuse of private information.[16] This tort has proven vital in the protection of privacy against the media, in interpersonal relations and many other areas. Other common law countries, such as Canada and New Zealand, have also developed stronger privacy protection through the recognition of specific privacy torts.[17] The courts in these countries were likewise able to take prompts from domestic human rights charters,[18] but were also influenced by the example of US tort law. This is apparent in the fact that they recognized, just as the US, two separate privacy torts – one for the wrongful disclosure of private information another for the wrongful intrusion into seclusion.

These developments, which occurred mostly over the last 20 years, now contrast strongly with the position in Australia. In 2001, the High Court of Australia declared in the decision of *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*,[19] that there was no obstacle to the common law recognizing a

13 See eg, Jeffrey J Rachlinski, 'Bottom-up versus Top-down Lawmaking' (2006) 73 The University of Chicago Law Review 933.

14 Douglas v Hello! Ltd [2000] EWCA Civ 353, [2001] QB 967.

15 Campbell v MGN Ltd [2004] UKHL 22, [2004] AC 457.

16 Douglas v Hello! Ltd (No. 3) [2005] EWCA Civ 595, [2006] QB 125; McKennitt v Ash [2006] EWCA Civ 1714, [2008] QB 73; Vidal-Hall v Google Inc [2015] EWCA Civ 311, [2016] QB 1003.

17 For further discussion, see Jeff Berryman, 'Remedies for Breach of Privacy in Canada' in Jason NE Varuhas and Nicole A Moreham (eds), *Remedies for Breach of Privacy* (Hart Publishing 2018) 323; Chris DL Hunt, 'New Zealand's New Privacy Tort in Comparative Perspective' (2013) 13 Oxford University Commonwealth Law Journal 157.

18 Significantly, neither the Canadian Charter of Rights and Freedoms nor the New Zealand Bill of Rights Act 1990 contain a broad right to respect for private life, as under European human rights law or the International Covenant on Civil and Political Rights (ICCPR). Instead, these instruments provide more limited protection against 'unreasonable search and seizure': Charter of Rights and Freedoms (Can) s 8; Bill of Rights Act 1990 (NZ) s 21.

19 [2001] HCA 63, (2001) 208 CLR 199.

right to privacy but no further steps have since been taken by Australian appellate courts. This position has been confirmed by the High Court as recently as 2020 in *Smethurst v Commissioner of Police.*[20] This puts Australia in a sort of holding pattern, where a privacy tort remains a possibility, but courts have not yet seen a need to recognize it. In the absence of a dedicated privacy tort, privacy interests remain protected only indirectly. Claimants need to rely on a patchwork of causes of action that apply in related areas and protect aspects of privacy incidentally. For example, the tort of defamation can be relied upon where privacy and reputational interests overlap. The tort of trespass to land protects territorial privacy,[21] the equitable doctrine of breach of confidence protects confidential information,[22] and various statutory rules such as copyright[23] and surveillance legislation[24] complete the jigsaw of incidental protection.

The adherence to this conservative position has had the consequence that Australia has over time become an outlier amongst the western common law jurisdictions. The Australian position now shares more commonalities with the law of Singapore,[25] Malaysia[26] and Hong Kong[27] – all of which have likewise not yet taken the step of protecting privacy interests through a dedicated privacy tort.

E The Privacy Act 1988

As mentioned above, the Australian Privacy Act 1988 is the key statute for the handling of personal information. Initially, its scope was limited to Australian federal government agencies. In 2000, it was expanded to cover the private sector,[28] but the Act contains a wide range of exemptions. The most important of these carve outs is the so-called small business exemption which applies to companies with a turn-

20 [2020] HCA 14, (2020) 376 ALR 575.

21 See eg, TCN Channel Nine Pty Ltd v Anning [2002] NSWCA 82, (2002) 54 NSWLR 333.

22 Agha v Devine Real Estate Concord Pty Ltd [2021] NSWCA 29.

23 Copyright Act 1968.

24 See n 11.

25 ANB v ANC [2015] SGCA 43, [2015] 5 SLR 522. See further Singapore Academy of Law's Law Reform Committee, *Civil Liability for Misuse of Private Information* (Report, 2020).

26 Lee Ewe Poh v Dr Lim Teik Man [2011] 4 CLJ 397; See further Usharani Balasingam and Saifullah Qamar Bin Siddique Bhatti, 'Between Lex Lata and Lex Ferenda: An Evaluation of the Extent of the Right to Privacy in Malaysia' (2017) 4 Malayan Law Journal 29.

27 Sim Kon Fah v JBPB & Co [2011] 4 HKLRD 45; See further Yun CJ Mo and AKC Koo, 'A Bolder Step towards Privacy Protection in Hong Kong: A Statutory Cause of Action' (2015) 9 Asian Journal of Comparative Law 345.

28 Privacy Amendment (Private Sector) Act 2000.

over of less than $3 million Australian dollars (which is the equivalent of 2 million €).[29] This exemption, which was introduced to minimize compliance cost for small business operators, has the effect that about 95% of Australian companies do not need to comply with the Act.[30] Other exemptions concern employee records[31] and journalism,[32] as well as registered political parties[33] and political acts and practices.[34] These exemptions significantly reduce the scope of application of the Privacy Act. However, the justifications of these exemptions have increasingly been put into question[35] – not least because comparable countries do not make use of similar carve outs. For example, the political exemption, which has the effect that Australia's political parties as well other political actors do not need to comply with privacy principles, was initially justified with the consideration that it would help with implied freedom of political communication. However, in more recent times it has become apparent that unrestricted data practices of political actors can themselves pose danger to political discourse and democratic decision-making.[36] A particularly problematic aspect of the exemptions is that these actors cannot be held legally accountable for their data processing practices, and that Australian citizens have very little insight into what happens with personal data in the political process.[37]

Following a comprehensive review of Australian privacy laws in 2008 by the Australian Law Reform Commission,[38] the Privacy Act was amended in 2012.[39] Among the important changes was the amalgamation of two previously distinct sets of privacy principles that applied to the public and private sectors, respectively. Now, a single set of so-called Australian Privacy Principles (APPs) applies in

29 Privacy Act 1988 ss 6C, 6D.

30 Australian Government, Office of the Australian Information Commissioner, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner* (2020) [4.11].

31 Privacy Act 1988 s 7B(3).

32 Privacy Act 1988 s 7B(4).

33 Privacy Act 1988 s 6C.

34 Privacy Act 1988 s 7C.

35 Australian Government, Attorney-General's Department, *Review of the Privacy Act – Discussion Paper* (2021) chs 4–7.

36 Information Commissioner's Office (UK), *Democracy disrupted? Personal information and political influence* (2018).

37 Normann Witzleb and Moira Paterson, 'Voter privacy in an era of big data: Time to abolish the political exemption in the Australian Privacy Act' in Normann Witzleb, Moira Paterson and Janice Richardson (eds), *Big Data, Political Campaigning and the Law: Privacy and Democracy in the Age of Micro-Targeting* (Routledge 2020) 164.

38 Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice (ALRC Report 108, 2008).

39 Privacy Amendment (Enhancing Privacy Protection) Act 2012.

largely identical form to all entities covered by the Privacy Act.[40] These APPs govern the collection, use, disclosure and storage of personal and sensitive information and how individuals may access and correct records containing such information. The principles differ from those in the GDPR in several key respects, as will be explained below. Similar to the GDPR and other data protection laws, the Privacy Act only applies to 'personal information'.[41] The current definition of 'personal information' was inserted into the Privacy Act in 2012. The definition states: information or an 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 a material form or not.

There has been some controversy around the word 'about' in this definition, which differs from 'relating to' in the GDPR. In a 2017 decision, the Full Court of the Federal Court confirmed a tribunal decision which had held that 'about' means that the information needs to have some biographical relevance for the individual concerned.[42] This has raised doubt as to whether the definition also applies to more technical information, such as device identifiers, IP addresses or location data.[43] Such information is potentially linked to an individual, but only has a tenuous connection to a person's life.

Australia also provides stricter protections for certain categories of information that are regarded as particularly sensitive. This might be seen as slightly surprising given that Australia, as other common law countries, based its data protection laws on the OECD Guidelines, which recognize the issue of sensitive data without, however, adopting that concept.[44] In a similar vein, the APEC Privacy Framework also does not single out specific categories of personal data as having a 'sensitive' quality and as such meriting extra legal protection.[45] Yet, in the Australian context, the appeal of the predominantly European idea of giving certain categories of data more protection has won the day. It seems ultimately to have outweighed concerns about the potential divergence with other common law regimes in the region, such as Canada and New Zealand, which do not recognize the 'sen-

40 Privacy Act 1988 Sch 1.

41 Privacy Act 1988 s 6.

42 Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4, (2017) 249 FCR 24.

43 Joshua Yuvaraj, 'How About Me? The Scope of Personal Information under the Australian Privacy Act 1988' (2018) 34 Computer Law and Security Review 47; Julian Wagner and Normann Witzleb, 'Personal Information' in the Australian Privacy Act and the Classification of IP Addresses' (2017) 3 European Data Protection Law Review 528.

44 Ibid, [1].

45 Asia-Pacific Economic Cooperation (APEC), Privacy Framework (2015).

sitive information' categories but adopt a more contextual approach.[46] The Privacy Act largely mirrors the EU's special data categories, although the additional protections available to such data are more restricted than under the GDPR.

F The Review of the Privacy Act

For the last two years, Australia has been engaged in another review of its Privacy Act.[47] The fact that Australia's privacy rules have not been subject to major review and reform for more than a decade is beginning to show because technology and commercial practices have developed significantly since then. A central objective of the reforms is to respond to the rise of digital platforms, big data analytics, and the increasing reliance on AI. There is growing recognition that the current Australian rules do not sufficiently protect digital privacy in a data-driven world and that they are increasingly falling short of community expectations.[48] Concerns arise in several areas, including in relation to the definition of personal information, the notice and consent requirements, the protection of children's personal data, and the strength of enforcement rights. Each of these will be discussed below, but space does not permit consideration of the protection against inferences, the use of automated decision-making, the right of erasure and other issues.

One of the triggers for the review was the recommendations to reform privacy laws made by the Australian Competition and Consumer Commission (ACCC). The ACCC, which is the regulator of market conduct, engaged in a very comprehensive and influential review of Digital Platforms from 2017–2019.[49] The ACCC Inquiry examined the transformative impact of digital platforms on the news media and advertising sector. Data protection and privacy laws were just one aspect of a broad-ranging inquiry that also included competition law, media law and consumer protection law.

---

46 Damian Clifford, Megan Richardson and Normann Witzleb, 'Artificial intelligence and sensitive inferences: new challenges for data protection laws' in Mark Findlay and others (eds), *Regulatory Insights on Artificial Intelligence: Research for Policy* (Edward Elgar, 2022) 19.

47 Attorney-General's Department, *Privacy Act Review: Issues Paper* (October 2020) and Attorney-General's Department (n 35). At the time of writing the Attorney-General's Department's Final Report was completed but yet unpublished.

48 Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* (2020).

49 Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, 2019).

One recommendation in the Final Report of the Inquiry that made international headlines was the suggestion for a news media bargaining code, which obliged the very large digital platforms that operate in Australia to pay local news publishers for the news content they made available through links on their platforms. This recommendation was accepted by the Government but strongly resisted by social media platforms, which feared that mandatory payments to news organizations might provide a model for similar laws in other countries. The code has eventually gone ahead, although it was somewhat watered down, and gives news publishers, including some public interest publishers, now some extra income which is taken from the profits made by the likes of Facebook and Google. This code is noteworthy for two reasons. The first is that it is one of the relatively rare examples where an Australian Government was prepared to take an internationally leading role in digital information regulation. The second reason is to show that, when the Australian Government chooses its battles wisely, it can succeed with its regulatory aims, even against the largest multinational corporations. Australia, although economically a smaller jurisdiction, is not condemned to be a follower.[50]

A second important reform process in recent times included the Australian Human Rights Commission's inquiry into Human Rights and Technology.[51] The remit of this inquiry also went beyond data protection, because it examined the impact of new technologies such as AI across the field of human rights. The Commission made proposals for responsible AI regulation, including addressing the use of biometric information and surveillance technologies. In particular, the Report recommended proactive protections of human rights in the development and use of these technologies, including the introduction of a right to privacy and a moratorium on the use of biometric technologies in high-risk decision making until proper regulation is in place.

These two reports have confirmed that Australia's privacy laws need to be reformed to respond appropriately to new technologies. The GDPR is widely regarded as the gold standard for data protection in many parts of the world,[52] going much beyond Europe itself. The 'Brussels effect' on the data practices of multinational

50 Another example is the 'plain-packaging laws', which required all tobacco products to be sold in standardized packaging that does not allow for any logos or promotional texts: Suzanne Zhou and Melanie Wakefield, 'A Global Public Health Victory for Tobacco Plain-Packaging Laws in Australia' (2019) 179 JAMA International Medicine 137.

51 Australian Human Rights Commission, *Human Rights and Technology* (Final Report, 2021).

52 See eg, Alessandro Mantelero, 'The future of data protection: Gold standard vs. global standard' (2021) 40 Computer Law & Security Review 105500, https://doi.org/10.1016/j.clsr.2020.105500. Critical: Lothar Determann, 'California Privacy Law Vectors for Data Disclosures', in this volume, at 121, 141 et seqq.

corporations has been well documented.[53] For these companies, it makes economic sense to adopt a single set of rules – and often they prefer to follow the rules set in Brussels for all their operations worldwide, rather than differing rules in different markets.[54] But apart from setting *de facto* standards for data processors, the GDPR also influences law-making in some countries. Some countries choose to align themselves closely with EU data protection framework because they desire to achieve adequacy status under the EU rules. However, that is a significant driver only for a relatively small number of countries.[55]

Unlike its regional neighbors New Zealand, South Korea or Japan, Australia has never applied for an adequacy decision. The wide exemptions in the Privacy Act have previously been identified as the main obstacle to obtaining an EU adequacy decision.[56] But even for countries that do not seek alignment with EU rules, the GDPR provides a benchmark for comparison. Throughout the recent Australian debate on updating the privacy framework, the GDPR has remained a constant reference point in the discussion. In other words, the 'Brussels effect' can be felt in Australia, too. However, even Australia's privacy regulator, the Office of the Australian Information Commissioner (OAIC) is not explicitly advocating for reforms that would guarantee to achieve adequacy under EU rules. Instead, it considers 'interoperability' of the Act with overseas privacy regimes overseas, including the GDPR, to be the more important objective and is content to leave the decision on whether to seek adequacy in the hands of the Australian Government.[57]

G Key Aspects of the Proposed Privacy Reforms

This section will consider and evaluate some of the key issues addressed in the reform. However, given that the Final Report of the current inquiry is still unpublish-

53 See generally Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020).

54 Lee A Bygrave, 'The "Strasbourg Effect" on data protection in light of the "Brussels Effect": Logic, mechanics and prospects' (2021) 40 Computer Law & Security Review 105460, https://doi.org/10.1016/j.clsr.2020.105460.

55 The EU has so far recognized Andorra, Argentina, Canada (in relation to commercial organizations), Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom under the GDPR and the Law Enforcement Directive, and Uruguay as providing adequate protection.

56 Article 29 Data Protection Working Party, Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000.

57 See discussion in Office of the Australian Information Commissioner (n 30) [8.35]–[8.40].

ed at the time of writing, the Government has yet to reveal its preferred approach on many issues and comments on the likely future shape of the laws are necessarily preliminary. Nonetheless, it is worthwhile to provide an overview of some of the identified issues and the degree to which Australia engages with international approaches on these matters.

I Definition of Personal Information

As mentioned above, the Australian definition of personal information is seen as slightly narrow at present. The proposals are to broaden the definition along the lines of the GDPR and, in line with international models, to replace the word 'about' with 'relating to'. This would clarify that non-biographical information relating to a person is included in the definition. It is also likely that the revised definition will clarify that 'inferred information' can be personal information. There is also significant stakeholder support to make individuation, rather than identifiability, of a person the touchstone of protection.[58] This is because many modern forms of profiling, such as behavioral advertising, do now operate without knowledge of a person's identity. These processes are based on a person's attributes (such as their income, marital status, residential suburb), rather than their identity, and draw inferences from these attributes to arrive at their interests, preferences and susceptibility to certain messages. A person may therefore suffer privacy harm in the form of loss of autonomy, manipulation, unwelcome targeting or discrimination, even if their identity is unknown throughout the process. While the GDPR also still links personal data to identification or identifiability,[59] it is arguably more alert to the digital harms that can arise when a person is 'singled out' on the basis of their personal characteristics.[60] More recent regimes such as that of California are moving beyond that,[61] because they also capture information that can be associated with a particular individual, whether they are identifiable or not. It is therefore to be welcomed that the Discussion Paper for the Privacy Act Review proposes that the updated definition would cover 'circumstances in

58 See Attorney-General's Department (n 35) 22–23; see further Anna Johnston, 'Individuation: re-imagining data privacy laws to protect against digital harms' (2020) Brussels Privacy Hub, Working Paper No 6.24 <https://brusselsprivacyhub.eu/publications/wp624.html> accessed 07.02.2023.

59 GDPR (n 1) Art. 4.

60 See eg ibid rec 26.

61 Californian Consumer Privacy Act 2018, s 1798.140(o)(1): 'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.'.

which an individual is distinguished from others or has a profile associated with a pseudonym or identifier, despite not being named'.[62]

II Strengthening Notice and Consent

In its present form, the Privacy Act gives significant room to data processors to seek consent through bundled, opaque and implicit processes that manipulate or undermine consumer choice. Many consumers do not read privacy notices and, if they read them, do not understand them. The Digital Platforms Inquiry suggested a range of measures to strengthen notice and consent, such as multi-layered and standardized notice and consent processes, as well as pro-consumer defaults.[63] These were intended to make the giving and withholding of consent easier and to ensure that the consumers are better informed when making their privacy choices. However, critics argue correctly that there are fundamental problems with the notice-and-consent model.[64] This is because of the well-established concerns that consumers are at a structural disadvantage when confronted with the myriad of privacy notices, including 'cognitive bias, bounded rationality and limits in time and experience in reading terms with legal import'.[65] Moreover, even if notices were read and understood, voluntary consent is in many cases illusory because data subjects are often not free to choose: if they want to access a particular service or are in a relationship of dependency, they need to accept the terms and conditions even if the proposed data practices contradict their preferences.[66] The GDPR does better in this area, including by having stricter notice and consent requirements. For example, it requires that employers generally need to find a basis for data collection and processing other than consent since employment causes

62 Attorney-General's Department (n 35) 27.

63 Australian Competition and Consumer Commission (n 49) rec 16.

64 See eg Damian Clifford and Jeannie Paterson, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law' (2020) 94 Australian Law Journal 741; for a comparative perspective, see Leon Trakman, Robert Walters and Bruno Zeller, 'Digital consent and data protection law – Europe and Asia-Pacific experience' (2020) 29 Information & Communications Technology Law 218.

65 Clifford and Paterson (ibid) 747.

66 The APP Guidelines state that consent will be voluntary if an individual 'is given a genuine opportunity to provide or withhold consent': Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines [B.43]. The requirements of consent, such as its voluntariness and whether it can be implied have been interpreted more strictly in recent determinations: Flight Centre Travel Group (Privacy) [2020] AICmr 57; Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54.

power imbalances that stand in the way of providing 'free' consent.[67] It is likely that the Australian reforms will reduce the scope for notice-and-consent as a justification for data collection and processing, and adopt more restrictions or even outright bans on some practices that are likely to cause harm to consumer interests.[68] During the consultations, it became apparent that there is also significant support for a general requirement to handle personal information in a fair and reasonable manner,[69] which already exists in the data protection laws of New Zealand[70] and Canada.[71] At this stage, it remains an open question whether the Government will press ahead with its intention to impose stricter requirements on social media platforms, which it proposed should be embedded in a binding Digital Platforms Privacy Code.

III Better Protection of Children's Privacy

Another area in which international developments are highly influential in the Australian debate are the data rights of children. The *Privacy Act 1988* currently contains no specific provisions regulating the privacy of children or young people and offers no additional protections to them.

As a result, where data processing requires consent, the ordinary principles relating to consent, and the capacity to give consent, apply.[72] If a child provides consent, this consent is valid only if the child has the requisite capacity to consent to the data processing in question. Capacity requires that the child has sufficient understanding and maturity to understand what is being proposed.[73] Currently, the OAIC's Australian Privacy Principles Guidelines suggest that, if it is not practicable or reasonable for an APP entity to assess a child's capacity on a case-by-case basis, the entity may rely on two presumptions: first, that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise; and

67 European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (2018) [21]–[22].

68 The Government has also proposed a binding Digital Platforms Privacy Code that would impose stricter requirements on social media platforms.

69 Attorney-General's Department (n 35) 85.

70 Privacy Act 2020 (NZ) s 22 (Information Privacy Principles 4 (b) (i), 10 (1) (d) and 11 (10 (d)).

71 Under Personal Information Protection and Electronic Documents Act 2000 (Can) s 3, an organization 'may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances'.

72 In Victoria, Privacy and Data Protection Act 2014 (Vic) s 28 contains detailed provisions on capacity to consent and the giving of consent by a representative.

73 APP Guidelines (n 66) B52.

second, that a child under 15 does not have capacity to consent.[74] But there is very little evidence to suggest to what extent these rules are actually observed in practice.

The Government has announced its intention to strengthen the online privacy protections of children and other vulnerable persons,[75] and the ACCC made several specific recommendations to this effect in its 2019 Digital Platforms report. The proposed rules would borrow substantially from the existing regimes in the US, under the Children Online Privacy Protection Rule (COPPA), as well as from the GDPR. A particular influential model is the Age-Appropriate Design Code of the Information Commissioner's Office in the UK (and similar provisions in Ireland) that puts the interests of child users at the center of the design process. Central elements of the Australian proposals are the prohibition of certain harmful practices through so-called 'no-go zones'.[76] This name was first coined in the Canadian context to describe practices that are altogether forbidden or allowed only in limited circumstances,[77] because they are reasonably considered to be inappropriate. In addition, again following the Canadian example, the Australian Government proposals consider introducing an overarching requirement that the collection, use or disclosure of personal data of children must be considered to be in the best interests of the child.[78]

IV A Direct Right of Action

With regard to enforcement, the review is proposing an array of measures to give the OAIC more powers of investigation and sanctioning. In addition, the Government proposes the introduction of a general right of action for interferences with privacy, which would enable direct judicial enforcement action by aggrieved individuals. Currently, the Privacy Act operates primarily as a complaints-based regime.[79] Where a person considers that their personal data has been mishandled, they are generally expected to approach the data processor first and, if no direct

74 Ibid B58.

75 Australian Government, Attorney-General's Department, *Tougher penalties to keep Australians safe online* (Media Release, 2019).

76 Attorney-General's Department (n 35) ch 11.

77 See Office of the Privacy Commissioner of Canada, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* (2018).

78 Attorney-General's Department (n 35) ch 13.

79 Privacy Act 1998 s 36.

resolution is reached, they can complain to the Privacy Commissioner.[80] The Privacy Commissioner may investigate into the breach and will dismiss complaints she considers unfounded.[81] If a complaint is substantiated, it is mostly resolved through a non-public conciliation process.[82]

The enforcement powers of the federal Privacy Commissioner,[83] as well as her counterparts in NSW and Vic,[84] include a power to declare that compensation must be paid to a complainant for loss or damage suffered as a result of a privacy interference.[85] Furthermore, tribunals can award compensation in administrative review proceedings.[86]

However, there have been only a small number of determinations[87] and even fewer legal proceedings initiated by the OAIC.[88] In response to the scarcity of its enforcement resources, the 'preferred regulatory approach of the OAIC is to work with entities to facilitate legal and best practice compliance'.[89] Commentators

80 Privacy Act 1998 s 40(1A).

81 Privacy Act 1998 s 41.

82 Australian Privacy Foundation, *Bringing Australia's Privacy Act up to international standards: Submission in response to the Privacy Act Review- Issues Paper* (2020) 33.

83 Privacy Act 1988 s 52; See Normann Witzleb, 'Determinations under the Privacy Act 1988 (Cth) as a Privacy Remedy' in Jason NE Varuhas and Nicole A Moreham (eds), *Remedies for Breach of Privacy* (Hart Publishing 2018) 377.

84 The Privacy and Personal Information Protection Act 1998 (NSW) expressly provides that its provisions do not give rise to any civil cause of action: s 69. However, in administrative review proceedings, the tribunals can award compensation and other relief: Privacy and Personal Information Protection Act 1998 (NSW) s 55 – compensation is capped at AU$40,000: s 55(2)(a). Similar provisions exist under the Privacy and Data Protection Act 2014 (Vic): see s 7 and 78 (compensation cap of AU$100,000, with specific acknowledgment that damages for injury to feelings and humiliation can be awarded).

85 Determinations with compensation awards include: 'EQ' and Great Barrier Reef Marine Authority [2015] AICmr 11; 'D' and Wentworthville Leagues Club [2011] AICmr 9; 'DK' and Telstra Corporation Limited [2014] AICmr 118.

86 The New South Wales Civil and Administrative Appeals Tribunal awarded compensation for breach of the Privacy and Personal Information Protection Act 1998 (NSW) on several occasions, including: CJU v SafeWork NSW [2018] NSWCATAD 300; ALZ v SafeWork (NSW) (No 4) [2017] NSWCATAD 1; and AOZ v Rail Corporation NSW (No 2) [2015] NSWCATAP 179.

87 The determinations are available from the OAIC website <https://www.oaic.gov.au/privacy/privacy-decisions/privacy-determinations> accessed 07.02.2023.

88 The most prominent of the latter is Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4, (2017) 249 FCR 24; but see also Australian Information Commissioner v Facebook Inc (No 2) [2020] FCA 1307 (civil penalty proceedings).

89 Office of the Australian Information Commissioner, 'Privacy regulatory action policy' (2018) [23] <https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy#approach-to-using-privacy-regulatory-powers> accessed 07.02.2023.

point out that giving the courts a greater role in enforcement action would raise the standards of protection and provide greater clarity of statutory requirements in the context of decided cases.[90]

The introduction of a direct right to action for privacy interferences has been recommended by the ACCC in its report on the Digital Platforms Inquiry.[91] After submitter were predominantly in favor of such a right, the ACCC recommended to give individuals and representative classes of individuals the right to seek compensatory damages, including aggravated damages, for the financial and non-financial harm resulting from breaches of the Privacy Act as well as, in exceptional circumstances, exemplary damages.

The various rationales put forward in favor of this recommendation correlate to the perceived weakness of the current enforcement model. The complaints-based enforcement model has long been criticized by stakeholders,[92] because the Australian Privacy Commissioner has had limited enforcement powers and been under-resourced for its multiple functions. In light of the current experience, the ACCC expected that a right of action would not only empower consumers, but also strengthen compliance with the Privacy Act.[93]

The Government has adopted the recommendation for a direct right of action. The Discussion Paper draws mainly on domestic models for the thresholds and modalities that should accompany such a right, such as similar rights under other regulatory regimes. However, submitters also made extensive reference to such rights in other jurisdictions, including the GDPR – generally to argue for a regime that is wider in its coverage and more accessible to individuals.

V A Statutory Privacy Tort

As mentioned above, it is a long-standing issue in Australia whether a privacy tort should be introduced.[94] Law reform bodies have uniformly and for many years an-

90 See submissions to Attorney-General's Department (n 35) 186.

91 Australian Competition and Consumer Commission (n 49) rec 16(e).

92 Australian Privacy Foundation, *Bringing Australia's Privacy Act up to International Standards: Australian Privacy Foundation Submission in Response to the Privacy Act Review: Issues Paper* (2020).

93 Australian Competition and Consumer Commission (n 49) 473.

94 See further Normann Witzleb, 'Another Push for an Australian Privacy Tort: Context, Evaluation and Prospects' (2020) 94 Australian Law Journal 765.

swered this question in the affirmative[95] – but the Government has so far hesitated. A privacy tort is once again on the legislative agenda, due to the recommendations by the ACCC as well as the AHRC in the reports mentioned earlier.[96] The ACCC reasoned that a statutory privacy tort would 'lessen the bargaining power imbalance between consumers and entities collecting their personal information, including digital platforms' and provide a deterrent and remedy against 'harmful data practices'.[97] But the proposed tort is not restricted to digital platforms or data misuses and would extend to all types of privacy invasion, including by the media. It would go beyond the Privacy Act, where acts and practices 'in the course of journalism'[98] currently enjoy a broad exemption from compliance with Australian data protection standards.

Unfortunately, the Government Discussion Paper for the Privacy Act Review presented once again only reform options, without expressing a concluded position on whether a statutory cause of action should be introduced.[99] Legislative progress has so far always been hampered by the strong resistance of the media, which (I submit, wrongly) believe that the current uncertain state of the law is preferable over a privacy tort that is the result of careful deliberation and extensive consultation during numerous past inquiries. This is certainly an area where trends in comparative common law jurisdictions point strongly towards reform, yet it remains to be seen whether the overwhelming evidence of strong community support in favor of increased protection is sufficient to overcome government inertia.

95 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report, No 108, 2008); New South Wales Law Reform Commission, *Invasion of Privacy* (Report, No 120, 2009); Victorian Law Reform Commission, *Surveillance in Public Places* (Final Report, No 18, 2010); South Australian Law Reform Institute, *Too Much Information: A Statutory Cause of Action for Invasion of Privacy* (Final Report, No 4, 2016); NSW Legislative Council Standing Committee on Law and Justice, *Remedies for the Serious Invasion of Privacy in New South Wales* (Report, No 57, 2016).

96 Australian Competition and Consumer Commission (n 49) rec 19; Australian Human Rights Commission (n 51) rec 21.

97 Australian Competition and Consumer Commission (n 49) 493.

98 Privacy Act 1998 s 7B(4).

99 Attorney-General's Department (n 35) ch 26.

H The Data Availability and Transparency Act 2022

Another important piece of legislation relevant to data disclosures is the new *Data Availability and Transparency Act 2022*. This legislation was first proposed in the 2017 Report into *Data Availability and Use* by the Australian Productivity Commission.[100] The Act is intended to facilitate better use of public sector data and to encourage innovation, while maintaining trust in the Government's use of public sector data.

The Act creates a new data sharing scheme that allows Commonwealth bodies, so-called 'data custodians',[101] to share public sector data with 'accredited users'.[102] These authorized users are other Australian state and federal government bodies and Australian public universities, but do not include the private sector or foreign entities. Data can only be shared for specified public purposes, namely the delivery of government services, to inform government policies and programs, and for research and development.[103] Enforcement-related purposes are specifically excluded.[104]

Data sharing must be consistent with the Act's data sharing principles[105] and occur pursuant to a registered data sharing agreement.[106] The data sharing principles identify 'project', 'people', 'setting', 'data' and 'output' as relevant parameters for assessing data sharing requests and for managing relevant risks.

Public sector data is defined as data that is lawfully collected, created or held by or on behalf of a Commonwealth body.[107] It includes personal data, although such data can only be shared if additional privacy protections are observed. Several purpose-specific privacy protections restrict the Government's ability to share personal information.[108] In addition, several general privacy protection obligations need to be adhered to.[109] These include that biometric data can only be shared with the consent of the individual. Furthermore, shared data containing

100 Australian Government, Productivity Commission, *Data Availability and Use* (Report, No 82, 2017).
101 See definition in Data Availability and Transparency Act 2022 s 11(2).
102 For details, see Data Availability and Transparency Act 2022 s 11(2).
103 Data Availability and Transparency Act 2022 s 15(1).
104 Data Availability and Transparency Act 2022 s 15(2).
105 Data Availability and Transparency Act 2022 s 16.
106 Data Availability and Transparency Act 2022 Part 2.6.
107 Data Availability and Transparency Act 2022 s 9.
108 Data Availability and Transparency Act 2022 s 16B.
109 Data Availability and Transparency Act 2022 s 16A.

personal information must not be stored, or provided access to, outside Australia. Lastly, if data that has been de-identified is shared, the data sharing agreement must prohibit the recipient from re-identifying the data.

The obligations on data custodians in other legislation, including the *Privacy Act*, need to be considered in the assessment of data sharing requests. However, once data sharing under the *Data Availability and Transparency Act 2022* is permissible and authorized, this authorization also fulfils the relevant authorization requirements for the collection, use and disclosure of personal information under the Australian Privacy Principles.

The Act also establishes the National Data Commissioner and the National Data Advisory Council. The Commissioner oversees the data sharing scheme, including advising on and enforcing it. The Commissioner has the power to make data codes, which data custodians and accredited entities must comply with.

The scheme has the potential to streamline the provision of Government services, which at present is sometimes hampered by the lack of access to relevant data. Whether it achieves its potential for more efficient service delivery will depend on the workability of the Act and the Data Commissioner's template data sharing agreement, as well as the level of trust into the scheme that relevant parties gain. At present, it is not yet clear whether the rules and codes around data sharing will impose the appropriate level of restrictions on custodians and accredited entities in a way that balances measures to curb the potential for misuse or loss of data with the value of the data being shared.

I Lesson from Privacy during the Pandemic

Lastly, it is also important to reflect on Australia's experience with privacy regulation during the pandemic. As is well-known, Australia went its own way during the pandemic adopting a strategy of suppressing the SARS-Co-V-2 virus as far as possible, including through tough border measures.[110] Some parts of the country endured long and strict lockdowns during which public and private life was largely limited to the digital. Australia was also a frontrunner of using electronic means to facilitate contact tracing. It was an early adopter of an electronic tracking app, called COVIDSafe, which relied on proximity tracing. The Government made use of the app voluntary but opted for uploaded data to be stored centrally. In response to community concern over the safe handling of data, the Government created a

110 Anika Stobart and Stephen Duckett, 'Australia's Response to COVID-19' (2022) 17 Health Economics, Policy and Law 95.

stand-alone regime for data collected by the app to maximize download and use of the app.

The COVIDSafe app 'failed'[111] to deliver on its public health objectives because it did not contribute significantly to contact tracing. Nonetheless, it is fair to say that the Australian Government made significant efforts to insulate the data management of the COVIDSafe app from nationwide schemes in the past. Some of these earlier schemes, including the Australia Card and the MyHealth record, suffered from low public confidence and had to be abandoned or were less successful than had been hoped. In contrast, the Government was more attentive to privacy protections in relation to the COVIDSafe app. Positive features included not only the voluntary character of the app, but also measures to prevent indirect coercion to use the app, the limitation of law enforcement access and the inclusion of a right of erasure.

The data protection framework of the European Union was sufficiently developed and flexible to accommodate the unprecedented challenges arising from COVID-19. Australia, however, needed to introduce a standalone legal framework dealing with COVIDSafe contact data because of some evident weaknesses in the existing framework under the Privacy Act.[112] They concern the adequacy of consent requirements, use limitations and the rights to erasure and deletion, data localization rules as well as more broadly the interplay between privacy and other human rights.

However, the lasting legacy of the COVIDSafe app is likely to be that it generated a national conversation around privacy and data practices. Data protection now has greater status in Australia. There is increasing recognition that data protection drives innovation and adoption of modern applications, rather than impedes it.[113] It has become apparent that trust in digital technologies can be undermined when data practices come across as opaque, creepy or unsafe.

The example of the COVIDSafe app shows that robust privacy protections are necessary to achieve a strong uptake of new technologies by the community. There are grounds to assume that Australian society now expects that the Government heeds these lessons more widely, especially in the current review of the general data protection framework contained in the Privacy Act.

---

111 Australian Senate, *Select Committee on COVID-19* (Final Report 2022) [4.113].

112 See further Normann Witzleb and Moira Paterson, 'The Australian COVIDSafe App and Privacy: Lessons for the Future of Australian Privacy Regulation' in Belinda Bennett and Ian Freckelton (eds), *Pandemics, Public Health Emergencies and Government Powers: Perspectives on Australian Law* (The Federation Press 2021) 160.

113 Macmillan Keck, Seharish Gillani and others, 'The role of data protection in the digital economy' (UNCDF Policy Accelerator, 2021).

J Reflections and Conclusion

Australia has an interesting position between the two western trading blocs (Europe and the US) on many issues of data regulation and privacy protection. It is neither aligned with the relative strict approach in the European Union, nor to the more permissive approach in the United States. While Australia has many cultural affinities to Europe, in particular to the United Kingdom, it does not share the human rights culture that underpins data protection regulation in the EU and Europe more widely. At the same time, Australia also does not share the long-held American belief into the superiority and strength of market-based solutions. It has relatively strong general consumer protection laws, but its data protection framework has always trailed behind, both in its substance and its enforcement.

Privacy protection continues to rely on an assemblage of common law and statutory rights, in which new dangers to individual rights are responded to with some delay. Corporate interests in minimizing regulation, be it those of the media or those of small business, have been allowed to influence the shape and strength of the laws. However, there are promising indications that there is now an appetite for stricter regulation. Consumer trust into the data practices of large digital platforms has been steadily eroded, and the pandemic has further reinforced the need for strong protections given society's increasing dependency on data-driven practices.

Australia engages with global trends but usually forges its own path that could be described as middle-of-the-road. The outcome of the current reform process is still unclear, not least because Australia's new federal Government has (at the time of writing) yet to outline its legislative agenda in this field. However, it is likely that the laws will bring evolutionary, rather than dramatic, change and pursue the purpose of making Australia's data protection framework fit for the 2020s. The influence of the European framework is clear, but the GDPR is understood, and referred to, as a benchmark rather than a model. Australia has a long-standing preference for creating laws that are interoperable with international regulatory frameworks, rather than to strive for adequacy with the EU model.

In some ways, the *Data Availability and Transparency Act 2022* is a good example of the direction that Australia likes to take. It is a modern data sharing framework that seeks to create value and efficiencies, that enables innovation and protects trust through granting adequate protections.

Daniela Wawra

Data Sensitivity and Data Protection Literacy in Cross-Cultural Comparison

A Introduction

There are many different factors that can influence the willingness to share personal data. In our interdisciplinary project *Vectors of Data Disclosure,* our overall goal is to better understand people's decisions about disclosing or withholding personal data. In the cultural part of the project, we are particularly interested in cultural variation in this respect, as well as in commonalities in relation to key parameters of data disclosure which we are investigating.[1] These are shown in the figure below:

Daniela Wawra is a professor of English Language and Cultural Studies at the University of Passau, daniela.wawra@uni-passau.de.

1 For an introduction, cf Daniela Wawra, 'The Cultural Context of Personal Data Disclosure Decisions' (2022) 22(2) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/Intro_bidt_Wawra_University_of_Passau_IRDG_Research_paper_Series.pdf> accessed 07.02.2023.

https://doi.org/10.1515/9783111010601-010

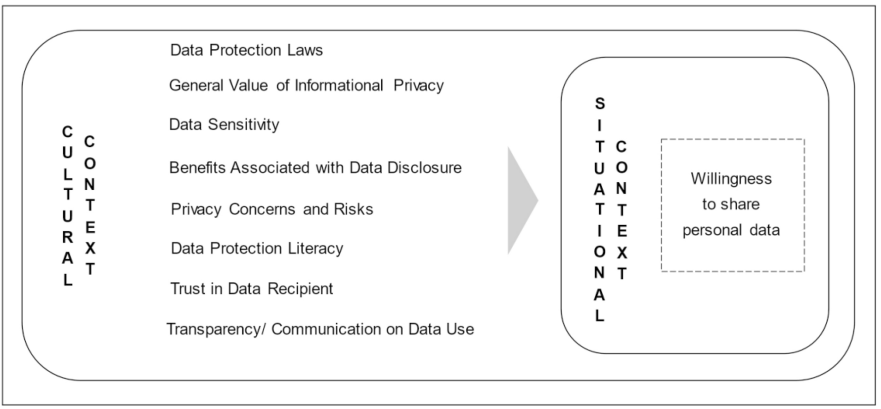

Fig. 1: Central Cultural Parameters of Data Disclosure.[2]

Individual country reports structured along these parameters (with the exception of data protection laws, which are presented in separate reports[3]) have already been published for Brazil, China, Germany, Japan, Russia, and the USA as part of our project.[4] The publication of reports on Ghana and Switzerland will fol-

2 Adapted from ibid 8.

3 For a summary, see Timo Hoffmann, in this volume, at 1.

4 See Sarah Howe, 'Cultural Influences on Personal Data Disclosure Decisions: German Perspectives' (2022) 22(14) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-14.pdf> accessed 07.02.2023; Lena Kessel, 'Cultural Influences on Personal Data Disclosure Decisions: US-American Perspectives' (2022) 22(04) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/Country_Report_USA_publication_LK_Final.pdf> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Brazilian Perspectives' (2022) 22(08) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-08.pdf> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Chinese Perspectives' (2022) 22(09) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-09.pdf> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Japanese Perspectives' (2022) 22(10) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-10.pdf> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Russian Perspectives' (2022) 22(11) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-11.pdf> accessed 07.02.2023.

low. This paper draws on these reports and focuses on the parameters of data sensitivity and data protection literacy in combination with data protection laws:

1) It provides a cultural comparison of what kinds of data are defined as sensitive in the data protection laws in the countries we selected for analysis in our interdisciplinary project: Brazil, China, Germany (the EU), Ghana, Japan, Russia, Switzerland, and the United States.
2) Furthermore, data protection literacy is compared in these countries, with the exception of Ghana, for which relevant data are not yet available but will soon be collected in the context of our project. Data protection literacy is defined here as a person's "awareness and knowledge of data protection, privacy rules and policies as well as the skills they report to have, and the measures they take to protect their personal data".[5]

Data protection laws and the other parameters of data disclosure listed in Figure 1 above are the subject of further contributions in this volume. It should be noted that it depends on the concrete disclosure situation which of the aforementioned factors influence an individual's willingness to share data and with what force. Apart from these parameters, which are central to the cultural context of data disclosure, other factors can come into play as well, such as personality traits and socio-demographic aspects. Furthermore, possible influences can be conscious or unconscious, and sometimes individuals share their data spontaneously.[6]

B Data Sensitivity

Data sensitivity occupies a central place among the parameters of data disclosure: In their meta-study of data disclosure literature, Ackermann and others,[7] for example, conclude that the more sensitive respondents consider certain data to be, the less other variables affect their willingness to share personal data:

> In other words, consumers will be very unlikely to share private data that they perceive as very sensitive, irrespective of what type of compensation they are offered in return or the degree of anonymity that is granted to them.[8]

5 Wawra, 'The Cultural Context of Personal Data Disclosure Decisions' (n 1) 9.

6 Cf ibid 6.

7 Kurt Alexander Ackermann and others, 'Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies' (2021) 21(2) Journal of Consumer Behaviour.

8 Ibid.

I Legal Definitions of Sensitive Data in Cultural Comparison

A comparison of what is defined as sensitive or special (personal) data or information in the main data protection laws in the eight countries included in our project shows that there is – partly considerable – cultural variation in terms of what type of data fall under this category. The central legal texts for the different cultures are the Brazilian General Data Protection Law[9] (LGPD 2019), the Personal Information Protection Law of the People's Republic of China[10] (PIPL 2021), the EU's General Data Protection Regulation[11] (GDPR 2016), which is applicable in Germany, Ghana's Data Protection Act 2012[12] (DPA 2012), the Japanese Act on the Protection of Personal Information[13] (APPI 2020), the Russian Data Protection Act No. 152 FZ[14] (DPA 2006), the (revised) Swiss Federal Act on Data Protection[15] (FADP 2020), and, for the USA, the California Privacy Rights Act[16] (CPRA 2020) and the Virginia Consumer Data Protection Act[17] (VCDPA 2021).[18] The latter two introduce 'sensitive personal

9 Brazilian General Data Protection Law (as amended by Law No. 13.853 of 8 July 2019), <https://www.dataguidance.com/sites/default/files/lgpd_translation.pdf> accessed 07.02.2023.

10 Personal Information Protection Law of the People's Republic of China (2021), <http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm> accessed 07.02.2023.

11 General Data Protection Regulation (VO (EU) 2016/679), <https://gdpr.eu/tag/gdpr/> accessed 07.02.2023.

12 Act of the Parliament of the Republic of Ghana Entitled Data Protection Act (2012). <https://nita.gov.gh/theevooc/2017/12/Data-Protection-Act-2012-Act-843.pdf> accessed 07.02.2023.

13 Amended Act on the Protection of Personal Information (2020), <https://www.ppc.go.jp/files/pdf/APPI_english.pdf> accessed 07.02.2023.

14 Russian Federation Federal Law on Personal Data (2006), Unofficial Translation: <https://www.dataguidance.com/sites/default/files/en_20190809_russian_personal_data_federal_law_2.pdf> accessed 07.02.2023.

15 Federal Act on Data Protection (FADP) of 25 September 2020 (effective 1 September 2023) <https://www.fedlex.admin.ch/eli/fga/2020/1998/de> accessed 07.02.2023.

16 California Privacy Rights Act (2020), California Civil Code § 1798.100 – § 1798.192 (effective 1 January 2023), <https://cpra.gtlaw.com/cpra-full-text/> accessed 07.02.2023.

17 Virginia Consumer Data Protection Act (2021), Code of Virginia § 59.1–575 – § 59.1–585 (effective 1 January 2023), <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/> accessed 07.02.2023.

18 Cf eg Clarip, 'Handling Sensitive Personal Information under the CPRA and the VCDPA' (2022) <https://www.clarip.com/data-privacy/handling-sensitive-personal-information-under-the-cpra-and-the-vcdpa/> accessed 07.02.2023; Apart from these legal texts, the following sources were consulted. They provide overviews of and more specific insights into data protection legislation in the eight countries studied: Rick Buck, *Complete Guide to LGPD: Brazil's Data Privacy Law* (2021) <https://wirewheel.io/blog/lgpd-brazil-data-privacy-law-guide/> accessed 07.02.2023; Raymond Codjoe, 'Ghana – Data Protection Overview' (2021) <https://www.dataguidance.com/notes/ghana-data-protection-overview> accessed 07.02.2023; DLA Piper, 'Data Protection Laws of the World: Japan – Definition of Personal Information' (2022) <https://www.dlapiperdataprotection.com/index.html?t=def

initions&c=JP&c2=>; DLA Piper, 'Data Protection Laws of the World: Russia – Definitions' (2021) <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=RU&c2> accessed 07.02.2023; DLA Piper, 'Data Protection Laws of the World: Switzerland – Definitions' (2021) <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=CH&c2> accessed 07.02.2023; DLA Piper, 'Data Protection Laws of the World: Brazil – Definition of Personal Data' (2022) <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=BR> accessed 07.02.2023; DLA Piper, 'Data Protection Laws of the World: China – Definition of Personal Data' (2022) <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=CN&c2=> accessed 07.02.2023; DLA Piper, 'Data Protection Laws of the World: Germany – Definitions' (2022) <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=DE&c2=>; DLA Piper, 'Data Protection Laws of the World: Ghana – Definitions' (2022) <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=GH&c2=> accessed 07.02.2023; DLA Piper, 'Data Protection Laws of the World: USA – Definitions' (2022) accessed 07.02.2023; Timo Hoffmann, 'Data Protection Act(ion) – Report on the Law of Data Disclosure in Ghana' (2022) 22(01) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/IRDG_Research_paper_Series_Country_Report_Ghana_Final.pdf> accessed 07.02.2023; Timo Hoffmann, 'Data Protection by Definition – Report on the Law of Data Disclosure in Japan' 22(03) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/Hoffmann_Data_Disclosure_Japan_Data_Protection_by_Definition.pdf> accessed 07.02.2023; Timo Hoffmann and Pietro Vargas, 'Report on the Law of Data Disclosure in Brazil' 22(06) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-06.pdf> accessed 07.02.2023; Daniel Hounslow, 'Japan – Data Protection Overview' (2022) <https://www.dataguidance.com/notes/japan-data-protection-overview> accessed 07.02.2023; Sarah Hünting, 'Endeavour to Contain Chinas' Tech Giants – Country Report on China' 22(15) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22_15.pdf> accessed 07.02.2023; Benedikt Leven, 'Land of the Free – Legal Country Report on the United States of America' 22(12) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-12.pdf> accessed 07.20.23; Dora Luo and Yanchen Wang, 'China – Data Protection overview' (2021) <https://www.dataguidance.com/notes/china-data-protection-overview> accessed 07.02.2023; OneTrust DataGuidance Analysts, 'EU – Data Protection Overview' (2021) <https://www.dataguidance.com/notes/eu-data-protection-overview> accessed 07.02.2023; Maria Otashenko, 'Russia – Data Protection Overview' (2022) <https://www.dataguidance.com/notes/russia-data-protection-overview> accessed 07.02.2023; Elisabeth Saponchik, 'Digital Citadel – Country Report on Russia' 22(13) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-13.pdf> accessed 07.02.2023; Michael Schmidl, 'Germany – Data Protection Overview' (2022) <https://www.dataguidance.com/notes/germany-data-protection-overview> accessed 07.02.2023; Peer Sonnenberg and Timo Hoffmann, 'Data Protection Revisited – Report on the Law of Data Disclosure in Switzerland' 22(17) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22_17.pdf> accessed 07.02.2023; Thomas Steiner, 'Switzerland – Data Protection Overview' (2022) <https://www.dataguidance.com/notes/switzerland-data-protection-overview> accessed 07.02.2023 ; Kai von Lewinski, 'Informational Gold Standard and Digital Tare Weight – Country Report on Data Disclosure in the European Union' 22(05) University of Passau IRDG Research Paper

information' into US privacy law. However, there were already some sector-specific laws at a federal level that functionally classified some data as requiring special protection/regulation such as the COPPA for children data, HIPAA for health data, and FCRA for financial data.

First, we will take a look at the commonalities of the legal texts with regard to data sensitivity: All laws of the eight countries define certain kinds of personal data that are considered to be in need of special protection. In some laws they are called sensitive (in the LGPD (2019), PIPL (2021), the FADP (2020), the CPRA (2020), and the VCDPA (2021), in others special data (in the APPI (2020), DPA (2006), DPA (2012), GDPR (2018)), or information (in the APPI[19], the CPRA, and the PIPL) (see Table 1 below for the exact reference in each law). The APPI (2020), for example, defines '[s]pecial care-required personal information' in Ch. I, Art. 2 (3). The legislation in all eight countries also has in common that personal data (or information) (and consequently sensitive personal data) are defined as such when the information can be linked to an individual. In Ghana's DPA, for example,[20] personal data are defined in Sec. 96 as

> data about an individual who can be identified, (a) from the data, or (b) from the data or other information in the possession of, or likely to come into the possession of the data controller.[21]

Data protection legislation varies cross-culturally, however, with regard to how many categories of sensitive data are included, what their exact denomination is and in how much detail they are outlined. This will be explained in more detail and summarized in Table 1 below.

First of all, there are only two broad data categories that are defined as sensitive in all eight countries: data relating to religious beliefs and activities as well as to health. Brazilian data protection law, for example, includes religious beliefs and membership in a religious organization,[22] while Swiss law includes 'religious views

Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/von_Lewinski_EU_L%C3%A4nderbericht_23.03.2022.pdf> accessed 07.02.2023; the parameter of data sensitivity is also detailed in each of the cultural country reports that we developed as part of our project (cf n 6).

19 The APPI uses both the terms 'personal information' and 'personal data' (Timo Hoffmann, 'Data Protection by Definition – Report on the Law of Data Disclosure in Japan' (n 18) 11, 12 for specifications).

20 Cf Timo Hoffmann, 'Data Protection Act(ion) – Report on the Law of Data Disclosure in Ghana' (n 18) 8.

21 Act of the Parliament of the Republic of Ghana Entitled Data Protection Act, sec. 96.

22 Brazilian General Personal Data Protection Law 7 August 2019, LGPD.

or activities' (Art. 5 (c) (1) FADP). The US VCDPA differentiates between physical and mental health. Ghanaian law is the most detailed and mentions 'physical, medical, mental health or mental condition [...] of the data subject'.[23] Japanese law, in contrast, only mentions 'medical history' for this sensitive data category.[24]

Japan is also the only country that does not explicitly define genetic or biometric information as sensitive: Brazil, Germany (the EU), Switzerland, and the USA include both types of data, Chinese and Russian law only mention biometric information; Ghanaian law uses the term 'DNA'.[25] Japanese law is again an exception in that it is the only one in which sex life or related data are not explicitly defined as sensitive. The Japanese law only contains a general reference to 'any other information that might cause the person to be discriminated against'.[26] Swiss legislation uses the term 'intimate sphere'.[27] The GDPR and US law both mention sex life and sexual orientation (CPRA).[28] Ghana's DPA interprets 'sexual life', the term that is used in the section 'Processing of special personal data prohibited', as 'sexual orientation' in the interpretation section, where 'special personal data' are listed.[29] Sexual orientation can be interpreted as extending to a person's gender identity. Chinese law completely avoids terms containing 'sex': The PIPL includes the category 'specific identity' as sensitive information, 'a term that is understood to cover personal attributes such as gender identity and sexual preferences'.[30]

With the exception of the Chinese information protection law, data on ethnicity or race are defined as sensitive in the corresponding laws of the remaining seven countries: Japan only uses the term race. Germany (the EU), Brazil, Ghana, Russia, Switzerland, and the USA mention both race and ethnicity. Ghana has the most explicit law with regard to this category: It also includes color and tribal origin as 'special personal data'.[31]

Five of the eight countries – Brazil, Germany (the EU), Ghana, Russia, and Switzerland – classify data that can reveal an individual's political views as sensitive.

---

23 DLA Piper, 'Data Protection Laws of the World: Ghana – Definitions' (n 18).

24 DLA Piper, 'Data Protection Laws of the World: Japan – Definition of Personal Information' (n 18).

25 DLA Piper, 'Data Protection Laws of the World: Ghana – Definitions' (n 18).

26 DLA Piper, 'Data Protection Laws of the World: Japan – Definition of Personal Information' (n 18).

27 DLA Piper, 'Data Protection Laws of the World: Switzerland – Definitions' (n 18).

28 The VCDPA includes only sexual orientation in this sensitive data category.

29 Act of the Parliament of the Republic of Ghana Entitled Data Protection Act (n 12) sec. 37 (1).

30 P. McKenzie, Gordon A Milner and Chuan Sun, 'China's Personal Information Protection Law (PIPL): Key Questions Answered' (2021) <https://www.mofo.com/resources/insights/210908-chinas-personal-information-protection-law.html> accessed 07.02.2023.

31 Cf DLA Piper, 'Data Protection Laws of the World: Ghana – Definitions' (n 18).

This may include political opinion, membership in a political organization or political activities in general. Swiss data protection law includes 'ideological' as sensitive data in addition to 'political [...] views or activities'.[32] The main Chinese, Japanese and US data protection laws do not explicitly include such expressions of political opinion in their general definitions of sensitive information (neither CPRA nor VCDPA). In Brazil, Germany (the EU), Ghana, Switzerland, and the USA, union membership or activity are also included in their sensitive data categories. In Brazilian data protection law, membership in a philosophical organization is also considered to be sensitive, and in German (EU), Ghanaian, Russian and US legislation philosophical beliefs are categorized as sensitive data.

Three of the eight countries, Ghana, Japan, and Switzerland, define criminal records as sensitive;[33] Japanese data protection law additionally includes information about having been the victim of a crime.[34]

Personal information on minors is explicitly included in the definitions of sensitive data in China, Ghana, and the USA.[35]

The following data categories are classified as sensitive by two of the eight countries we studied: Financial data are mentioned in the Chinese and US data protection laws: The CPRA (Sec. 1798.140 (L) (3) (ae) (1) (B)) categorizes any information as sensitive

> that reveals [...] a consumer['s] [...] account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.[36]

Chinese data protection legislation is not as detailed and only mentions financial accounts. Social security measures are considered to be sensitive information in

32 Cf DLA Piper, 'Data Protection Laws of the World: Switzerland – Definitions' (n 18).

33 The GDPR does not include criminal records in its definition of "special categories of personal data" (GDPR 2018 Art. 9). In Art. 10, however, it restricts the processing of such data as follows: "Processing of personal data relating to criminal convictions and offences or related security measures based on Art. 6(1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority".

34 Cf DLA Piper, 'Data Protection Laws of the World: Japan – Definition of Personal Information' (n 18).

35 Special regulations for the processing of data concerning minors are in place in Germany (the EU), and Brazil. This is not the case in Japan, Switzerland and Russia.

36 Cf also DLA Piper, 'Data Protection Laws of the World: USA – Definitions' (n 18).

Switzerland and the USA. Location tracking or a person's precise geolocation are included in the sensitive data categories in Chinese and US data protection law.

Some data categories are explicitly defined as sensitive in one country's main data protection legislation only, mostly in US law: Accordingly, personal identification numbers are considered sensitive information, such as social security, driver's license, state identification card and passport numbers.[37] Account logins, digital signatures, and correspondence contents and records are also classified as sensitive information in US law, the latter with the restriction "unless the business is the intended recipient of the communication" (CPRA Sec. 1798.140 (L) (3) (ae) (1) (E)). Citizenship or immigration status is included here as well.[38] Property information is categorized as sensitive in Chinese law only. Finally, social status is defined as sensitive exclusively in Japanese data protection law.

Table 1 on the following pages summarizes the findings from the analysis of the data protection laws in the eight countries. It provides an overview of which data are defined as sensitive in the main data protection law of each country (see above): According to this categorization, 20 categories of sensitive data can be found in the definitions of sensitive data in the main data protection laws of the eight countries studied. Each contains between 5 and 16 categories of sensitive data in their respective law. Japanese legislation is the leanest in this respect, while US law is the most detailed. One reason for this could be Japan's reportedly pragmatic approach to privacy, which will be discussed in more detail below.[39] An explanatory factor for the California's and Virginia's detailed data protection legislation in relation to sensitive data categories could be the United States' constant leading role in the field of digitalization: Thus, it has occupied first place in the IMD World Digital Competitiveness Ranking (WDCR) since 2018.[40] The WDCR "analyses and ranks the extent to which countries adopt and explore digital technologies leading to transformation in government practices, business models and society in general".[41] One consequence of this could be that they have more experience with potential threats to data security (including new digital areas) in the USA, which has already resulted in corresponding protective regulations.

37 Ibid.

38 DLA Piper, 'Data Protection Laws of the World: USA – Definitions' (n 18); Code of Virginia Chapter 53. Consumer Data Protection Act. § 59.1–575 2021.

39 See *infra,* C.

40 Cf IMD, 'IMD World Digital Competitiveness Ranking 2021' (2021) <https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/> accessed 07.02.2023.

41 Ibid 32.

Tab. 1: Cross-Cultural Comparison of Sensitive Data Categories in Main Data Protection Laws.

Country **Data**	**Brazil** LGPD (2019) Art. 5(II)	**China** PIPL (2021) Sec. 2 Art. 28	**Germany** (the EU) GDPR (2018) Art. 9, 10	**Ghana** DPA (2012) Sec. 37(1), 96	**Japan** APPI (2020) Ch. I Art. 2(3)	**Russia** DPA (2006) Art. 10(1), 11(1)	**Switzerland** FADP (2020) Art. 5(c)	**USA** CPRA (2020) Cal. Civ. Code 1798.140 (L) (3) (ae), VCDPA (2021) CoV § 59.1–575
religious beliefs or activities	x	x	x	x	x	x	X	x
health data	X	x	x	x	x	x	x	x (VCDPA physical or mental)
genetic and biometric information	x x	x	x x	x (DNA)		x	x x	x x
sex (life) and gender identity	X	x (special identity)	x (sex life or sexual orientation)	x (sexual life [37(1)], sexual orientation [96]		x	x (intimate sphere)	x (sex life or sexual orientation)
ethnicity or race	x x		x x	x x	x	x x	x x	x x
political views and activities	x		x	x		x	x (and ideological views and activities)	
union membership or activity	X		x	x			x	x

Tab. 1: Cross-Cultural Comparison of Sensitive Data Categories in Main Data Protection Laws. *(Continued)*

Country **Data**	**Brazil** LGPD (2019) Art. 5(II)	**China** PIPL (2021) Sec. 2 Art. 28	**Germany** (the EU) GDPR (2018) Art. 9, 10	**Ghana** DPA (2012) Sec. 37(1), 96	**Japan** APPI (2020) Ch. I Art. 2(3)	**Russia** DPA (2006) Art. 10(1), 11(1)	**Switzerland** FADP (2020) Art. 5(c)	**USA** CPRA (2020) Cal. Civ. Code 1798.140 (L) (3) (ae), VCDPA (2021) CoV § 59.1–575
membership in a philosophical organization / philosophical beliefs	x		x	x		x		x
criminal records and data on having been the victim of a crime				x	x x		x	
personal information of a minor		x		x				x
financial data		x						x
social security measures							x	x
location (tracking)		x						x
personal identification number								x
account login								x

Tab. 1: Cross-Cultural Comparison of Sensitive Data Categories in Main Data Protection Laws. *(Continued)*

Country **Data**	**Brazil** LGPD (2019) Art. 5(II)	**China** PIPL (2021) Sec. 2 Art. 28	**Germany** (the EU) GDPR (2018) Art. 9, 10	**Ghana** DPA (2012) Sec. 37(1), 96	**Japan** APPI (2020) Ch. I Art. 2(3)	**Russia** DPA (2006) Art. 10(1), 11(1)	**Switzerland** FADP (2020) Art. 5(c)	**USA** CPRA (2020) Cal. Civ. Code 1798.140 (L) (3) (ae), VCDPA (2021) CoV § 59.1–575
digital signature								x
correspondence records and contents								x (unless the business is the intended recipient of the communication)
citizenship or immigrant status								x
property information		x						
social status					x			
total number of sensitive data categories	8	8	8	10	5	7	9	16

II Cross-Cultural Surveys on Sensitive Data Categories

What a country defines as sensitive data in its main data protection law and what people consider to be sensitive data does not always correspond. A comparison of the legally defined data categories with the assessments of respondents from Brazil regarding the sensitivity of data in a large-scale survey by Markos, Milne, and Peltier,[42] for example, reveals the following: Respondents consider security & access codes and passwords, as well as credit score to be the most sensitive data categories included in the study.[43] However, these do not fall under the legal definition of sensitive data according to Brazil's main data protection legislation, the LGPD.[44] Another example of a discrepancy between the law and people's assessment of what constitutes sensitive data can be found for Japan: Financial data are among the most sensitive according to Japanese respondents in surveys conducted by Roose and Pang, and Fukuta and others[45] However, they are not explicitly included in the APPI's definition of sensitive data either.[46] Globally, financial data usually fall under the category of personal data, and while some countries – such as China and the USA in our study sample – include them in their definitions of sensitive data in their main information protection laws, others do not. There are, however, regularly specific regulations for the financial sector on how these data should be handled and protected,[47] such as Brazil's "Bank Self-Regulation Standard 025/2021 ('SARB Standard 025/2021'), in force since 18 February 2022",[48] for instance.

---

42 Ereni Markos, George R Milne and James W Peltier, 'Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil' (2017) 36(1) Journal of Public Policy & Marketing.

43 Cf also Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Brazilian Perspectives' (n 4).

44 See *supra.* B.1.

45 Jochen Roose and Natalie Pang, *Data Security, Privacy and Innovation Capability in Asia: Findings from a Representative Survey in Japan, Singapore and Taiwan* (2021) <https://www.kas.de/documents/252038/11055681/Survey+on+Data+Security%2C+Privacy+and+Innovation+Capability+in+Asia.pdf/1b96fbea-5f0c-5716-dbc4-a426eca190bc?version=1.0&t=1628241322758> accessed 07.02.2023; Yasunori Fukuta and others, 'Personal Data Sensitivity in Japan' (2017) 1(2) The ORBIT Journal 1; cf also Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Japanese Perspectives' (n 7).

46 See *supra,* B.1.

47 Cf eg, for Japan: Hounslow (n 18).

48 A Ferreira de Melo Brito and R da Fonseca Chauvet, 'Brazil: New Data Protection Regulations for Banks' (2022) <https://www.dataguidance.com/opinion/brazil-new-data-protection-regulations-banks> accessed 07.02.2023.

> It [...] establishes minimum procedures regarding protection of personal data. Among these minimum requirements are the formulation and implementation of a privacy governance program ('the Program'), which specifies the minimum content that must be observed by all Brazilian financial institutions.[49]

One example is:

> Privacy applies to all personal data treated by institutions. This means safeguarding not only the data of customers, but also the data of all other individuals that interact with the customers.[50]

In another study, by Trepte and Masur,[51] which compares sensitivity ratings for various kinds of personal data cross-culturally, here between Chinese, German, and US respondents, Germany has by far the highest ratings for all data categories included – except for the food and music items (cf Figure 2):

After sexual behavior (6.49 rating on a seven-point Likert scale) (which is included in the GDPR), financial data (6.43 rating) and political views (4.33) (which also count as sensitive data according to the GDPR) are indicated as being above a medium sensitivity level.[52] Yet again, financial data are not explicitly mentioned in the definition of sensitive data in the GDPR. This is in contrast to the inclusion of the category of financial data in the definitions of sensitive information in Chinese and US law.[53] No large-scale surveys on perceptions of data sensitivity in Ghana, Russia, and Switzerland could be found. A systematic cross-cultural survey on this topic that includes all sensitive data categories that occur in the laws of the countries studied is a follow-up project. The aim is to address for each country whether it adequately meets people's privacy needs, or whether additional or fewer sensitive data categories should be included in its data protection legislation. For this purpose, data protection experts' assessments will be surveyed.

How can the survey results of Trepte and Masur's[54] comparative study of respondents' perceptions of the sensitivity of specific information (see Fig. 2) be explained? Why are German respondents the most concerned about their privacy compared to Chinese and US respondents? This can be interpreted to mean that

49 Ibid.

50 Ibid.

51 Sabine Trepte and Philipp K Masur, *Cultural Differences in Social Media Use, Privacy, and Self-Disclosure* (2016) <http://opus.uni-hohenheim.de/volltexte/2016/1218/pdf/Trepte_Masur_ResearchReport.pdf> accessed 07.02.2023.

52 See B.I.

53 Ibid.

54 Trepte and Masur (n 51).

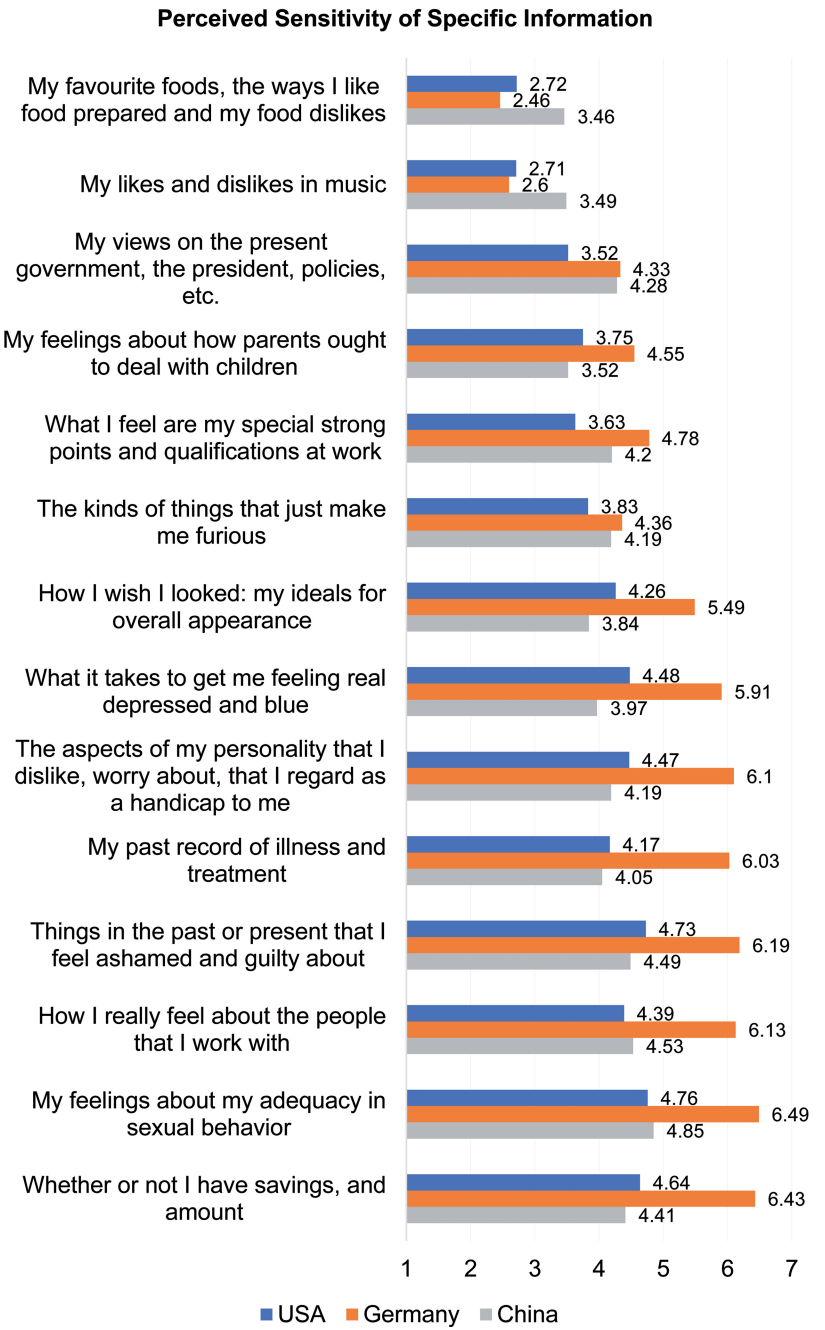

Fig. 2: Perceived Sensitivity of Specific Information in Cross-Cultural Comparison.

Germans tend to be more concerned about what will follow from the disclosure of the respective information than respondents from the other countries. Since this is always an unknown, it can be seen as an indication for high Uncertainty Avoidance practice. This has often been considered as characteristic of German culture: Hofstede[55], who introduced the Uncertainty Avoidance dimension to compare cultures, defines it as "the degree to which the members of a society feel uncomfortable with uncertainty and ambiguity"[56]:

> Countries exhibiting strong UAI [Uncertainty Avoidance Index] maintain rigid codes of belief and behavior, and are intolerant of unorthodox behavior and ideas. Weak UAI societies maintain a more relaxed attitude in which practice counts more than principles.[57]

The higher a country's score on Hofstede's Uncertainty Avoidance Index (UAI) (from 0–100), the more the collective is assumed to avoid uncertainty. Indeed, Germany has the highest score at 65, followed by the USA at 46, and China at 30.[58] Chinese respondents in Trepte and Masur's study,[59] however, were not always less concerned about their privacy than US respondents, as would be expected according to the countries' Hofstede scores. This suggests that countries' Uncertainty Avoidance scores are too general a cultural indicator to be meaningful for such specific aspects as perceptions of data sensitivity.

In another widely used survey that uses cultural dimensions, the Globe study, Uncertainty Avoidance is defined as "[t]he extent to which a society, organization, or group relies on social norms, rules, and procedures to alleviate unpredictability of future events"[60]: If we compare Globe's Uncertainty Avoidance practice (UA) scores for the three countries, Germany again has the highest score of 5.16, followed by China at 4.94 and the USA at 4.15.[61] While China has a higher UA than

55 Geert Hofstede, *Culture's Consequences: International Differences in Work-Related Values* (Sage Publications 1980); Geert Hofstede, *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations* (2nd edn: Sage Publications 2001); Geert Hofstede, 'The Dimensions of National Culture' (2022) <https://hi.hofstede-insights.com/national-culture> accessed 07.02.2023; Geert Hofstede, 'Country Comparison Graphs' (2022) <https://geerthofstede.com/country-comparison-graphs/> accessed 07.02.2023.

56 Hofstede, 'The Dimensions of National Culture' (n 55).

57 Ibid.

58 Hofstede, 'Country Comparison Graphs' (n 55).

59 Trepte and Masur (n 51).

60 Globe, 'An Overview of the 2004 Study: Understanding the Relationship Between National Culture, Societal Effectiveness and Desirable Leadership Attributes' (2020) <https://globeproject.com/study_2004_2007#theory> accessed 07.02.2023.

61 Globe, 'Country Map' (2020) <https://globeproject.com/results/#country> accessed 07.02.2023.

the USA here, in contrast to the Hofstede ranking[62] (see above), Germany's ranking as the country with the highest uncertainty avoidance (according to the respective definitions) remains constant. This also shows that it is problematic to link cultural dimensions – which are designed for a wider cultural context – to narrower contexts such as data disclosure. Another critical factor is that cultural dimensions are supposed to reflect rather stable attitudes that dominate in a country. However, the stability of the attitudes expressed in specific surveys such as those on data sensitivity cited above (and those on data protection literacy below) is unclear. At the same time, the countries' scores on the cultural dimensions might change at some point. Regular diachronic analyses would be necessary to check these aspects. Nevertheless, it is not unusual to check whether country scores correlate with certain synchronic (survey) findings. This is discussed controversially, and the results of studies that try to find correlations are mixed.[63]

C Data Protection Literacy

Another parameter that can influence an individual's willingness to share personal data is their data protection literacy (see Figure 1 above). Data Protection Literacy

62 Hofstede, 'Country Comparison Graphs' (n 55).

63 Cf eg Sandra J Milberg, H. J Smith and Sandra J Burke, 'Information Privacy: Corporate Management and National Regulation' (2000) 11(1) Organization Science 35; Steven Bellman and others, 'International Differences in Information Privacy Concerns: A Global Survey of Consumers' (2004) 20(5) The Information Society 313; Haejung Yun, Gwanhoo Lee and Dan J Kim, *A Meta-Analytic Review of Empirical Research on Online Information Privacy Concerns: Antecedents, Outcomes and Moderators* (2014); Hai Liang, Fei Shen and King-wa Fu, 'Privacy protection and self-disclosure across societies: A study of global Twitter users' (2017) 19(9) New Media & Society 1476; Sabine Trepte and others, 'A Cross-Cultural Perspective on the Privacy Calculus' (2017) 3(1) Social Media + Society 205630511668803; Lemi Baruh, Ekin Secinti and Zeynep Cemalcilar, 'Online Privacy Concerns and Privacy Management: A Meta-Analytical Review' (2017) 67(1) Journal of Communication 26; Yao Li and others, 'Cross-Cultural Privacy Prediction' (2017) 2017(2) Proceedings on Privacy Enhancing Technologies 113; Haejung Yun, Gwanhoo Lee and Dan J Kim, 'A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs' (2019) 56(4) Information & Management 570; Shintaro Okazaki and others, 'Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review' (2020) 96(4) Journal of Retailing 458; Yao Li, 'Cross-Cultural Privacy Differences' in Bart P Knijnenburg and others (eds), *Modern Socio-Technical Perspectives on Privacy* (2022).

> captures [people's] awareness and knowledge of data protection, privacy rules and policies as well as the skills they report to have, and the measures they take to protect their personal data.[64]

This parameter includes very different aspects that can operate in different directions (like vectors) in data disclosure situations.[65] It has therefore been suggested to differentiate between the awareness and the knowledge aspect, the skills people report to have (which does not mean that they actually have them), and the measures they allegedly take.[66] We have to restrict our cultural comparison to the aspects of awareness and knowledge, as well as people's (reported) efforts to protect their data due to the lack of a sufficiently broad and detailed data base for all the countries we studied. Respective data are included, as far as they were available, in the individual cultural country reports that were published as part of our project.[67] A systematic large-scale survey and analysis of the different aspects of data protection literacy in more countries and in cultural comparison is a research gap to be closed.

We will first take a look at "people's awareness and knowledge of data protection, privacy rules and policies" (see above). How aware are people of the protection and privacy rules in their respective countries?

Germany is the only country in which a clear majority of 59 % feels they are very or somewhat aware of their country's data protection and privacy rules. Slightly fewer, but still half of the Russian respondents indicate this as well. In the other countries, large majorities are not very or not at all aware.

Again, this is not in accordance with the expectations that result from the countries' Uncertainty Avoidance scores:[68] Respondents from a country with a higher score on this dimension would be expected to place greater importance on rules and laws, as they can help reduce uncertainty. One could therefore assume that these respondents overall are more aware of their country's data protection and privacy rules than respondents from countries with a lower UA(I) score. However, a look at the country scores shows that this hypothesis does not hold: Russia, for example, is the country with the highest uncertainty avoidance

64 Wawra, 'The Cultural Context of Personal Data Disclosure Decisions' (n 1) 9; see also A.

65 Cf ibid, 9, 10.

66 Cf Baruh, Secinti and Cemalcilar (n 63), 47; Philipp K Masur, 'How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information' (2020) 8(2) Media and Communication 258; also Wawra, 'The Cultural Context of Personal Data Disclosure Decisions' (n 1) 3, 4, 9, 10.

67 Cf Howe (n 4); Kessel (n 4).

68 Cf Hofstede, 'Country Comparison Graphs' (n 55); Globe, 'Country Map' (n 61).

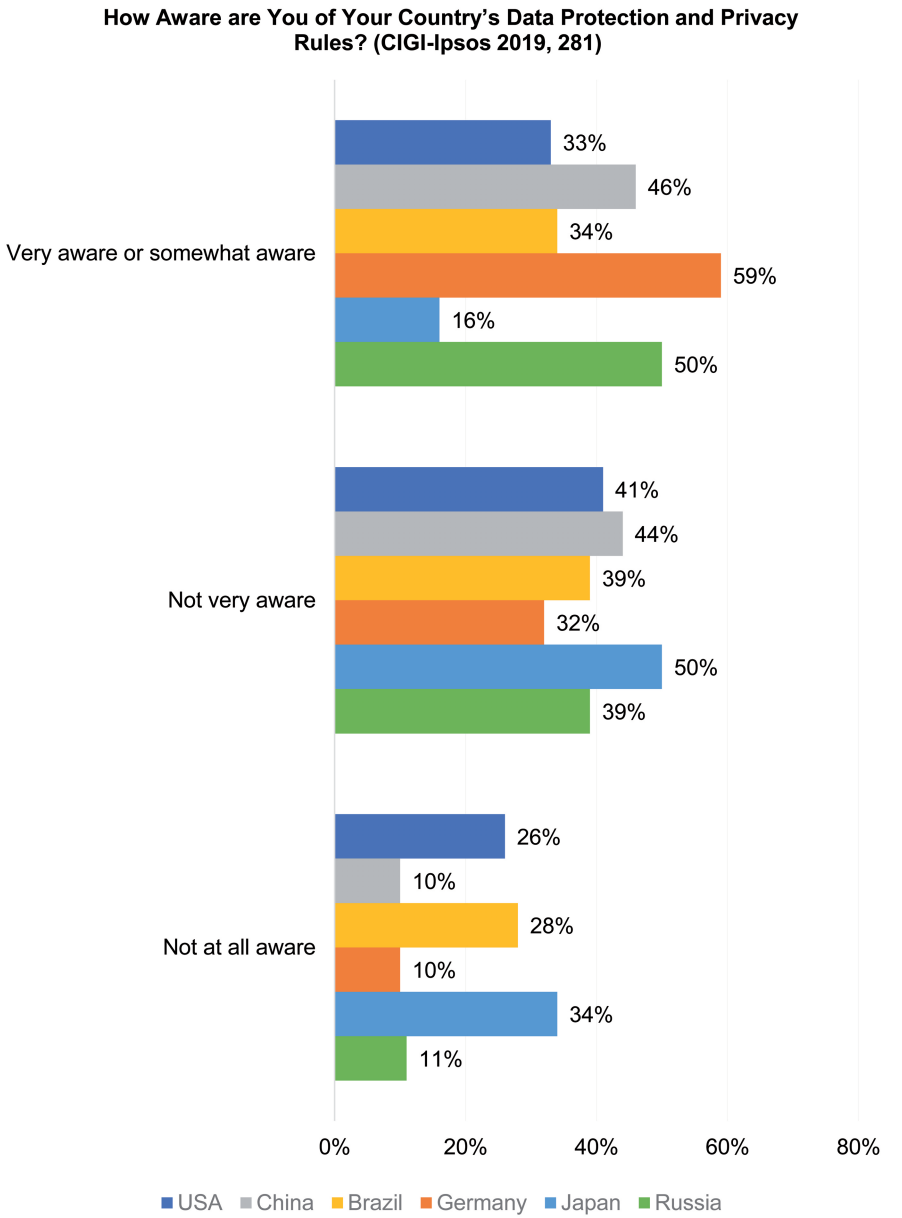

Fig. 3: Awareness of Data Protection and Privacy Rules in Cross-Cultural Comparison.

according to its score on the Hofstede dimension[69] (95), followed by Japan (92), Brazil (76), Germany (65), the United States (46), and China (30). But, for example, Japanese respondents are the least aware of their country's data protection and privacy rules, although one would expected them to be the second most aware collective after the Russian respondents, who are, after all, second only to Germans in their awareness. Therefore, there must be other factors that have a greater impact on people's awareness of data protection and privacy rules.

Another particularly remarkable result of the survey is that respondents from Japan are by far the least informed about their country's data protection and privacy rules according to their self-report. One facet of an explanation for this is that Japanese culture in general has often been described as 'pragmatic'[70] and as 'not [...] very sensitive to the protection of privacy'[71]. This has been attributed "to the Japanese cultural and social environment".[72] Orito and Murata, for example, emphasize that

> [t]here is no Japanese word corresponding precisely to the English word privacy. Many Japanese use the word *puraibashi*, an adopted word for privacy, without clearly understanding its meaning.[73] For ordinary Japanese, privacy is an imported idea; some feel that the sense of a right to privacy may be subjective and timeserving because it means that anyone can arbitrarily reject interference by others.[74]

This Japanese restraint with regard to privacy rights is also explained with their "emphasis on group mentality:" The cultural concepts of *amae* and *enryo* are central in this respect: "[...] *amae* [...] means presuming on the good will of others"; *enryo*, a concept closely linked to privacy, "means that one holds back on the basis that one must not presume [or rely] too much [...] on the good will of others." It "counter-balances" the concept of *amae.*[75]

Capurro traces the differences between the Japanese and the Western concept of privacy. He states that "in Japanese Buddhist traditions the 'self' is 'nothing' and

---

69 Hofstede, 'Country Comparison Graphs' (n 55).

70 Charah Scroope, 'Japanese Culture. The Cultural Atlas: Core Concepts' (2021) <https://culturalatlas.sbs.com.au/japanese-culture/japanese-culture-core-concepts> accessed 07.02.2023.

71 Yohko Orito and Kiyoshi Murata, *Privacy Protection in Japan: Cultural Influence on the Universal Value* (2005) <https://www.researchgate.net/publication/260021544_Privacy_Protection_in_Japan_Cultural_Influence_on_the_Universal_Value> accessed 07.02.2023; T. Hiramatsu, 'Protecting Telecommunications Privacy in Japan' (1993) 36(8) Communications of the ACM 74.

72 Orito and Murata (ibid).

73 Kiyoshi Murata, 'Is Global Information Ethics Possible?: Opinions on the Technologically-Dependent Society' (2004) 2(5) Journal of Information, Communication and Ethics in Society 518.

74 Orito and Murata (n 71).

75 Ibid.

that "the Japanese conception of privacy, [...] is community-oriented."[76] Against this background,

> insistence on the right to privacy as 'the right to be let alone' indicates a lack of cooperativeness as well as an inability to communicate with others. The right to privacy, understood as 'the individual's right to control the circulation of information concerning him or her', is considered a shameful excess of mistrust in relation both to a cooperative society and to those who collect, store, share, and use personal data. Consequently, the sense of a right to privacy is foreign and less important to Japanese society than it is in Western societies.[77]

Capurro also states that "for Japanese, private things are less worthy than public things".[78] He concludes:

> The key difference with regard to the Western conceptions of privacy seems to be that the self within *Seken* [roughly 'social contexts'][79] is something that should be denied, not protected while in the West the self is the basis for critical thinking and moral action.[80]

Orito and Murata state that for these reasons "detailed discussion of the essential value of protecting privacy and personal data has been relatively rare"[81] in Japan. These and probably further aspects can contribute to a better understanding of why such a low percentage of Japanese respondents report that they are aware of their country's data protection and privacy rules.

---

76 Rafael Capurro, 'Privacy: An Intercultural Perspective' (2005) 7(1) Ethics in Information Technology 37.

77 Orito and Murata (n 71).

78 Capurro (n 76).

79 "The Japanese script for *seken* combines the two Chinese characters meaning 'world' [...] with 'space-between' [...]. *Seken* refers to the appearance of the total network of social relations that surround an individual. It conveys the corresponding cultural norms and values that function to regulate social behavior, and hints at how such relations and behavior are maintained. *Seken* is thought to be a concept native to Japan that has existed since the seventh century. It corresponds roughly to *shakai*, the translated word for 'society,' derived from the West, which came into circulation in the Meiji period (1898–1920) as western concepts, ideals, and values became popularized by politicians and intellectuals. 'The public' is at times used as *seken*' *s* English equivalent. However, the two terms are by no means synonymous; a conceptual lacuna exists between "the public," with its universalistic connotations, and *seken*, which, by comparison, when referring to one of its meanings – network – points rather more specifically to a social context or *aidagara.* [...]. Thus *seken* can be described as the sum of interrelations as a result of the accumulation of subnetworks of *aidagara*". Tomoko Kurihara, 'Seken', *The Blackwell Encyclopedia of Sociology* (2007).

80 Capurro (n 76).

81 Orito and Murata (n 71).

When those who said they knew the law were asked whether the privacy laws in their country had a positive, neutral or negative impact, legislation in China received the most approval, with 77 % attributing a positive effect to China's Cyber Security Law (CSL) (only 3 % expected a negative effect, 20 % were neutral). In Brazil, 63 % expressed a positive attitude towards Brazil's LGPD, and in Japan it was still a majority of 55 % stating that the APPI had a positive effect. Germany is the only one of the four surveyed countries that are part of our project where a minority, ie, only 40 %, felt that the GDPR had an overall positive effect, 50 % took a neutral stance and 10 % saw a negative effect.[82]

The results of the survey reveal that Chinese respondents are by far the most likely to attribute a positive impact to their country's data protection law, followed by Brazilian and Japanese respondents (where approval rates are above 50 %). German respondents are clearly the least satisfied with their GDPR. This is in stark contrast to the country's performance in the Internet Privacy Ranking, for example. This ranking captures "which countries worked the hardest to protect a user's privacy".[83] In order to create it, "data on a variety of topics that can affect internet privacy" are collected: 'Press freedom', 'Data privacy laws', 'Democracy statistics', 'Freedom of opinion and expression', and 'Cybercrime legislation worldwide'.[84] 110 countries are ranked according to their prioritization of data protection on the internet: "A high privacy score means the country takes steps to protect information shared online. The higher the score, the more protected the information".[85] Russia and Switzerland are not included in this ranking, the internet privacy scores for the other countries are: Germany 83.3, Japan 71.3, United States 68.6, Brazil 60.6, Ghana 49.2, and China 13.1, which ranks last of all 110 countries included. While the ranking is restricted to data protection on the internet and comprises different aspects (see above), one might nevertheless expect the Germans to be the most satisfied with their data protection laws and the Chinese the least. However, according to the survey cited above, it is the other way around. Furthermore, based on the Internet Privacy Ranking, Brazilians would be expected to be less satisfied with their data protection law than the Japanese. Again, other factors must have a greater influence.

82 Cf Cisco, 'Consumer Privacy Survey: Building Consumer Confidence Through Transparency and Control' (2021) 10 <https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf> accessed 07.02.2023. The Chinese PIPL was passed in 2021 and therefore this study only took the older CSL into account.

83 A Grant, 'Internet Privacy Index' (2020) <https://bestvpn.org/privacy-index/> accessed 06/03/2022.

84 Ibid.

85 Ibid.

The starkest contrasts are seen between the survey results of German respondents and Germany's internet privacy score, as well as between the responses of Chinese respondents and China's score in the ranking. Germany's high score in the ranking suggests that Germans are used to a high level of data protection, and the survey results show that they seem to take this more or less for granted. The relatively high level of dissatisfaction with the GDPR expressed in the survey is likely primarily due to the excessive bureaucratic regulation of the GDPR, which affects the convenience of surfing the internet. This is supported by a YouGov survey[86], according to which more than half of German respondents (56 %) say that the GDPR has no influence on the security of their personal data on the internet. Only 13 % are of the opinion that the GDPR has improved the security of their data on the internet. Almost one in three, ie, 32 %, however, feel that the GDPR has made the internet less user-friendly. In addition, as, for example, the EU Commission and supporters critically note, public discussion about the GDPR has been dominated not by what they consider to be "core issues such as the 'right to be forgotten' or the improved rules for moving personal data from one service provider to another".[87] Instead, the

> number one topic of excitement is the ubiquity of cookie queries that have been popping up permanently on the net since the GDPR came into force. According to the survey, 53 percent of people in Germany feel annoyed by the consent banners. 14 percent say: 'I don't care about the consent banners, I just click on anything.' Only twelve percent think that the cookie banners give them a 'feeling of self-determination over their data.[88]

As for the overall very positive assessment by Chinese respondents of the impact of their data protection law according to the study cited above, it must first be considered that they may not have answered freely for fear of negative consequences if they criticized their government's law. Their answers may also have been censored. Thus, the Internet Privacy Ranking (see above) cites a number of reasons, why China was ranked last, among them: 'Censorship' – "China doesn't adhere to a free speech; the exact opposite actually. Information posted by citizens can be censored or blocked. Major offenses result in arrests." They continue: "In 2017, 128,000 site (sic!) were blocked and 1900 people were arrested or punished

86 Lisa Inhoffen, 'DSVGO: Die Hälfte sieht keinen Einfluss auf die Sicherheit ihrer Daten im Internet' *YouGov* (5 February 2019) <https://yougov.de/news/2019/02/05/dsvgo-die-halfte-sieht-keinen-einfluss-auf-die-sic/> accessed 07.02.2023.

87 My translation of 'Vier Jahre DSGVO: Monster oder Datenschutzvorbild?' *Süddeutsche Zeitung* (24 May 2022) <https://www.sueddeutsche.de/politik/datenschutz-vier-jahre-dsgvo-monster-oder-datenschutzvorbild-dpa.urn-newsml-dpa-com-20090101-220524-99-407459> accessed 07.02.2023.

88 Ibid.

by the Chinese government, which claims its actions are for the good of the people".[89] Furthermore, widespread and extensive surveillance in China and its social or citizen credit system are factors that need to be considered:[90]

> China is working to become the first country to create an algorithm to create profiles of every citizen. These profiles will help the government assign each person a 'citizen score' based on their digital and physical behaviour. Posting anti-government blogs, for example, or being caught via a street camera jaywalking can lower a citizen's score. The lower the score, the less privileges the citizen receives. For example, a low score results in slow internet speed or puts a passport application at the bottom of the pile.[91]

In addition, "[u]ntil recently, China had few privacy laws in place. However, the country did implement a data privacy standard recently that sets regulations for consent and puts rules in place for how data is collected, stored and shared." While "[c]ritics of this new legislation [...] point out that the new law fails to offer enforcement plans",[92] this could also explain why a large majority of Chinese respondents attribute a positive effect to China's Cyber Security Law (CSL): It seems like an improvement compared to earlier privacy regulations or the lack thereof.

Closing on a final aspect of data protection literacy, people's efforts regarding data protection, the following picture emerges from respondents' self-reports in a large survey by CIGI-Ipsos: Apart from Japan, the majority of respondents from all countries included feel that they do enough to protect their data: Brazil leads with 78 % agreement, followed by Russia (69 %), Germany (65 %), the USA (60 %), and Japan (35 %).[93] One explanation for this result could again be a tendency to take a more pragmatic approach to privacy in Japan (see above). Many questions arise from these survey results, among them: Are people's estimations correct? What kind of impact does their country's data protection law have – overall and with regard to specific aspects and areas (eg, digital competitiveness, bureaucracy,

89 Grant (n 83); Wang Zhicheng, 'China – Official Data on Internet Censorship' AsiaNews (1 September 2018) <https://www.asianews.it/news-en/Official-data-on-internet-censorship-42781.html> accessed 07.02.2023.

90 See Wawra, in this volume, at 51.

91 Grant (n 83); Anna Mitchell and Larry Diamond, 'China's Surveillance State Should Scare Everyone' *The Atlantic* (02 February 2018) <https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/> accessed 07.02.2023.

92 Grant (n 83); Samm Sacks, 'New China Data Privacy Standard Looks More Far-Reaching than GDPR' (2018) <https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr> accessed 07.02.2023.

93 Cf CIGI-Ipsos, 'CIGI-Ipsos Global Survey on Internet Security & Trust: Detailed Results Tables' (2019) 283 <https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/> accessed 07.02.2023; Unfortunately, Ghana and Switzerland were not part of the survey.

different business sectors)? How do experts assess this? We are therefore planning to conduct a corresponding and more detailed survey among data protection experts in the eight countries studied. Its main objective is to compare the survey data and to obtain experts' views on the strengths and weaknesses of the data protection legislations.

D Conclusion and Outlook

This study focused on two central parameters of data disclosure: data sensitivity and data protection literacy. It provided a systematic comparative overview of what types of data are defined as sensitive personal data in the main data protection laws of eight countries: Brazil, China, Germany, Ghana, Japan, Russia, Switzerland, and the USA. It was shown that the respective laws differ with respect to how many categories of sensitive data they define (ranging from 5 in Japan to 16 in the USA), how explicitly they are described and what terms are used. In addition, the "law in books"[94] in this respect was compared to and contrasted with people's assessments of what constitutes sensitive data. Explanations for the results of the comparative analyses were sought and critically discussed.

The second part of this contribution was dedicated to data protection literacy. It comprises quite different aspects that should better be treated separately. Respondents' awareness of their country's data protection and privacy rules, their assessment of their impact and their estimation of their own data protection activities were compared cross-culturally. Explanations for the most noticeable results were sought and critically discussed here as well.

Furthermore, important research gaps were identified and follow-up research in the form of a systematic cross-cultural survey of data protection experts' assessments of sensitive data categories and of the impact of their country's data protection regulations, including their strengths and weaknesses, was proposed.

The concrete effects that the parameters of data sensitivity and a person's data protection literacy have in a specific data disclosure context are difficult to predict. As a general rule, the more sensitive a person considers certain information to be, the more their willingness to share these data decreases. However, this tendency towards withholding their (very sensitive) data can potentially be cancelled by other factors (or vectors) of data disclosure, such as – above all – anonymity, trust in the data recipient, or expected benefits of data disclosure that seem to out-

94 Roscoe Pound, 'Law in Books and Law in Action' (1910) 44(1) American Law Review 12 <https://de.scribd.com/document/354119384/POUND-Law-in-Books-and-Law-in-Action> accessed 07.02.2023.

weigh the risks.[95] If a person does not care much about their informational privacy, they may not think twice about sharing even sensitive data, and if a data recipient communicates transparently what the data will be used for, and if the data provider agrees with this use of the data, this can work in favor of data disclosure as well. The same applies to the parameter of data protection literacy. Additionally, it is not even possible to indicate whether it generally promotes or hinders a person's willingness to share their data: Firstly, the different facets of data protection literacy can work against each other, and secondly, the effect of the individual facets is evidentially hardly predictable:[96] A greater awareness of data protection laws can, for example, mean that a person is more anxious, more aware of possible risks of data disclosure and therefore more reluctant to share data. However, the opposite may also occur, ie, a person who knows the law may feel well protected and therefore be more willing to share data. The same is true for someone who feels they are doing enough to protect their data and who thinks they have the necessary skills to do so: This feeling can be deceptive and can lead a person to feel rather safe and therefore more willing to disclose data. It can also have the opposite effect: They might in fact take many precautions and be very restrictive, leading to greater reluctance to disclose data. Further research is needed to better understand people's decisions regarding data disclosure and cultural variations with regard to potentially influential parameters. In particular, mapping the interplay of the multiple parameters of data disclosure (see Fig. 1) – which in addition include personality traits and socio-demographic factors – in concrete data scenarios remains a challenge for research.

95 Cf Lemi Baruh, in this volume, at 105.

96 Cf Wawra, 'The Cultural Context of Personal Data Disclosure Decisions' (n 1), 3, 4.

Kai von Lewinski

Collision of Data Protection Law Regimes

PNR[1], Schrems I[2], Schrems II[3]: these transatlantic cases illustrate different attitudes towards and concepts of data protection, privacy and data business on

Kai von Lewinski is a professor of Public Law, Media Law and Information Law at the University of Passau, kai.lewinski@uni-passau.de.

1 Case C–817/19 Ligue des droits humains ASBL v Conseil des ministres [2022] ECLI:EU:C:2022:491; see only Timo Zandstra and Evelien Brouwer, 'Fundamental Rights at the Digital Border: ETIAS, the Right to Data Protection, and the CJEU's PNR judgment' (2022) Verfassungsblog <https://verfassungsblog.de/digital-border/> accessed 07.02.2023.

https://doi.org/10.1515/9783111010601-011

both sides of the Atlantic[4]. They constitute a big problem for transatlantic data transfer.[5] However – and that is what this text is about –, they are only part of a larger picture: the collision of data protection law regimes.

---

2 Case C–362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650; see only Christina Eckes and Vigjilenca Abazi, 'Safeguarding European Fundamental Rights or Creating a Patchwork of National Data Protection?' (2015) Verfassungsblog <https://verfassungsblog.de/safeguarding-european-fundamental-rights-or-creating-a-patchwork-of-national-data-protection-2> accessed 07.02.2023; Christopher Kuner, 'The Sinking of the Safe Harbor' (2015) Verfassungsblog <https://verfassungsblog.de/the-sinking-of-the-safe-harbor-2/> accessed 07.02.2023; Orla Lynskey, 'Negotiating the Data Protection Thicket: Life in the Aftermath of Schrems' (2015) Verfassungsblog <https://verfassungsblog.de/negotiating-the-data-protection-thicket-life-in-the-aftermath-of-schrems-2/> accessed 07.02.2023; Lorenz Marx and Lucas Wüsthof, 'CJEU shuts down Safe Harbor for Transatlantic Data Transfer: Case C-362/14 Maximilian Schrems v Data Protection Commissioner' (2015) 4 (6) EuCML 242; Franz C Mayer, 'The Force awakens – The Schrems case from a German perspective' (2015) Verfassungsblog <https://verfassungsblog.de/the-force-awakens-the-schrems-case-from-a-german-perspective-2/> accessed 07.02.2023; Russell A Miller, 'Schrems v Commissioner: A Biblical Parable of Judicial Power' (2015) Verfassungsblog <https://verfassungsblog.de/schrems-v-commissioner-a-biblical-parable-of-judicial-power-2/> accessed 07.02.2023; Bilyana Petkova, 'Could the Schrems decision trigger a regulatory 'race to the top'?' (2015) Verfassungsblog <https://verfassungsblog.de/could-the-schrems-decision-trigger-a-regulatory-race-to-the-top/> accessed 07.02.2023; Daniel Sarmiento, 'What Schrems, Delvigne and Celaj tell us about the state of fundamental rights in the EU' (2015) Verfassungsblog <https://verfassungsblog.de/what-schrems-delvigne-and-celaj-tell-us-about-the-state-of-fundamental-rights-in-the-eu/> accessed 07.02.2023; Martin Scheinin, 'The Essence of Privacy, and Varying Degrees of Intrusion' (2015) Verfassungsblog <https://verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion-2/> accessed 07.02.2023; Gero Ziegenhorn and Katharina von Heckel, 'The Schrems Judgement: New Challenges for European and international companies' (2015) Verfassungsblog <https://verfassungsblog.de/the-schrems-judgement-new-challenges-for-european-and-international-companies-2/> accessed 07.02.2023.

3 Case C–311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559; see only Marcelo Corrales Compagnucci, Mateo Aboy and Timo Minssen, 'Cross-Border Transfers of Personal Data After Schrems II: Supplementary Measures and new Standard Contractual Clauses (SCCs)' (2021) 4(2) NJEL 37; Joseph Liss and others, 'Demystifying Schrems II for the cross-border transfer of clinical research data' (2021) 8(2) Journal of Law Biosci lsab032; Joshua P. Meltzer, 'Case Note: After Schrems II: The Need for a US-EU Agreement Balancing Privacy and National Security Goals' (2021) 2(1) GPLR 83; Maria H Murphy, 'Assessing the Implications of Schrems II for EU-US Data Flow' (2022) 71(1) ICLQ 245; Marc Rotenberg, 'Schrems II , from Snowden to China: Toward a new alignment on transatlantic data protection' (2020) 26(1-2) European Law Journal 141, 149–150; Monika Zalnieriute, 'Data Transfers after Schrems II: The EU-US Disagreements Over Data Privacy and National Security' (2022) 55 Vanderbilt Journal of Transnational Law 1.

4 Theodore Christakis and Fabien Terpan, 'EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options' (2021) 11(2) International Data Privacy Law 81; Sabrina Seak, *Grenzen der Datenübermittlungen aus der EU in Drittstaaten – anhand des Beispiels der USA* (Beiträge zum Informationsrecht vol 42, Duncker & Humblot 2022), passim.

A Data Protection: Conflicts and Collisions

I Data Protection is not a Universal Concept

Data transfer is international. As economic (and media) developments trend towards personalization and payments for privacy or data use (data economy)[6], there will be no business sector without privacy and data protection issues in the future (or even is today).

Data protection is not such a universal concept as we EU Europeans might think and believe – there is not only 'one calculus to rule them all'[7]. Privacy orientation differs among societies[8]. More collectivistic societies (as they are in Afri-

5 See only in the media (former US Secretary of Commerce, 2017–2021) Wilbur Ross, 'Europe's data privacy laws are likely to create barriers to trade' *Financial Times* (31 May 2018) 9 and in academic literature Christopher Kuner, 'The Schrems II judgment of the Court of Justice and the future of data transfer regulation' (2020) European Law Blog <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/> accessed 07.20.2023; Maria H Murphy, 'Assessing the Implications of Schrems II for EU-US Data Flow' (2022) 71(1) ICLQ 245, 258–261 as well as – with a focus on standard contractual clauses (SCC) as coping mechanism – Anupam Chander, 'Is Data Localization a Solution for Schrems II?' (2020) 23(3) Journal of International Economic Law 771, 774.

6 Stacy-Ann Elvy, 'Paying for Privacy and the Personal Data Economy' (2017) 117(6) Colombia Law Review 1369; See also Moritz Hennemann and Lukas von Ditfurth, 'Datenintermediäre und Data Governance Act' (2022) NJW 1905, 1906–1907; Moritz Hennemann and Björn Steinrötter 'Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?' (2022) NJW 1481. See also the European Commission's strategy for data, European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data' (Brussels 19 February 2020) COM (2020) 66 final, 1–2, 6–8.

7 Cf Lemi Baruh, in this volume, at 105.

8 Cf ibid (as to USA and Turkey) and the cultural country reports Lena Kessel, 'Cultural Influences on Personal Data Disclosure Decisions' [2022] <https://ssrn.com/abstract=4068964> accessed 07.02.2023; Sarah Howe, 'Cultural Influences on Personal Data Disclosure Decisions – German Perspectives' [2022] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4134330> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Chinese Perspectives' [2022] <https://ssrn.com/abstract=4079624> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Japanese Perspectives' [2022] <https://ssrn.com/abstract=4079634> accessed 07.02.2023; Daniela Wawra, 'The Cultural Context of Personal Data Disclosure Decisions' [2022] <https://ssrn.com/abstract=4048250> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions – Brazilian Perspectives' [2022] <https://ssrn.com/abstract=4079617> accessed 07.02.2023; Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions – Russian Perspectives' [2022] <https://ssrn.com/abstract=4079628> accessed 07.02.2023.

ca)[9] do not focus so much and exclusively on individual privacy but rather on 'group privacy'[10]. Moreover, in societies in Asia[11] an individual's personality and status are more dependent on social affiliation, which means that individual anonymity is not so much valued as it is in the – so-called – West.[12]

Not having data protection laws or not having a particular expression for data protection in one's language does not mean that culture or legislation does not have a concept to balance private and other interests such as personal data and information. The question regards optimal and specific privacy, not maximum privacy,[13] or maximum data protection.

When it is said that 'privacy is universal'[14], this is, of course, true from a behavioral perspective: Every human being shows a need for privacy to some extent.[15] But this need varies and exists to a different degree depending on individual preferences and cultural backgrounds[16]. The need for privacy in this sense does not automatically equal an urge for a specific kind or level of privacy and data protection but rather a need for specific protection of one's need and against particular threats.

---

9 See only the debates by Patricia Boshe, Moritz Hennemann and Ricarda von Meding, 'African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward' (2022) 3(2) GPLR 56, 73–74; Alex B Makulilo, 'The Context of Data Privacy in Africa' in Alex B Makulilo (ed), *African Data Privacy Laws* (Issues in Privacy and Data Protection vol 33, 1st edn. Springer International Publishing 2017), 11–17.

10 Group privacy, though, has a double meaning. The term has been coined for anonymisation methods (cf Linnet Taylor, Luciano Floridi and Bart van der Sloot, *Group Privacy* (Springer 2017)) as they have been in Google's FLoC (Federated Learning of Cohorts) technology. In this contribution, group privacy means the protection of the data of a group of individuals.

11 Cf as to the situation in China and Japan, see Daniela Wawra, in this volume, at 51.

12 See especially regarding China, Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Chinese Perspectives' (2022) 22(09) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-09.pdf> accessed 07.02.2023, and to a lesser degree regarding Japan, Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions: Japanese Perspectives' (2022) 22(10) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-10.pdf> accessed 07.02.2023.

13 Jana Dombrowski, in this volume, at 89.

14 Ibid.

15 See only Alessandro Acquisti and Jens Grossklags, 'Privacy Attitudes and Privacy Behavior' in LJ Camp and Stephen Lewis (eds), *Economics of Information Security* (Advances in information security vol 12, Kluwer Acad. Publ 2004) 166 and from a legal point of view Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008) 2–4.

16 Kai von Lewinski, *Die Matrix des Datenschutzes* (Mohr Siebeck 2014) 22–23.

Examples vary depending on the context and perception of, for example, nudity amongst various cultures (eg, nudity at beaches, at saunas, or in workplace environments; perceptions of nudity in US television, at – primarily eastern – German naturist area beaches, mandatory wearing of burkas or hijabs, or culturally or religiously impacted nudity in various cultures) and experiencing shame (eg, in the form of feelings of embarrassment or failure).[17]

II Unilateral Data Protection Concept of the EU

EU regulation, namely the GDPR, does address the fact of different approaches towards data protection and privacy on an international level. It does so unilaterally since it defines (in a very broad manner) the scope of its own application (Art. 3 GDPR)[18] and it stipulates a differentiated set of provisions for the transfer of personal data to third countries (Articles 45 et seq. GDPR).

> This unilateral and one-sided approach can be called 'imperial'[19]. And it is no excuse from the history of transatlantic data economics bickering that the GDPR's approach primarily aims at the business practices of US internet giants. In that regard – it is true – that two 'data empires' are struggling, one armed with 'data business power', the other one with 'data protection power'. But the European data protection approach shall under no circumstances be reduced to the transatlantic relationship: Whereas in this constellation, fighting US 'data imperialism' with EU 'data protection imperialism' seems to be adequate, other and less strong countries and data economies have to surrender to one of these data (protection) powers (or even to both…).
>
> There are quite some examples from around the world to illustrate the effective influence of EU's data protection law model: In Ghanaian law, the Data Protection Act 2012 predates the GDPR and still reveals many similarities.[20] In Brazil, under the impression of the Cambridge Analytica scandal, the Lei Geral de Proteção de Dados (LGPD) was passed as a comprehensive

17 See with further references only ibid.

18 See also the discussion by Marian Thon, 'Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO' (2020) 84(1) Rabels Zeitschrift für ausländisches und internationales Privatrecht 24 passim.

19 Especially as to Africa, Cara Mannion, 'Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets' (2020) 53 Vanderbilt Journal of Transnational Law 685–711; from a more general perspective von Kai von Lewinski, *Medienrecht* (C.H. Beck 2020) ch 7 para 36.

20 See only Timo Hoffmann, 'Data Protection Act(ion): Report on the Law of Data Disclosure in Ghana' (2022) 22(01) University of Passau IRDG Research Paper Series 1–2 with further references <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/IRDG_Research_paper_Series_Country_Report_Ghana_Final.pdf> accessed 07.02.2023.

data protection law which is inspired by the GDPR.[21] The most imminent example of the GDPR's influence beyond the EU's borders can be seen in Switzerland, where the 'Brussels effect' demanded a GDPR-like amendment of the Swiss Federal Act on Data Protection.[22]

B Problem Setup and Solution Setup

The EU-US quarrels[23] about transatlantic data flows are only a manifestation of the problems of international law in the digital age: data is ubiquitous, whereas regulations are local. Digitalization, distributed cloud computing, and internet services are global phenomena; digital content and digitized personal data can be accessed from potentially everywhere. Moreover, effective regulation is only working at State-level or the level of a political union such as the European Union.

Focusing on digital content, an intuitive example stems from defamation law: A video with critical (political, religious, or graphical) content when uploaded to a website may be accessed – at least in theory, and in practice via VPN – worldwide. Thus, its content is spread in various States, including diverse cultural attitudes and sensitivities.[24]

---

21 See only Timo Hoffmann and Pietro LPdM Vargas, 'LGPD Et Al.: Report on the Law of Data Disclosure in Brazil' (2022) 22(06) University of Passau IRDG Research Paper Series 3–4 <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-06.pdf> accessed 07.20.2023; Danilo Doneda and Laura Schertel Mendes, 'A Profile of the new Brazilian General Data Protection Law' in Luca Belli and Olga Cavalli (eds), *Internet Governance and Regulations in Latin America: Analysis of infrastructure, privacy, cybersecurity and technological developments in honor of the tenth anniversary of the South School on Internet Governance* (1st edn, FGV Direito Rio 2019) 292–293 with further references.

22 See only Peer Sonnenberg and Timo Hoffmann, 'Data Protection Revisited: Report on the Law of Data Disclosure in Switzerland' (2022) 22(17) University of Passau IRDG Research Paper Series 1–3 <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22_17.pdf> accessed 07.02.2023; Moritz Hennemann, 'Schweizer Datenschutzrecht im Wettbewerb der Rechtsordnungen' in Boris P Paal, Dörte Poelzig and Oliver Fehrenbacher (eds), *Deutsches, Europäisches und vergleichendes Wirtschaftsrecht* (C.H. Beck 2021).

23 See with a focus on possible solutions, Theodore Christakis and Fabien Terpan, 'EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options' (2021) 11(2) International Data Privacy Law 81.

24 See only Sebastian J Kasper, 'Doctrinal Methods of Harmonisation in Defamation Law – A European Focus' (2023) forthcoming and with a focus on cultural heterogeneity on freedom of speech, blasphemy, and pornography Robert C Post, 'Cultural Heterogeneity and Law: Pornography, Blasphemy, and the First Amendment', (1988) 76(2) California Law Review 297.

I Congruency of Problem and Solution

It is a general rule for normative solutions and any regulatory concept that the level (or layer) of the problem shall not be higher (or larger) than its solution. This can be named the 'congruency of problem and solution'.[25]

II Three Concepts for Finding Solutions

A starting point and inspiration can be Wolfgang Friedmann's three levels of international law[26], which I have modified slightly. One can identify three general approaches in international data law to match the solution's size with the size of the problem: (1) universal law (= uplevelling the solution), (2) maintaining sovereignty (= downsizing the problem), or (3) conflict of laws (= connecting problem and solution through a network)[27].

1 Solution Concept #1: Universal Data Protection Law

The first – and, for globalist progressives, the most attractive – way would be uplevelling the solution. If one considers globalization a necessary consequence of digitalization[28], it seems reasonable to argue for a universal data protection law or a uniform concept of data protection or privacy[29] because, in that instance, we need not have to bother about a collision of data protection regimes because they would not materially collide.

---

25 With a focus on 'the appropriate levels of government and particularly within the European Union', the 'levels of government at which it is best to regulate' and the 'institutional design', see only Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation* (Oxford University Press 2011) 373-387.

26 Cf Wolfgang Friedmann, *The Changing Structure of International Law* (University Presses of California, Columbia and Princeton 1964) 60–71.

27 Kai von Lewinski, 'Nachhaltigkeit und Resilienz' in Hermann Hill and Veith Mehde, *Herausforderungen für das Verwaltungsrecht* (2023) forthcoming.

28 Cf Thomas L Friedman, *The World Is Flat: A Brief History of the Twenty-first Century* (1st edn, Farrar Straus & Giroux 2005).

29 For not on a global level but for the relation of federal and state level, cf Lothar Determann, in this volume, at 140.

At least a couple of concepts have been discussed in the past decades:

– Cyber Law Concept: Most prominently, this concept was argued for by *John Barlow*[30] of the Electronic Frontier Foundation (EFF) in 1996. It did not succeed in real life because a separated cyberspace does not exist; we simply have too many interconnections between the online and the offline world. From a more legal or political science perspective, one might add that whatever cyber law might contain, it does not have a democratic legislator[31].
– Lex Informatica: A similar concept is the lex informatica which was coined into the phrase that 'code is law' by *Lawrence Lessig*[32]. From a democratic perspective, it shows the same drawbacks as the cyber law concept. However, compared to the cyber law concept, it does exist in reality: Internet regulation is widely based on code; blockchain-based smart contracts, and cryptocurrencies are based on algorithms as well.
– Data Sphere Concept:[33] It is similar to the idea of cyberspace but focuses on data, not on chips and cables.

However: There is no such thing as a universal data law[34]. It is utopia. There is no hope for the (near) future that mankind will establish a universal set of rules for data, data protection and the internet – as it has not done so as to life, the universe or everything (else).

> This perspective does not ignore the achievements of the United Nations (UN), the World Trade Organization (WTO), or the United Nations Commission on International Trade Law (UNCITRAL) – to only name a few – but rather makes the point that we have not achieved harmonization in many fields of law and especially not in culture- and diversity-sensitive fields like personality rights.[35] Significant achievements have been reached in regards to tech-

30 John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (EFF, 8 February 1996) <https://www.eff.org/cyberspace-independence> accessed 07.02.2023.

31 But this is not opposed to a widespread notion of Internet activists who claim to 'believe in rough consensus and running code' and to 'reject kings, presidents and voting' (IETF motto, usually attributed to Dave Clark 1992).

32 Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 2000); Lawrence Lessig, *Code and Other Laws of Cyberspace, Version 2.0* (Basic Books 2006).

33 Jean–Sylvestre Bergé and Stephane Grumbach, 'La sphère des données et le droit: nouvel espace, nouveaux rapports aux territoires' (2016) Journal du droit international (JDI-Clunet) 1153–1173.

34 Cf von Lewinski (n 19) ch 4 para 15 (in a media law context).

35 A different, yet related, aspect regards the realization of socio-economic rights and their justiciability. Whereas some States understand social-economic rights, – which, according to the International Covenant on Economic, Social and Cultural Rights (ICESCR) include, *inter alia,* a right to work, fair working conditions, social security, recognition of family, maternal, and children's rights,

nical questions, such as (ITU) rules on the distribution of transmission frequencies, (international) postal service, and civil aviation.

2 Solution Concept #2: Data Sovereignty

The second approach is not to uplevel the solution but to downsize the problem. The level where political solutions are usually found is … state level. This approach is pursued with great consistency in North Korea, with great consequence *and* success in China,[36] and with notably less consequence and success in Russia[37].

This downsizing approach means a restriction of the respective digital sphere to a State's own borders; the respective regulation does not collide with other jurisdictions anymore because the digital content and data does not leave the country. Nationalizing the internet (so-called 'splinternet'[38] with subnetworks such as Russia's 'Runet' and Iran's 'Halal Internet') addresses the problems of transnational data flows and transnational regulation by cutting off transnational links. As

---

a right to an adequate standard of living, housing, clothing, education, and cultural life, – as justiciable, others deny such a standard, and again others consider only some minimum standards enforceable by courts. Even if such rights might be seen as justiciable, at least in principle, the question remains how the power of the judiciary and the legislative are (fairly) divided considering the idea of progressive realization of such rights. On the history of socio-economic rights and the ICESCR in general, see only Eibe Riedel, 'International Covenant on Economic, Social and Cultural Rights (1966) (April 2011)' in Anne Peters and Rüdiger Wolfrum (eds), *Max Planck Encyclopedia of Public International Law* (online. Oxford University Press 2022) paras 2–3, 5, and with a focus on 'western' views on socio-economic rights, see Daniel J Whelan and Jack Donnelly, 'The West, Economic and Social Rights, and the Global Human Rights Regime: Setting the Record Straight' (2007) 29(4) Human Rights Quarterly 908. On the justiciability of socio-economic rights in the EU, see only Oliver Gerstenberg, 'The Justiciability of Socio-economic Rights, European Solidarity, and the Role of the Court of Justice of the EU' (2014) 33(1) Yearbook of European Law 245. On the German approaches towards (social) participation rights and benefit entitlements (Teilhabe- und Leistungsrechte), see only Thorsten Kingreen and Ralf Poscher, *Grundrechte. Staatsrecht II:* (Schwerpunkte Pflichtfach, 35 edn, CF Müller 2019) ch 4 paras 155–162.

36 See only Sarah L Hünting, 'Endeavour to Contain Chinas' Tech Giants – Country Report on China' (2022) 22(15) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22_15.pdf> accessed 07.02.2023. See also China's fines imposed on Didi Global, Paul Mozur and John Liu, 'China Fines Didi $1.2 Billion as Crackdown on Tech Sector Continues' *The New York Times* (22 July 2022) B1.

37 See only Elisabeth Saponchik, 'Digital Citadel: Country Report on Russia' (2022) 22(13) University of Passau IRDG Research Paper Series <https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/institute/irdg/Research_Paper_Series/22-13.pdf> accessed 07.02.2023.

38 The German iteration of the splinternet would be called 'Schlandnetz'.

such, this data sovereignty approach works: We have not heard any complaints about data protection violations of North Korean citizens in the US....

The downside of this approach is obvious for open-minded Westerners. Restricting cross-border exchange of content, ideas, and the like is not very much the trademark of an open – let alone democratic – society.

3 Solution Concept #3: Conflict of Laws

If the uplevelling approach is too utopian and the downsizing approach is too unattractive, we have – as a third option – to accept that the problem's level is higher than the solution's level. This does not mean surrendering to the issue at hand. Instead, we have to coordinate the different solutions amongst various jurisdictions; metaphorically speaking one has to sew a patchwork quilt from the different regulatory regimes to bring the solution level up to the level of the problem. This constellation (and its solution) is termed 'conflicts of laws'.

A conflict, or collision, of laws appears if a case has links to more than only one jurisdiction. And if (at least) two jurisdictions apply to the same case, they collide. Sometimes with only little effect and difference, usually the differences will result in different results, and this is a conflict.

> Conflicts of law' is an ancient concept, dating back to the merchant law between Greek póleis (πόλεις) and the Romans. The course of history can be briefly outlined with the following keywords[39]: Starting with the effective protection of foreigners by a 'proxenos'[40], even 'barbarians' gained legal status by applying the (ancient) *ius gentium* to Non-Romans. During the early Migration Period, the principle of personality ('*Personalitätsprinzip*') became predominant; when the Germanic migrants settled, this transformed into a principle of territoriality ('*Territorialitätsprinzip*').[41] Methodologically, from the 14th century, the so-called statute doctrines have prevailed in Europe[42]. The foundations of today's modern conflict of laws doctrine were laid in the 19th century and are commonly associated with the name of F.C. von Savigny.[43]

39 Cf Max Gutzwiller, *Geschichte des internationalen Privatrechts. Von den Anfängen bis zu den großen Privatrechtskodifikationen* (Helbing & Lichtenhahn 1977).

40 The ancient Greek term 'πρόξενος' means 'instead of a foreigner'; it is still present in today's legal language as 'proxy'.

41 Otto Brunner, *Land und Herrschaft* (5th edn, Duncker & Humblot 1965) 188.

42 In detail Günter Hermann, *Johan Nikolaus Hert und die deutsche Statutenlehre* (Neue Kölner rechtswissenschaftliche Abhandlungen 1963) 3-31.

43 Paul Heinrich Neuhaus, 'Savigny und die Rechtsfindung aus der Natur der Sache' (1949) 15 Rabels Zeitschrift für ausländisches und internationales Privatrecht 364-381.

Conflict of law provisions provide a set of rules to decide which jurisdiction's laws shall apply to a certain case if a case has connections to more than one jurisdiction. Although the conflict of law legislation is national, at least in Europe it is largely harmonized in most constellations.

C Data Protection as a Conflict of Law Constellation

Given the different concepts in data protection around the world, given the absence of a universal data protection law and since a Great Firewall of Europe is not feasible and not desirable, international data transfer is a matter of conflict of laws. In this context, it is no argument that the GDPR does not (explicitly) regulate this topic; it does not mean that there is no data protection conflict of laws.

This blind spot of the GDPR – be it imperial, be it naïve, be it ignorant – has to be looked at by practitioners and academics alike. And here, we see a combination of undercomplexity and overcomplexity: It is undercomplex because the current conflict of laws regime, ie, private international law and private international law relating to civil procedure, does mainly address private law cases, whereas the data protection regime of the GDPR also includes administrative law instruments to a large extent (I.). It is overcomplex because traditional private international law criteria for establishing a 'connex', ie, the so-called connecting factors[44], do not adequately fit for data protection cases (nor do they fit for digital cases in general) (II.). And it is simultaneously over- and undercomplex because the numerous connecting factors fog and dazzle the (so-called) genuine link (III.).

I Data Protection is not only (Procedural and Material International) Private Law

Conflicts of law are, in practice as well as from the ivory tower, mainly discussed as questions of *private* international law, both in terms of materially applicable law and procedurally competent jurisdiction. From a (medium high-flying) academic perspective, this restricted focus is quite understandable because, in a public law context, the precise line of conflict of law is the borderline between two states;

44 See only Heinz-Peter Mansel, 'Connecting factor' in: Jürgen Basedow, Giesela Rühl, Franco Ferrari und Pedro de Miguel Asensio (eds), *Encyclopedia of Private International Law* (Edward Elgar Publishing 2017) 441.

the exercise of power is in principle only allowed within a State's own territory, unless a State permits another State to exercise such power within its territory. Conflicting public law jurisdictions are therefore not the question of conflict of law rules but rather a question of war.

> There are, however, examples that demonstrate that – with a State's consent – another State may exercise power on that State's territory. As such, nine European States have ratified a treaty that – reciprocally – allows for the formal service of an administrative act on their territories.[45] Similarly, States sometimes invite foreign police or military forces into their territory for various reasons.

However, many States also entrust their (public) administration with issuing sanctions or regulating in the sphere of data protection.[46] In that regard, it cannot be denied that administrative actions might have *(de facto)* effects beyond a State's own territory (multi-national merger authorizations can at least *de facto* have an extraterritorial dimension; the same applies regarding an order to install age-verification systems in an internet adult entertainment system[47]). Otherwise, the legislation respectively the regulations would be categorically hindered from addressing such international cases by means of public / administrative law. Thus, the international administrative law dimension has to be added if we talk

45 Eg according to the European Convention on the Service Abroad of Documents relating to Administrative Matters 24 November 1977, ETS No 94, entered into force 01 November 1982.

46 See only the legal country reports Timo Hoffmann and Pietro Luigi Pietrobon de Moraes Vargas, 'LGPD Et Al.: Report on the Law of Data Disclosure in Brazil' [2022] 49 <https://ssrn.com/abstract=4082390> accessed 07.02.2023; Timo Hoffmann, 'Data Protection Act(ion): Report on the Law of Data Disclosure in Ghana' [2022] 18 <https://ssrn.com/abstract=4037928> accessed 07.02.2023; Timo Hoffmann, 'Data Protection by Definition – Report on the Law of Data Disclosure in Japan' [2022] 29 <https://dx.doi.org/10.2139/ssrn.4055510> accessed 07.02.2023; Sarah L Hünting, 'Endeavour to Contain Chinas' Tech Giants: Report on China' [2022] 33 – 34 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4198256> accessed 07.02.2023; Benedikt Leven, 'Land of the Free - Legal Country Report on the United States of America' [2022] 35 <https://ssrn.com/abstract=4079640> accessed 07.02.2023; Kai von Lewinski, 'Informational Gold Standard and Digital Tare Weight - Country Report on Data Disclosure in the European Union' [2022] 13 – 14 <https://ssrn.com/abstract=4068987> accessed 07.02.2023; Elisabeth Saponchik, 'Digital Citadel: Country Report on Russia' [2022] 21 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4134322> accessed 07.02.2023; Peer Sonnenberg and Timo Hoffmann, 'Data Protection Revisited: Report on the Law of Data Disclosure in Switzerland' [2022] 54 – 55 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4198277> accessed 07.02.2023.

47 Xhamsters vs. LMedienA NRW, OVG Nordrhein-Westfalen, Order of 07.09.2022, 13 B 1911/21 and others, arguing for restrictive blocking orders amid the existing geo-location technology; John Quinn 'Geo-location technology: restricting access to online content without illegitimate extraterritorial effects' 11(3) International Data Privacy, passim.

about conflict of law regimes in the data protection context[48]. (And we probably have to add an international criminal law dimension as well – just consider *ne bis in idem* with regard to data protection sanctions!)

Consequently, one has to look at the dimensions of material law, procedure and enforcement not only with regards to civil but also public law despite the fact that laws regulating procedure and enforcement are of a public law nature.

> When focusing on arbitration and mediation, at least procedural aspects are often left for the parties to determine which would also justify categorizing them as private law. However, enforcement of such settlements in accordance with their national laws remains for the States to guarantee.[49]

II Connecting Factors

Commonly, five connecting factors are recognized in a (private) collision of law context: territoriality, passive personality, active personality (nationality), protective principle, and universality.[50] Neither of them does sufficiently apply in data protection cases (let alone digital cases in general).

1 Universality

To start with the first (and to exclude it from a data protection context from the outset): universality. Some issues are so universal that they give good cause to allow for jurisdiction in every place on Earth.

> Universality as a connecting factor is not disputed in principle, but rather it is disputed whether a principle is universal... Consequently, cultural differences in the field of data protection can complicate or make impossible any agreement on the universality principle.

---

48 Marian Thon, 'Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO' (2020) 84 Rabels Zeitschrift für ausländisches und internationales Privatrecht 24, 29 calls this 'Zweispurigkeit' ('two lanes') of conflicts of law which can especially be observed in data protection law constellations.

49 This is also evidenced by the international conventions on enforcement of arbitration awards and mediation settlements, see Convention on the Recognition and Enforcement of Foreign Arbitral Awards (entered into force 07 June 1959) 330 UNTS 3; United Nations Convention on International Settlement Agreements Resulting from Mediation (entered into force 12 September 2020); UN General Assembly Resolution of 20 December 2018, A/RES/73/198.

50 See in general on connecting factors only Mansel (n 44) 441-452.

> Should every State, however, choose its own connecting factor and apply it universally, this could lead to obstacles in enforcement proceedings.

However, data protection (in the EU's and in the GDPR's meaning) is – as was already mentioned above – far from being a universal concept. This can be demonstrated by the famous distinction between the European dignity-based approach and the Anglo-Saxon freedom-based approach to data protection and privacy.[51]

And even if we had a common understanding of data protection in the West, it would be far from globally accepted. Asian and African cultures are said to be more community-based and less individualistic which is why they might consider Western data protection concepts – the same goes for privacy concepts – as cultural imperialism (or even worse). It has been shown in the cultural science sections of the bidt project 'Vectors of Data Disclosure'[52] that privacy and data protection are valued differently and with different preferences around the world – at least with regard to the eight countries that are in the bidt study's focus. This can very broadly (and with a Eurocentric twist) be illustrated by the juxtaposition of Western individualism and (more) collective concepts elsewhere, especially in Asia and Africa.[53]

Since perceptions of data protection and privacy are diverse around the globe, it can easily be expected that the connecting factor of universality would be met with reluctance by many States.

2 Territoriality

If universality as a connecting factor does not fit, one might want to turn to territoriality. But territoriality just does not fit for digital cases either. Because of the ubiquity of modern data transfers in the cloud age, it is difficult to localize data processing and data storage. And even if one succeeds in localizing such a case, it is very likely that the connecting factor points equally to all jurisdictions concerned because of distributed IT infrastructure. This would, then again, not result in a sensible data protection collisions of laws regime…

---

51 Robert C Post, 'Three Concepts of Privacy' (2001) 89 Georgia Law Journal 2087; James Q Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 Yale Law Journal 1151.

52 Cf Daniela Wawra, in this volume, at 51 and 169.

53 For detailed figures as to informational privacy preferences see Wawra, in this volume, at 51.

3 (Active or Passive) Personality

A third (and fourth) connecting factor is personality. Personality links to the nationality of the person (or entity) that is harmed (passive personality) or it links to the nationality of the tortfeasor (active personality).

At first glance, this seems to be a clear point for the EU interpretation, especially regarding Art. 3(2) GDPR: Third country internet companies violate basic informational rights of EU inhabitants. But: It is another valid interpretation that EU data protection legislation restricts the entrepreneurial freedom of third countries' companies.

Thus, personality as a connecting factor does not give clear guidance for conflict of laws constellations. This holds when envisaging that harm can occur in more than one jurisdiction; a comparable situation exists in defamation cases.[54] Therefore, the aggrieved party may have an interest to bring claims in more than one jurisdiction (the so-called 'mosaic approach' confines these respective claims to the damage caused in that particular State).[55]

4 Protective Principle

The last connecting factor is called 'protective' so that a State can claim jurisdiction over cases in which national security interests are affected. It is related to the legal concept of the *ordre public*.

> Security aspects are prominent in the PNR constellation, but they are inherent to every data constellation (cf US CLOUD Act).

Again, we face the problem of different attitudes and concepts of data protection and privacy. In some jurisdictions, the processing of personal data is regarded to be a (potential) tort (eg, in the EU), in other places of the world it is rather the exercise of (entrepreneurial) freedoms by the data processor.

---

54 See only Matthias Lehmann and others, 'Special Jurisdiction' in Andrew Dickinson, Eva Lein and Andrew James (eds), *The Brussels I regulation recast* (1st edn, Oxford University Press 2015) para 4.110.

55 Ibid para 4.111.

III Finding the Genuine Link

If a case has links to more than one legal system or regulatory regime, *inter alia*, legal certainty (for the tortfeasor and the aggravated person), reduction of legal costs, and aspects of efficiency may call for establishing only one clear link to a single jurisdiction. The idea underlying that one link is that there is a so-called 'genuine link' that demonstrates the closest, most natural, and foreseeable connection to one jurisdiction. That 'genuine link' shall then determine the applicable law to decide the case at hand.

> When considering that different jurisdictions have been built on different cultural backgrounds and legally protected rights (may) have been balanced differently in different States, States may have an interest to maintain jurisdiction over a case – at least for their citizens – although there might be a 'closer' link to another jurisdiction.
> In most cases, the starting point is territoriality (domicile) or personality (citizenship), but it can as well be the mutual choice of law, the marketplace, the place of infringement, or the place of protection.

The problem is not to find a link (there are plenty and every person asked might make a case for one of them) but to find the genuine one. And that is difficult because an identical provision might have to be categorized differently in different countries.

> To give an example: The processing of customer data beyond the purpose of a contract might constitute a breach of contract in the US, a violation of an (absolute) personality right and regulatory law ('*Ordnungsrecht*') in the EU and Germany, perhaps the disregard of trade regulations in China, and in a transnational commercial law context it is the non-compliance with business standards. – And that is exactly what the prominent row between the US and the EU about the transfer of personal data across the Atlantic is about: The data subject sits in the EU, and the (data) controller resides in the US. This is a classic constellation in conflicts of law; classic insofar as it cannot be clearly decided on the grounds of the genuine link doctrine.

IV Conflicting and Confusing Conflict of Law Regimes

In view of the deficits of conventional conflict of laws for data protection cases one has two options now: shrugging shoulders or scratching the head: Shrugging the shoulders would mean to say: 'Okay, it is a kind of imperial deadlock of data superpowers. There is nothing I can do about it. The world is complicated. And: It is not that bad.' Or one could scratch one's head and start thinking further about a solution.

D Holistic Approach(es) to Data Protection Conflicts of Law

And the solution that we are thinking about and researching on in the bidt project is whether holistic approaches might help to overcome the deadlock of traditional concepts to solve conflicts of law. Here, we follow a two-step approach:

- As a first step, we have analyzed data protection legislation from around the world. This analysis was meant as a full-take. We did not only want to identify the regulations which correspond to GDPR provisions. Instead, we took off our GDPR glasses to avoid a GDPR bias and chose a matrix approach (I.).
- The second step will follow when we analyze the interdependencies of the elements of our matrix. We want to find out whether different data protection regimes exist and how different they are (II.). If different types exist, we will try to find out whether some of them can be categorized. Subsequently, we will assess whether they can nevertheless be compared.
- And hopefully, this will result in new insights into how to determine the level of data protection and privacy in different cultures and across legislations (III.).

I Matrix Approach

The idea of the matrix[56] was not so much inspired by the 1999 movie but by anecdotes by US-Americans who were wondering why Europeans boast so much about 'their' data protection and the GDPR but, at the same time, do not worry about having obligatory civil registers, identity cards, and national identification numbers. – Obviously, different perspectives on privacy and data protection exist…

1 The Idea of the Matrix

The idea of the matrix approach we take in the bidt project was born by the wish to broaden the perspective. Consequently, we expanded our analysis grid from only private law (which is the classic conflicts of laws perspective) to the other fields of law, namely administrative law and criminal law, perhaps additionally economic and competition law. And we have added additional dimensions to the (traditional)

56 Cf Timo Hoffmann, in this volume, at 1.

level of material law: the level of procedure and the one of enforcement. – This forms a matrix of three times three or four elements, respectively:

	Private Law	Administrative Law	Criminal Law	Economic/Competition Law
Material Law				
Procedure				
Enforcement				

2 The Value of the Matrix: Regulatory Heatmap

The matrix is not for display only. It is thought to be a tool for the use of comparing legal systems and finding the key to solving conflicts of law conflicts and perhaps even a solution for the EU–US lockup described above.

The first thing we are aiming at is a deeper understanding of the structure of data protection or privacy regulation, respectively, in particular legislations.

> We are working under the assumption that European data protection law very much emphasizes material law and procedure in a private law context, which is compensated by a significant or even structural enforcement deficit. On the other side (of the Atlantic), in the US, no comprehensive privacy provisions exist.[57] But if the existing (sectoral) provisions become enforced (for example, by the FTC), this is often more effective than in the EU. This constellation is often referred to as the difference between 'law in the books' and 'law on the ground'[58]. Another blind spot of the EU's GDPR is that its data protection law focuses on the data subject and the data controller, not addressing the interests, rights and freedoms of third parties and the (general) public[59] in a working data environment (cf now the coming EU Data Act which does not modify the GDPR's application).[60]

This helps us to understand why conflicting parties – such as the US and the EU – do not come to a working agreement when they focus on different aspects of data protection and privacy safeguards. One can see these difficulties best when he looks at the current state of negotiations concerning the upcoming 'Trans-Atlantic

57 With a focus on the Californian law, cf Determann, in this volume, at 121.
58 Cf Kenneth A Bamberger and Deirdre K Mulligan, *Privacy on the ground* (MIT Press 2015).
59 Notably, more recent legal acts and respective proposals have chosen a less individualistic approach, eg, the EU Data Act (DA), the EU Data Governance Act (DGA), the EU Digital Markets Act (DMA), the EU Digital Services Act (DSA), and the EU Artificial Intelligence Act (AIA).
60 Cf Hennemann and Steinrötter (n 6).

Data Privacy Framework'.[61] US-President Joseph Biden has just recently signed an Executive Order[62] which aims to appease European criticism of the level of protection of EU data in the USA and to build a basis for a future agreement between the two countries. Whether this Executive order will meet the high requirements for EU adequacy of both, the European Commission and the CJEU, still remains questionable; especially in the topics of proportionality of mass surveillance and adequate legal protection before an independent court.

II Regime Comparison as an Academic Model

With these insights, we want to develop a method (or methodology) to compare data protection and privacy regulation regimes around the world. Our aim is to overcome the quite simple equitation of the European Union (namely: of the European Court of Justice), which is not prepared to recognize an adequate level of data protection in a third country if it is not modelled closely to the GDPR. Its attitude is rather undercomplex when it says (or thinks): 'Well, it does not read like the GDPR, so it cannot be adequate.'

This broader perspective has been inspired by Art. 45 GDPR and the European Commission (*and* has been disappointed by the European Court of Justice). Further inspiration stem from Gunther Teubner and Andreas Fischer-Lescano and their work on '*Regime-Kollisionen*' ('Regime Collisions')[63], who take a *Systemtheorie* approach itself. The works of Hannah L. Buxbaum[64] regarding the comparison of regulatory law provisions will deepen our understanding in this field.

Research questions which we have to address in the further course of our bidt project are, *inter alia*, the following: What role does a certain rank of a data protection legal system or privacy regime (constitutional value or mere business law) play? Do (too) holistic regime comparisons serve as a reasonable connecting factor? Do we have to broaden our perspective to (cultural) comparison to include cultural, social, political, economic, and technological factors as well.[65]

---

61 European Commission, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' (2022) <https://ec.europa.eu/commission/presscorner/detail/nl/ip_22_2087> accessed 07.02.2023.

62 Executive Order 14086 of 7 October 2022 <https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf> accessed 07.02.2023.

63 Günther Teubner and Andreas Fischer-Lescano, *Regime-Kollisionen* (Suhrkamp 2006).

64 Hannah Buxbaum, 'Public Regulation and Private Enforcement in a Global Economy: Strategies for Managing Conflict' (2019) 399 Recueil des Cours.

65 Baruh, in this volume, at 105.

III Practical Outcome?

What do we hope to achieve besides scientific progress? What are the insights for data protection practice?

1 Mapping Conflicts

With a deeper understanding of the different and differing structures of data protection and data privacy law, it might be possible to find adequate jurisdiction to adjudicate a case. As such, the 'matrix' may be used as a tool by data practitioners and data protection advocates for the assessment of litigation risks as well as for data protection impact assessments (DPIA). Even political decision-makers might find it useful to understand why some countries adopt GDPR-style regulations easier than others:

> An example might be Australia's revision of its Privacy Act: It aims more at an interoperability with the GDPR, but does not reach for adequacy[66] because Australia does not have a significant data industry and wants to stay with their legal (common law) traditions.

2 Predicting Adequacy Decisions

A more holistic approach towards data protection regime comparison might help to recognize more (and different) legislations in the context of adequacy decisions under Articles 44 et seq GDPR. Perhaps such adequacies can be reached without copying the GDPR but rather maintaining the respective cultural approach to privacy protection.[67] (Originally, the European Commission had thought of a broad palette of legal traditions to be considered adequate.[68])

E Summary

If not only Brussels, but the entire EU were a spaceship, then we might be travelling well with our regulations. But because we are not alone on the planet, the ubiquity of data protection issues means that the international dimension must

66 Normann Witzleb, in this volume, at 147, 157.

67 Moritz Hennemann, 'Wettbewerb der Datenschutzrechtsordnungen' (2020) 84 Rabels Zeitschrift für ausländisches und internationales Privatrecht 864.

68 European Commission, COM (2017) 7.

be taken into account. The EU does not do this, perhaps because it feels strong enough in terms of economic policy and morally superior. But this blind spot will cause us a lot of trouble in the future. If we are not strong enough and rely only on being on the right side of the history of data protection law, we may end up as the 'Global East' of the digital age[69] – ideologically in possession of the truth, accompanied by a handful of satellite States, but separated from the rest of the world by an iron curtain of our data protection doctrine.

69 Similar conclusion for the European AI regulation Kai von Lewinski, 'Kollisionsrechtliche Fragen an die Nachvollziehbarkeit und Überprüfbarkeit von KI-Systemen' in Frauke Rostalski (ed), *Deutschland und Europa auf dem Weg zu einer Regulierung von nachhaltiger Künstlicher Intelligenz* (Tagungsband der Verbraucherrechtstagung 2023) 295, 314.