

The Problem of Control in Data Protection Law

Joshua Hovsha

Thesis Submitted for the Degree of PhD in Law at
Trinity College Dublin, 2024

I declare that this thesis has not been submitted as an exercise for a degree at this or any other university and it is entirely my own work. I agree to deposit this thesis in the University's open access institutional repository or allow the Library to do so on my behalf, subject to Irish Copyright Legislation and Trinity College Library conditions of use and acknowledgement.

I consent to the examiner retaining a copy of the thesis beyond the examining period, should they so wish (EU GDPR May 2018).



Joshua Hovsha

06.11.2024



The research for this thesis was made possible through funding from the European Union's Horizon 2020 research and innovation programme under Marie Skłodowska-Curie grant agreement No 812 497.

'We have a private life and hold it infinitely the dearest of our possessions'

Virginia Woolf, Montaigne, The Common Reader, 1925

*To Cécile, for making every word of this possible and giving me so much to safeguard
dearly.*

*For Xavier, may the beauty of this world guide you far and may you always know that
you have a home and sanctuary waiting for you.*

Table of Contents

Acknowledgments	i
List of Abbreviations	iii
Table of Cases	v
Table of Legislation	xiv
List of Tables	xxi
List of Figures	xxi
Chapter One: Introduction	1
1. Background.....	1
2. Problem Statement: ‘ <i>The Problem of Control</i> ’ in EU Data Protection Law.....	3
3. Research Questions	7
4. Structure and Methodology.....	9
5. Limitations of this Study	18
PART I: STATE OF THE ART.....	21
Chapter Two: The Foundations of Data Protection	23
1. Introduction.....	23
2. From Privacy to Data Protection	24
3. The Emergence of Data Protection	34
4. Conceptual Foundations	41
5. The ‘Essence’ of Data Protection.....	53
6. The Relationship Between Privacy and Data Protection.....	62
7. Conclusion	69
Chapter Three: Data Protection’s Nature and Ambitions	75
1. Introduction	75
2. Context of the GDPR: The Need for New Legislation	76
3. The Ambitions of the EU Data Protection Regime	77

4. Data Protection: Individual Control v Societal Protection	82
5. Conclusion	93
Chapter Four: Key Elements of the Data Protection Regime	97
1. Introduction	97
2. Key Definitions	98
3. Actors and Accountability	103
4. Scope of Application	108
5. Data Protection Principles	113
6. Risk Assessment	119
7. Regulators and Supervision	123
8. Liability under the GDPR	127
9. Conclusion	130
Chapter Five: An Expanding Regime	133
1. Introduction	133
2. Legislative Expansion	134
3. Judicial Expansion	163
4. Conclusion	172
PART II: THE PROBLEM OF CONTROL	175
Chapter Six: The Problem of Control - History and Case Law	177
1. Introduction	177
2. Controller Based Accountability: Historical Origins	179
3. Advancing Models and Challenges to Controllership	185
4. Complete and Effective Protection	187
5. CJEU Decision in <i>Wirtschaftsakademie</i>	190
6. CJEU Decision in <i>Jehovan todistajat</i>	193
7. CJEU Decision in <i>Fashion ID</i>	195

8.	CJEU Decision in <i>NVSC</i>	200
9.	CJEU Decision in <i>Belgian State</i>	203
10.	CJEU Decision in <i>IAB Europe</i>	206
11.	Conclusion	209
Chapter Seven: The Consequences of the Problem of Control		213
1.	Introduction	213
2.	Framing and Linguistic Problems	214
3.	Diminishing Legal Certainty	216
4.	Undermining Consent and Transparency	223
5.	Weakening Individual Control and Obscuring Data Commodification	227
6.	Impact on ‘Complete and Effective Protection’	229
7.	Conclusion	235
Chapter Eight: The Disappearing Sanctuary of the Home		241
1.	Introduction	241
2.	The Home in Law	242
3.	The Smart Home Reversal	246
4.	The Impact of Smart Home Devices	249
5.	The Smart Home: Roles and Expectations	252
6.	The Disappearing Household Exemption	255
7.	Conclusion	260
Chapter Nine: AI Services and the Limits of the Control Model		262
1.	Introduction	262
2.	Defining AI	266
3.	The Challenge of AI Data Harvesting	269
4.	AI Service Types	272
5.	Actors within AI Processing Chains	273

6.	Stages of AI Service Provision	274
7.	Roles and Accountability in AI Services	279
8.	The Increasing Complexity of AI Service Processing Chains	283
9.	Complementing and Competing Obligations	286
10.	Conclusion.....	289
PART III: RECOMMENDATIONS AND CONCLUSION.....		291
Chapter Ten: Addressing the Problem of Control.....		293
1.	Introduction.....	293
2.	Extended Responsibilities for Processors	294
3.	Non-Controller Based Accountability.....	297
4.	Moving to a Model of Control as Orchestration	301
5.	Flexibility in Judicial and Regulatory Action	303
6.	Towards a Taxonomy of Control in Data Processing Relationships.....	308
7.	The Taxonomy	309
8.	Conclusion	341
Chapter Eleven: Conclusion.....		345
1.	Research Problem.....	345
2.	The Rise of Data Protection Law	346
3.	The Nature and Ambitions of the Data Protection Regime	347
4.	An Expanding Regime	349
5.	The Problem of Control.....	351
6.	Domains Where the Problem Manifests	354
7.	Complete and Effective Protection	359
8.	Potential Solutions.....	362
9.	Further Research	364
Bibliography.....		369

Acknowledgments

Dear Pat, You came upon me carving some kind of little figure out of wood and you said, "Why don't you make something for me?" I asked you what you wanted, and you said, "A box". "What for?" "To put things in." "What things?" "Whatever you have," you said. Well, here's your box. Nearly everything I have is in it, and it is not full. Pain and excitement are in it, and feeling good or bad and evil thoughts and good thoughts—the pleasure of design and some despair and the indescribable joy of creation. And on top of these are all the gratitude and love I have for you. And still the box is not full. JOHN

John Steinbeck, East of Eden

This is a work that has been made full through the unending kindness of so many.

To my supervisor Eoin O'Dell whose guidance began while I was still in South Africa. Thank you for your support in all matters, for boundless insight, and unending hours of fascinating conversation. To Dave Lewis, whose PROTECT project at the ADAPT Centre Trinity College Dublin made this research possible. But even more than this, whose empathy, advice, and boundless knowledge led the path forward.

My gratitude goes also to the members of my examination jury, Róisín Costello and Orla Lynskey for their time, discussion, comments, and suggestions. This work has been brought to a new level through their input.

This work would not have been possible without the generous support of the European Commission's Marie-Skłodowska-Curie action, the PROTECT Project, and Science Foundation Ireland.

To Maria Grazia Porcedda and David Fennelly who were so much more generous with their guidance, input and wisdom than could ever have been asked. To Kelley McCabe, Jessie Greene, and Valerie De Moor you have moved heaven and earth for so many of us and we are so very grateful.

Particular thanks are owed to David Prendergast, Harsh Pandit, Surya Roy, Oran Doyle, Katherine O’Keefe, and Daragh O’Brien for their comments, advice, and keen interest in this research as it has evolved.

To my friends from afar who have patiently read far too much about Data Protection Law. Most especially Daniella Hovsha, Dovi Brom, Kevin Levy, James Lomberg, and Bianca Shulman, thank you for your generosity of spirit and insight.

To my mother Rolene and sister Dani, for their love, support, and passion for even the driest of subjects if that is what I am pursuing.

Most of all to you Cécile, who has driven me forward with love, understanding, compassion, and humour.

List of Abbreviations

AG – Attorney General

AI – Artificial Intelligence

AI Act – The Artificial Intelligence Act (EU)

AIaaS – Artificial Intelligence as a Service

AI-HLEG – The European Commission’s High-Level Expert Group on Artificial Intelligence

API – Application Programming Interface

AWS – Amazon Web Services

CCPA – The California Consumer Privacy Act (California)

Charter – Charter of Fundamental Rights of the EU

CIL – Commission on Informatics and Liberties (France)

CNIL – National Committee on Informatics and Liberties (France)

COPPA – Children's Online Privacy Protection Act (USA)

CPRA – California Privacy Rights Act (California)

DGA – Data Governance Act (EU)

DIB – Data Inspection Board (Sweden)

DL – Deep Learning

DMA – The Digital Markets Act (EU)

DPA – Data Protection Authorities, the data protection supervisory authorities established throughout EU member states.

DPC – The Data Protection Commission (Ireland)

DPIA – Data Protection Impact Assessment

DSA – The Digital Services Act (EU)

ECHR – The European Convention on Human Rights (Council of Europe)

ECommHR – European Commission of Human Rights

ECtHR – The European Court of Human Rights (Council of Europe)

EDPB – The European Data Protection Board

EDPS – The European Data Protection Supervisor

EEA – The European Economic Area

FIPPs – Fair Information Processing Principles

FLOPs – Floating Point Operations

FRIA – Fundamental Rights Impact Assessment

FTC – Federal Trade Commission (United States)

GDPR – The General Data Protection Regulation (EU)

GPDP – Data Protection Authority (Italy)

Convention 108 – The Convention for the protection of individuals with regard to automatic processing of personal data (Council of Europe)

Hessian DPC – Data Protection Commissioner (German State of Hesse)

IaaS – Infrastructure as a Service

ICCPR – International Covenant on Civil and Political Rights (United Nations)

ICTs – Information and Communication Technologies

ISP – Internet Service Provider

LIFL – Law on Informatics, Files and Liberties of 1978 (France)

LLM – Large Language Models

ML – Machine Learning

NIST – National Institute of Standards and Technology (US Department of Commerce)

OECD – Organisation for Economic Co-operation and Development

OECD Guidelines – The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

OSK – Committee on Publicity and Secrecy Legislation (Sweden)

PaaS – Platform as a Service

ROPA – Record of Processing Activities

SA – Supervisory Authority

SaaS – Software as a Service

TCF – Transparency and Consent Framework

TC String – Transparency and Consent String

TEU – Treaty on the European Union (EU)

TFEU – Treaty on the Functioning of the European Union (EU)

UDHR – Universal Declaration of Human Rights (UN)

WP29 – The Article 29 Working Party

Table of Cases

Court of Justice of the European Union ('CJEU')

A, B, and C

Joined Cases C-148/13 to C-150/13 [2014] EU:C:2014:2406

Åklagaren v Hans Åkerberg Fransson

Case C-617/10 [2013] EU:C:2013:105

Bara v Presedintele Casei Nationale De Asigurari De Sanatate (CNAS)

Case C-201/14 [2015] EU:C:2015:638

Belgian State

Case C-231/22 [2024] EU:C:2024:7

Belgian State

Case C-231/22 [2023] EU:C:2023:468, Opinion of AG Medina

Breyer v Bundesrepublik Deutschland

Case C-582/14 [2016] EU:C:2016:779

Buivids v Datu valsts inspekcija

Case C-345/17 [2019] EU:C:2019:122

College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer

Case C-553/07 [2008] EU:C:2008:773, Opinion of AG Ruiz-Jarabo Colomer

College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer

Case C-553/07 [2009] EU:C:2009:293

Dereci and others v Bundesministerium für Inneres

Case C-256/11 [2011] EU:C:2011:734

Digital Rights Ireland

Joined Cases C-293/12 and C-594/12 [2014] EU:C:2014:238

Digital Rights Ireland

Joined Cases C-293/12 and C-594/12 [2013] EU:C:2013:845, Opinion of AG Cruz Villalón

European Commission v Austria
Case C-28/09 [2011] EU:C:2011:854

European Commission v The Bavarian Lager Co. Ltd.
Case C-28/08 P [2010] EU:C:2010:378

Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit
Case C-645/19 [2021] EU:C:2021:483

Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV
Case C-40/17 [2019] EU:C:2019:629

Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV
Case C-40/17 [2018] EU:C:2018:1039, *Opinion of AG Bobek*

GC and Others v Commission nationale de l'informatique et des libertés (CNIL)
Case C-136/17 [2019] EU:C:2019:773

Google LLC v CNIL
Case C-507/17 [2019] EU:C:2019:772

Google LLC v CNIL
Case C-507/17 [2019] EU:C:2019:15, *Opinion of AG Szpunar*

Google Spain SL, Google Inc v Agencia Española de Protección de Datos, González
Case C-131/12 [2014] EU:C:2014:317

Google Spain SL, Google Inc v Agencia Española de Protección de Datos, González
Case C-131/12 [2013] EU:C:2013:424, *Opinion of AG Jääskinen*

IAB Europe v Gegevensbeschermingsautoriteit
Case C-604/22 [2024] EU:C:2024:214

Karlsson and Others
Case C- 292/97 [2000] EU:C:2000:202

La Quadrature du Net and Others v Premier ministre and Others
Joined Cases C-511/18, C-512/18 and C-520/18 [2020] EU:C:2020:791

Ligue des droits humains ASBL v Conseil des ministres
Case C-817/19 [2022] EU:C:2022:491, *Opinion of AG Pitruzzella*

Lindqvist v Åklagarkammaren i Jönköping
Case C-101/01 [2003] EU:C:2003:596

McB v L.E.
Case C-400/10 PPU [2010] EU:C:2010:582

Meta Platforms and Others (General terms of use of a social network)
Case C-252/21 [2023] EU:C:2023:537

Nacionalinis visuomenės sveikatos centras v Valstybinė duomenų
Case C-683/21 [2023] EU:C:2023:949

Nowak v Data Protection Commission
Case C-434/16 [2017] EU:C:2017:994

Opinion 1/15 of 26 July 2017 pursuant to Article 218(11) TFEU [2017] EU:C:2017:592

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others
Case C-623/17 [2020] EU:C:2020:790

Productores de Música de España (Promusicae) v Telefónica de España SAU
Case C-275/06 [2007] EU:C:2007:454, Opinion of AG Kokott

Productores de Música de España (Promusicae) v Telefónica de España SAU
Case C-275/06 [2008] EU:C:2008:54

Ryneš v Úřad pro ochranu osobních údajů
Case C-212/13 [2014] EU:C:2014:2428

Schecke and Eifert v Land Hessen
Joined Cases C-92/09 and C-93/09 [2010] EU:C:2010:662

‘Schrems I’ – Schrems v Data Protection Commissioner
Case C-362/14 [2015] EU:C:2015:650

‘Schrems II’ – Data Protection Commissioner v Facebook Ireland Limited and Schrems
Case C-311/18 [2020] EU:C:2020:559

Schwarz v Stadt Bochum
Case C-291/12 [2013] EU:C:2013:6

Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson

Joined Cases C-203/15 and C-698/15 [2016] EU:C:2016:970.

Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta

Case C-25/17 [2018] EU:C:2018:551

TK v Asociația de Proprietari bloc M5A-Scara A

Case C-708/18 [2019] EU:C:2019:1064

U v Stadt Karlsruhe

Case C-101/13 [2014] EU:C:2014:2249

Wachauf v Bundesamt für Ernährung und Forstwirtschaft

Case C- 5/88 [1989] EU:C:1989:321

WebMindLicenses Kft.

Case C-419/14 [2015] EU:C:2015:832

Weltimmo s.r.o v Nemzeti Adatvédelmi és Információszabadság Hatóság

Case C-230/14 [2015] EU:C:2015:639

Wirtschaftsakademie

C-210/16 [2018] EU:C:2018:388

Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT) *Case*

C-342/12 [2013] EU:C:2013:355

X and Others

Joined Cases C-199/12 to C-201/12 [2013] EU:C:2013:72

X and Z v Autoriteit Persoonsgegevens

C-245/20 [2022] EU:C:2022:216

X and Z v Autoriteit Persoonsgegevens

C-245/20 [2021] EU:C:2021:822, *Opinion of AG Bobek*

European Court of Human Rights (ECtHR)

Ahrens v Germany

Application no. 45071/09 [2012] CE:ECHR:2012:0322JUD004507109

Al-Nashif v Bulgaria

Application no. 50963/99 [2002] CE:ECHR:2002:0620JUD005096399

Andersson v Sweden

Application no. 12963/87 [1992] CE:ECHR:1992:0225JUD001296387

Big Brother Watch and Others v the United Kingdom

Applications nos. 58170/13, 62322/14 and 24960/15 [2021]

CE:ECHR:2021:0525JUD005817013 Partly Concurring, partly dissenting Opinion of Judge Pinto de Albuquerque

Buck v Germany

Application no. 41604/98 [2005] CE:ECHR:2005:0428JUD004160498

Copland v the United Kingdom

Application no. 62617/00 [2007] CE:ECHR:2007:0403JUD006261700

Chiragov v Armenia

Application no. 13216/05 [2015] CE:ECHR:2015:0616JUD001321605

Christie v United Kingdom

Application no. 21482/93 [1994] CE:ECHR:1994:0627DEC002148293

Çiçek v Turkey

Application no. 44837/07 [2020] CE:ECHR:2020:0204DEC004483707

Denisov v Ukraine

Application no. 76639/11 [2018] CE:ECHR:2018:0925JUD007663911

Emonet and Others v Switzerland

Application no. 39051/03 [2008] CE:ECHR:2007:1213JUD003905103

Ernst and Others v Belgium

Application no. 33400/96 [2003] CE:ECHR:2003:0715JUD003340096

Evans v the United Kingdom

Application no. 6339/05 [2007] CE:ECHR:2007:0410JUD000633905

Goodwin v The United Kingdom

Application no. 28957/95 [2002] CE:ECHR:2002:0711JUD002895795

Guerra v. Italie

Application no. 14967/89 [1998] CE:ECHR:1998:0219JUD001496789

Halford v the United Kingdom

Application no. 20605/92 [1997] CE:ECHR:1997:0625JUD002060592

Hämäläinen v Finland

Application no. 37359/09 [2014] CE:ECHR:2014:0716JUD003735909

Hatton v the United Kingdom

Application no. 36022/97 [2003] CE:ECHR:2003:0708JUD003602297

Iliya Stefanov v Bulgaria

Application no. 65755/01 [2008] CE:ECHR:2008:0522JUD006575501

Jeunesse v The Netherlands

Application no. 12738/10 [2014] CE:ECHR:2014:1003JUD001273810

Johnston and Others v Ireland

Application no. 9697/82 [1986] CE:ECHR:1986:1218JUD000969782

Keegan v Ireland,

Application no. 16969/90 [1994] CE:ECHR:1994:0526JUD001696990

Klass and Others v Germany

Application no. 5029/71 [1978] CE:ECHR:1978:0906JUD000502971

Kroon and Others v the Netherlands

Application no. 18535/91 [1994] CE:ECHR:1994:1027JUD001853591

Kryževičius v Lithuania

Application no. 67816/14 [2018] CE:ECHR:2018:1211JUD006781614

K.U. v Finland

Application no. 2872/02 [2008] CE:ECHR:2008:1202JUD000287202

López Ostra v Espagne

Application no. 16798/90 [1994] CE:ECHR:1994:1209JUD001679890

Lüdi v Switzerland

Application no. 12433/86 [1992] CE:ECHR:1992:0615JUD001243386

Marckx v Belgium

Application no. 6833/74 [1979] CE:ECHR:1979:0613JUD000683374

Maslov v Austria

Application no. 1638/03 [2008] CE:ECHR:2008:0623JUD000163803

Niemietz v Germany

Application no. 13710/88 [1992] CE:ECHR:1992:1216JUD001371088

Olsson v Sweden (No. 1)

Application no. 10465/83 [1988] CE:ECHR:1988:0324JUD001046583

P.G. and J.H. v the United Kingdom

Application no. 44787/98 [2001] CE:ECHR:2001:0925JUD004478798

Peck v the United Kingdom

Application no. 44647/98 [2003] CE:ECHR:2003:0128JUD004464798

Petrov v Bulgaria

Application no. 15197/02 [2008] CE:ECHR:2008:0522JUD001519702

Petri Sallinen and Others v Finland

Application no. 50882/99 [2005] CE:ECHR:2005:0927JUD005088299

Pretty v the United Kingdom

Application no. 2346/02 [2002] CE:ECHR:2002:0429JUD00234602

Roemen and Schmit v Luxembourg

Application no. 51772/99 [2003] CE:ECHR:2003:0225JUD005177299

S and Marper v the United Kingdom

Applications nos. 30562/04 and 30566/04 [2008] CE:ECHR:2008:1204JUD003056204

Saber v Norway

Application no. 459/18 [2020] CE:ECHR:2020:1217JUD000045918

Société Colas v France

Application no. 37971/97 [2002] CE:ECHR:2002:0416JUD003797197

Stolyarova v Russia

Application no. 15658/09 [2016] CE:ECHR:2016:0628DEC001565809

Üner v the Netherlands

Application no. 46410/99 [2006] CE:ECHR:2006:1018JUD004641099

Van Der Heijden v the Netherlands

Application no. 42857/05 [2012] CE:ECHR:2012:0403JUD004285705

Vavříčka v the Czech Republic

Application nos. 47621/13, 3867/14, 73094/14, 19298/15 19306/15, and 43883/15 [2021]

CE:ECHR:2021:0408JUD004762113

Wieser and Bicos Beteiligungen GmbH v Austria

Application no. 74336/01 [2007] CE:ECHR:2007:1016JUD007433601

X v the United Kingdom

Application no. 7308/75 [1978] CE:ECHR:1982:1018JUD000721575

X, Y and Z v the United Kingdom

Application no. 75/1995/581/667 [1997] CE:ECHR:1997:0422JUD002183093

National Case Law

France

Bonnet v Société Olibet Trib Comm Seine (13 juin 1882) Ann Prop Ind.

Dumas v Liébert Cour de Paris (25 mai 1867) Ann Prop Ind.

Félix v O'Connell, Trib Civ Seine (16 juin 1858) DP.

Germany

BVerfG, Order of the First Senate of 15 December 1983 [1983] 1 BvR 209/83 (German Federal Constitutional Court)

Ireland

DPP v O'Brien [2012] IECCA 68, [2012] 7 JIC 0201

Schrems v Data Protection Commissioner [2014] IEHC 310, [2014] 2 ILRM 401

Sullivan v Boylan [2012] IEHC 389, [2012] 10 JIC 0407

United Kingdom

Millar v Taylor [1769] 4 Burr2303, [1769] 98 ER 201 (Court of the King's Bench)

Prince Albert v Strange [1849] 2 De G & Sm 652, [1849] 64 ER 293 (High Court of Chancery)

United States

California v Greenwood 486 U.S. 35 [1988]

Federal Trade Commission v Ring LLC, [2023] 1:23-cv-1549 (US, District of Columbia)

Florida v Riley 488 U.S. 445 [1989]

Griswold v Connecticut, 381 U.S. 479 [1965]

Katz v United States 389 U.S. 347 [1967]

Olmstead v. United States 277 U.S. 438 [1928]

Whalen v Roe. 429 U.S. 589 [1977]

Table of Legislation

Council of Europe

Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No 1-16), ETS No 005, 4 November 1950.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CET 108), 28 January 1981 ('Convention 108').

European Union

Charter of Fundamental Rights of the European Union [2016] OJ C 202/2.

Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1, 7 June 2016 ('Lisbon Treaty').

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 ('Data Protection Directive') (repealed).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market [2000] OJ L178/1 ('eCommerce Directive').

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, as amended by Directive 2009/136/EC of 25 November 2009 [2002] OJ L201/37 ('ePrivacy Directive').

Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and Repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 ('Law Enforcement Directive').

Explanations relating to the Charter of Fundamental Rights [2007] OJ C 303/02 ('Explanations to the Charter').

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 OJ L 119/1 ('General Data Protection Regulation').

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC OJ L 295.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L152/1 ('Data Governance Act').

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 ('Digital Markets Act').

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC ('Digital Services Act').

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 ('Data Act').

European Union Bills and Drafts

Council of EU, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ('ePrivacy Regulation') Brussels, 10.1.2017 COM (2017) 10 final 2017/0003 (COD) 2017.

——Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence ('Artificial Intelligence Act') and

amending certain Union legislative acts - General approach Brussels, 25 November 2022
14954/22 Interinstitutional File: 2021/0106 (COD).

European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (2021) OJ L 199/31

— Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence ('Artificial Intelligence Act') and Amending Certain Union Legislative Acts, COM (2021) 206 final

— Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data ('Data Act') Brussels, 23.2.2022 COM (2022) 68 final 2022/0047 (COD) final

— Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 COM/2023/348 (2023) final.

European Parliament, Artificial Intelligence Act Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)) P9_TA (2023)0236 Artificial Intelligence Act.

United Nations

General Assembly, Universal Declaration of Human Rights (UDHR). Resolution 217', 10 December 1948

— International Covenant on Civil and Political Rights, I-14668, UNTS No 999 (ICCPR)

OECD

Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, C (80)58/FINAL, as amended on 11 July 2013 by C (2013)79

Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

National Law

Argentina

Bill 87/2023 Bill for the Protection of Personal information '*Proyecto de Ley de Protección de Datos Personales*' (2023).

Australia

Privacy Act 1988 (Cth) No. 119 1988 (as amended).

Austria

Federal Act of 18 October 1978 on the protection of personal data, '*Bundesgesetzblatt für die Republik Österreich*' (1978).

Brazil

General Data Protection Law '*Lei Geral de Proteção de Dados Pessoais*' ('LGPD') As amended by Law No. 13,853/2019).

Canada

Personal Information Protection and Electronic Documents Act ('PIPEDA') S.C. 2000

Estonia

Constitution of Estonia, *Eesti Vabariigi põhiseadus*, June 28, 1992. Chapter II, para. 11.

France

Constitution of 3 September 1791, *Constitution du 3 septembre 1791*, tit. III, ch. V, art. 17.

Constitution of the Year III, *Constitution de l'an III* (1795).

Constitution of the Year VIII, *Constitution de l'an VIII* (1799).

Declaration of the Rights of Man and of the Citizen of 1789, *Déclaration des droits de l'Homme et du citoyen de 1789*, Adopted by the National Assembly during its Sessions on August 20, 21, 25 and 26, and Approved by the King.

Decree no. 74-938 of 8 November 1974 establishing the Committee on Informatics and Liberties, J.O. 13 November 1974, p. 11403.

Law no. 70-539 of 24 June 1970 on the centralisation of the documentation relative to road traffic.

Law no. 70-643 of 17 July 1970 seeking to reinforce the protection of the rights of individuals and citizens, J.O. 19 July 1970, p. 6755

Law no. 79-1204 of 31 December 1970 on hospital reform.

Law no. 78-17 of 6 January 1978 concerning informatics, files and liberties [“Loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés”], Official Journal of the French Republic 7 January 1978, p. 227–231. (corr. 25 January 1978).

Germany

The Basic Law for the Federal Republic of Germany, *Grundgesetz für die Bundesrepublik Deutschland* (as amended July 2002). Articles 13 (Inviolability of the Dwelling) and 19 (Restriction of Basic Rights).

Ireland

Constitution of Ireland, *Bunreacht na hÉireann*, 1937. Article 40.5.

Kenya

The Data Protection Act No. 24 of 2019.

New Zealand

Privacy Act 2020, Version as of 6 December 2023.

Portugal

Constitution of Portugal, *Constituição Da República Portuguesa*, 1976. Articles 18(3), 35.

Singapore

Personal Data Protection Act 2012, 2020 Revised Edition.

South Korea

Personal Information Protection Act 2011 (as amended in 2023).

Spain

Constitution of Spain, *Constitución Española*, 1978. Articles 18(4), 53(1).

Sweden

Sweden Data Act (Datalagen), SFS 1973: 289.

United States of America

Constitution of the United States of America, 1787 as amended.

Children's Online Privacy Protection Act [1998] 15 U.S.C. §§ 6501–6506 (Public Law) 112 Stat. 2681-728.

Uruguay

Law No. 18331 on the Protection of Personal Data and *Habeas* Data Action.

Decree No. 414/009 Regulating Law 18.331 on the Protection of Personal Data

State and Regional Law

California, USA

The California Consumer Privacy Act as Amended November 3, 2020, by initiative Proposition 24. Cal. Civ. Code § 1798.140(v)(2).

Colorado, USA

SB21-190, Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1303 (2021).

Connecticut, USA

SB6, Connecticut Personal Data Privacy and Online Monitoring Act Public Act No. 22-15 (2022).

Delaware, USA

HB 154, Delaware Personal Data Privacy Act (2023).

Hesse, Germany

Law of 16 December 1969 establishing the data processing centre of the State of Hesse and regarding the data processing centres of local communities, HE GVBI, 22 December 1969, No. 32.

Hesse Data Protection Act of 7 October 1970, Hessen Datenschutzgesetz vom 7. Oktober 1970] Gesetz- und Verordnungsblatt für das Land Hessen (HE GVBl)

Indiana, USA

SB 5, Indiana Consumer Data Protection Act (2023)

Iowa, USA

SF 262, Iowa Consumer Data Protection Act (2023)

Montana, USA

SB 384, Montana Consumer Data Protection Act (2023).

Oregon, USA

SB 619, Oregon Consumer Privacy Act (2023).

Tennessee, USA

HB1181, Tennessee Information Protection Act (2023).

Texas, USA

HB 4, Texas Data Privacy and Security Act (2023).

Utah, USA

SB 227, Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101(29)(b) (2022).

Virginia, USA

Virginia Consumer Data Protection Act (CDPA) Va. Code § 59.1-571 (2021).

List of Tables

Table 1. Comparison: Article 7 of CREU and Article 8(1) ECHR.....	31
Table 2. Solove's Taxonomy of Privacy	47
Table 3. Essential Elements of the Right to Data Protection per Porcedda.....	59
Table 4. Dualism of Goals in Digitally Focussed EU Legislation.....	78
Table 5. Obligations under the DSA	144
Table 6. VLOPs and VLOSEs Designated by The European Commission	147
Table 7. Cloud Service Provider Actors and their Data Protection Roles.....	328
Table 8. Social Media Data Categories	329
Table 9. Social Media Actors and their Roles under the GDPR.....	338
Table 10. Smart Home Devices Actors and Data Processing Roles	339

List of Figures

Figure 1. Relationship Between Privacy and Data Protection (Model 1).....	63
Figure 2. Relationship Between Privacy and Data Protection (Model 2).....	66
Figure 3. Relationship Between Privacy and Data Protection (Model 3).....	68
Figure 4. Stages of Data Processing Timeline per Van Ooijen and Vrabec	90
Figure 5. Controller, Processor, and Sub-Processor Relationship.....	105
Figure 6. Joint Controller Relationship	106
Figure 7. Concentric Circles of EU Digital Law	134
Figure 8. Tiered Approach under DSA.....	144
Figure 9. Risk-Based Approach of the AI Act.....	154
Figure 10. Classic Model of Data Processing in 1970s	179
Figure 11. Classic Model of Data Processing and Roles.....	181
Figure 12. Controller Relationships per Fashion ID Part 1	199
Figure 13. Controller Relationships per Fashion ID Part 2	199

Figure 14. Ring’s ‘Neighbors’ App.....	254
Figure 15. Ring Owner/User as Controller.....	255
Figure 16. Ring Owner/User as Joint Controller	259
Figure 17. AI Service Chain Based on Cobbe and Singh.....	275
Figure 18. AI Service Processing Chain (Stage 1).....	276
Figure 19. AI Service Processing Chain (Stage 2).....	276
Figure 20. AI Service Processing Chain (Stage 3).....	277
Figure 21. AI Service Processing Chain (Stage 4).....	277
Figure 22. Simple Division of Roles in AI Service Processing Chain.....	280
Figure 23. Division of Roles in Service Processing Chain per Cobbe and Singh	282
Figure 24. Indicative Complex AI Supply Chain	284
Figure 25. Complementing and Competing Relationship under AI Act (Part 1)	287
Figure 26. Complementing and Competing Relationship under AI Act (Part 2)	287
Figure 27. Collaboration Between Controllers per Olsen and Mahler.....	310
Figure 28. Archetypal Data Processing Relationship	310
Figure 29. Service Provider Acting with Limited Autonomy	318
Figure 30. Service Provider Acting with Significant Autonomy	319
Figure 31. Actors within Simple Cloud Service Processing Chain.....	326

Chapter One: Introduction

1. Background

The division between public and personal domains is not a modern conception. However, the relationship between the two spheres has been shaken in the past century in ways which could not have been imagined by our forebears. In particular, the growth of information and communications technology has fundamentally altered the way in which individuals, societies, and political regimes interact globally.

As a result, the individual of the 2020s emerges into a digital plane beyond the conceptions of her predecessors. She participates in this realm with more information, connection, and ease of access than could hitherto have been conceived. However, she does so not as a digital pioneer, but instead as a ‘data subject’ within a *colonised space* – akin to the corporation dominated colonies of the 19th century.¹ Compared to the digital frontier of the 1990s, the burdens of entry for individuals are low, levels of infrastructure are high, and representation rights are minimal. The rapid growth in commercially available Artificial Intelligence (‘AI’) systems threatens to exacerbate this estrangement. Addressing this alienation is the central concern of this thesis.

¹ Although the term ‘data subject’ has legal significance, as is explored throughout this thesis, here the term is chosen to emphasise the asymmetry of power within the digital domain. The distinction between the subjects of a principality or colony as opposed to the citizens of a modern republic is reminiscent of the contemporary experience of powerlessness and lack of control.

Introduced in 2016, the General Data Protection Regulation ('GDPR')² marked a significant shift in the balance between individual rights on one side and the increasingly entwined forces of multinational tech commerce and government surveillance on the other. Yet, the GDPR's aims are often lost amidst complex data flows and a marked asymmetry in power and knowledge. What is more, significant legal responsibilities fall onto parties who are unaware of their legal obligations, further undermining the aims of European Data Protection Law.³

Since the commencement of the GDPR a host of other legal instruments have been proposed and enacted as part of the EU's European Digital Strategy.⁴ The proliferation of these laws is indicative of the scale and complexity of the task of regulating the digital domain. The changing nature of the challenges present are clear as at the time of writing the European Union has recently passed the world's first AI Regulation, the Artificial Intelligence Act ('AI Act').⁵ As the confines of EU Digital Law are expanded to include AI Regulation the conceptions, ambitions, and models which underpin this branch of law require reassessment. As such, we

² 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 OJ L 119/1 ('General Data Protection Regulation').

³ This term is used interchangeably with EU Data Protection Law. Each of these terms refer to Data Protection Law as governed by the European Union specifically, and not European states on their own, or by the Council of Europe.

⁴ European Commission, 'EU Digital Strategy' <<https://eufordigital.eu/discover-eu/eu-digital-strategy/>> accessed 7 March 2024. See also Vagelis Papakonstantinou and Paul De Hert, 'Post GDPR EU Laws and Their GDPR Mimesis. DGA, DSA, DMA and the EU Regulation of AI' (*European Law Blog*, 1 April 2021) <<https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/>> accessed 7 March 2024.

⁵ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 OJ L, 2024/1689 ('Artificial Intelligence Act').

must ask if our goals can still be met with the tools which have thus far been developed to achieve them.

2. Problem Statement: ‘*The Problem of Control*’ in EU Data Protection Law

This thesis contributes to EU Data Protection Law by articulating and exploring *the Problem of Control* within this realm. At the simplest level *the Problem of Control* is linguistic in nature as there are multiple distinct appeals to the idea of *control* in this area of the law. The first is that of the *controller*, a role central for allocating accountability. While the second usage refers to the deeper ambition of granting power over one’s information through the ideal of *individual control*. Finally, Article 8(3) of the Charter of Fundamental Rights of the European Union (‘the Charter’ or ‘CFREU’) entrusts independent authorities with safeguarding ‘the rules’ of Data Protection through *regulatory control*. It is clear that these terms each carry their own meaning and these references may create confusion. However, this does not represent a crisis in the discipline itself. Rather, we must focus upon the breakdown of the EU Data Protection Regime’s accountability model which results in the hollowing out of all meanings of *control*.

2.1 ‘*The Problem of Control*’ as a ‘*Controller Problem*’

Central to the European Data Protection Regime⁶ are the twin ambitions of (a) protecting individual rights and freedoms and (b) facilitating innovation by

⁶ This term is used interchangeably with EU Data Protection Regime and EU Data Protection Law. Each of these terms refer to Data Protection Law as governed by the European Union specifically, and not European states on their own or by the Council of Europe. See (n 3).

expanding the digital market.⁷ These goals are expressly laid out in the European Commission's initial proposal for the GDPR⁸ and find clear articulation in the text of the Regulation itself.⁹

In order to give effect to these aims, the GDPR places obligations upon the different actors within 'data processing relationships'.¹⁰ Specifically, the GDPR employs a 'controller-based' responsibility system¹¹ wherein the chief onus for fulfilling its obligations falls upon 'controllers'¹² and 'joint controllers'.¹³ While, secondary responsibility is placed upon 'processors'.¹⁴ This regime centres upon

⁷ Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 46–88. These goals will be explored in depth in [Chapter Three, Section 2. The Ambitions of the EU Data Protection Regime](#).

⁸ European Commission, 'Press Release. Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses. European Commission.' (25 January 2012) <https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46> accessed 7 March 2024.

⁹ See GDPR, Article 1 and Recitals 6-7.

¹⁰ This term is used interchangeably with 'data control relationships' and 'relationships of control' throughout this thesis.

¹¹ See Benjamin Wong, 'Problems with Controller-Based Responsibility in EU Data Protection Law' (2021) 11 *International Data Privacy Law* 375.

¹² The terms 'data controller' and 'controller' are used interchangeably throughout this thesis. The definition of a controller is given in Article 4(7) of the GDPR as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data' (emphasis added). The concept of controller under the GDPR is discussed in detail in [Chapter Four, Section 4. Actors and Accountability](#).

¹³ The terms 'joint controller' and 'joint data controller' are used interchangeably throughout this thesis. A joint controller relationship is defined in Article 26 of the GDPR. 'Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.' (emphasis added). The concept of a joint controller is discussed in detail in [Chapter Four, Section 4. Actors and Accountability](#).

¹⁴ The terms 'data processor' and 'processor' are used interchangeably throughout this thesis. The definition of a data processor is given in Article 4(8) of the GDPR as 'the natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller. The concept of processor is discussed in detail in [Chapter Four, Section 4. Actors and Accountability](#).

the protection of ‘data subjects’.¹⁵ As such, properly identifying ‘relationships of control’¹⁶ is vital for apportioning accountability and liability, as well as ensuring full transparency to individuals and the public.

This model of accountability traces its origins to the first data protection laws of the 1970s and 1980s and has calcified within the contemporary EU Data Protection Regime. However, data processing relationships are often elaborate, featuring numerous parties and data transfers. Our concern surrounds the difficulty in defining these relationships and the parties within them. This challenge has been heightened through a series of recent CJEU judgments which have stretched the definition of *controllanship* to new limits.

2.2 The Emptiness of Control

There are numerous conceptions through which the rights to privacy and data protection may be understood and operationalised. However, as is explored in Chapter Three, contemporary EU Data Protection Law has tied itself to a model of individual control over one’s personal information.¹⁷ The appeal to individual control emerged from the zeitgeist of the 2000s and 2010s. The consensus around this ‘control model’¹⁸ has solidified just as the idea of *control* in the digital domain has become an unattainable goal. With the advent of complex data flows that intertwine numerous actors, the clarity of who controls and processes data is often muddled, making it difficult for individuals to exercise autonomy with regards to

¹⁵ The definition of ‘data subject’ is drawn from Article 4(1) of the GDPR as referring to the identified or identifiable natural person to whom personal data pertains. See [Chapter Four, Section 3. Key Definitions](#).

¹⁶ This term is used interchangeably with ‘data control relationships’ and ‘data processing relationships’ throughout this thesis as is explained in (n 11).

¹⁷ See [Chapter Three, Section 3. The Nature of the Data Protection Regime](#).

¹⁸ See [Chapter Three, Section 3.1 The Individual Control Model](#).

their own information. This complexity is further exacerbated by the rise of AI systems, which process vast amounts of data in ways that are often opaque and beyond the comprehension of the user. As a result, individuals find themselves in a web of data processing relationships where their ability to manage and oversee their personal data is significantly diminished, if not altogether illusory. This evolving digital ecosystem challenges the very notion of personal data autonomy, underscoring the need for robust legal frameworks and innovative solutions to safeguard individual rights in an age dominated by intricate data exchanges.

Individuals seeking to exercise *control* must do so by employing their rights against *controllers*. Similarly, independent Supervisory Authorities ('SAs')¹⁹ levy their powers against actors according to the level of responsibility placed upon them by the law, but focus specifically upon controllers. Thus, without clear demarcation of the role of controller, the autonomy of individuals is stymied while the powers of SAs are misdirected. All three appeals to control thus depend on the clarity and efficacy of the controller-based accountability regime.

2.3 The Consequences

The result of *the Problem of Control* is an uncertainty which cuts in two distinct directions. The first impacts the individual who is the data subject in a labyrinth of data processing relationships. The second places unanticipated burdens upon the user of technology who now finds herself to be a controller or joint controller with legal responsibilities under the GDPR. This confusion may arise unwittingly through a controller simply trying to carry out a data processing operation without realising its full implications. However, in other cases, the distinction between parties is rendered purposefully opaque.

¹⁹ See [Chapter Four, Section 7. Supervisory Authorities](#) for an overview of these regulators.

These difficulties have only been exacerbated by the rapid development and deployment of AI Systems which raise new foundational challenges to this paradigm. Soon, AI Services are to be governed by both the GDPR and the AI Act. The anticipated result is one in which an individual will now hold what may be termed ‘complementing and competing’ obligations under both laws. This will only serve to compound *the Problem of Control* as will be demonstrated in Chapter Nine.

3. Research Questions

Stemming from *the Problem of Control*, laid out above, this thesis seeks to answer the primary research question:

How do the increasing complexities of data processing relationships and the broadening interpretation of ‘controllership’ by the CJEU impact the efficacy of EU Data Protection Law’s controller-based accountability, and what are the consequent effects on individual autonomy and regulatory oversight?

To this end the following sub-questions must be answered:

1. *Under what circumstances has the EU Data Protection Regime and its accountability model emerged?*
2. *What is the nature of the EU Data Protection Regime and its controller-based responsibility model?*
 - *What are the core ambitions which underpin EU Data Protection Law?*
 - *What are its principles?*
 - *What other accountability models exist?*

3. *What uncertainties result from the controller-based responsibility model under EU Data Protection Law?*
4. *What are the consequences of these uncertainties for controllers, data subjects, regulators, and other parties?*
5. *What solutions have been proposed to address the issues that arise in practice and to what extent are they capable of addressing these challenges?*

These questions guide this study which will combine methodological techniques to provide an understanding of the uncertainties emerging from data processing relationships. These uncertainties give rise to *the Problem of Control* which is the central concern of this work. *The Problem of Control* will be examined with reference to its impact upon the core ambitions which underpin EU Data Protection Law.

The obscurities of data processing relationships have been explored by the CJEU in the cases of *Wirtschaftsakademie*,²⁰ *Jehovan todistajat*,²¹ *Fashion ID*,²² *NVSC*,²³ *Belgian State*,²⁴ and most recently *IAB Europe*.²⁵ These decisions and their ramifications will be investigated with an emphasis upon their real world impacts.

Finally, this thesis will outline potential solutions to the challenges identified. One such solution is developed in the form of a taxonomy of accountability in data

²⁰ Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie* [2018] EU:C:2018:388.

²¹ Case C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* [2018] EU:C:2018:551.

²² Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* [2019] EU:C:2019:629.

²³ Case C-683/21 *Nacionalinis visuomenės sveikatos centras v Valstybinė duomenų NVSC* [2023] EU:C:2023:949.

²⁴ Case C-231/22 *Belgian State* [2024] EU:C:2024:7.

²⁵ Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* [2024] EU:C:2024:214.

processing relationships. It is believed that this may serve as a mechanism for mitigating *the Problem of Control*.

4. Structure and Methodology

This thesis is divided into three parts (I): State of the Art; (II) The Nature and Impact of the Problem of Control; and (III) Recommendations and Conclusion. The focus of each and the methodologies which underpin our analysis are explained in the following subsections.

4.1 Part I: State of the Art

In Part I the following research questions will be explored:

- *Under what circumstances has the EU Data Protection Regime and its accountability model emerged?*
- *What is the nature of the EU Data Protection Regime and its controller-based responsibility model?*
 - *What are the core ambitions which underpin EU Data Protection Law?*
 - *What are its principles?*
 - *What other accountability models exist?*

To understand *the Problem of Control* it is first essential to establish the theoretical and legal tradition from which EU Data Protection Law is derived. At the onset we must note that Data Protection Law has a stronger foundation under the GDPR, than it did under the 1995 Data Protection Directive²⁶ which preceded it. Initially, Data Protection Law was understood as emerging from the right to privacy. However, the passage of the Charter of Fundamental Rights of the EU

²⁶ 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 ('Data Protection Directive') (repealed) 1995.

provided a separate right to data protection under Article 8 which sits next to the right to privacy in Article 7.

The relationship between the two rights however remains unclear. As such a necessary, albeit necessarily abridged, account of the evolution of data protection is undertaken in Chapter Two. We will explore the right to data protection focusing upon its origins, conceptual underpinnings, and distinguishing ‘essence’.²⁷ Thereafter we will examine three possible readings of the relationship between the two rights. As the GDPR forms the basis of contemporary Data Protection Law and this thesis, Chapter Three will focus upon its nature and ambitions, while Chapter Four will be devoted to its accountability regime, provisions, and key elements.

However, the GDPR is only one part of the EU’s larger regulatory framework for online services, markets, AI, and data sharing. This framework includes the Digital Services Act (‘DSA’),²⁸ the Digital Markets Act (‘DMA’),²⁹ and the Artificial Intelligence Act (‘AI Act’).³⁰ Of particular relevance to this thesis are the diverse accountability models employed across these legislative instruments. These approaches demonstrate that the controller-based model is not the sole approach to safeguarding digital rights. As such, a brief overview of the subject matter and

²⁷ The meaning of ‘essence’ in this context is explained later in this chapter in [Section 4.5 Methodology](#).

²⁸ Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market For Digital Services [2022] OJ L277/1 (‘Digital Services Act’).

²⁹ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 reference OJ L 265/1 (‘Digital Markets Act’).

³⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 OJ L, 2024/1689 (‘Artificial Intelligence Act’).

accountability frameworks of these laws is undertaken in Chapter Five which focuses upon this expanding regime.

Moreover, the foundational concepts, roles, and responsibilities initially established by the 1995 Directive have been substantially expanded through judicial interpretation. Data Protection's core concepts are now broadly defined, with exceptions narrowly interpreted. This widespread applicability has resulted in data protection being conceptualised as an all-encompassing legal framework. Thus, adopting terminology introduced by Purtova,³¹ data protection has come to be referred to as 'the law of everything.'

Numerous instances of this expansion can be observed, with two key examples highlighted in the second part of Chapter Five: (i) the expanded scope of the definition of personal data itself, and (ii) the heightened requirements for transferring personal data outside of the European Economic Area ('EEA'). Both demonstrate the judicial expansion of Data Protection Law with the ambition of ensuring 'complete and effective' protection of individuals.³² This same motivation has guided the CJEU in broadening the scope of controllership.³³ A central concern of this thesis is whether this expansive approach does in fact ensure such protection.

³¹ Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40.

³² See Orla Lynskey, 'Complete and Effective Data Protection' (2023) 76 Current Legal Problems 297.

³³ The appeal to 'complete and effective' protection as the rationale for a broad interpretation of controllership can be found in *Case C-131/12 Google Spain SL, Google Inc v Agencia Española de Protección de Datos, González* [2014] EU:C:2014:317 at [34]; a close variation of this phrasing appears in *Jehovan todistajat* at [66], *Wirtschaftsakademie* at [45], *Belgian State* at [28], and *IAB Europe* at [55].

4.3 Part II: The Nature and Impact of the Problem of Control

In Part II focus is given to the following research questions:

- *What uncertainties result from the controller-based responsibility model under EU Data Protection Law?*
- *What are the consequences of these uncertainties for controllers, data subjects, regulators, and other parties?*

Part II aims to document *the Problem of Control* and trace its effects. Here attention is given to the impact on data subjects as well as controllers, regulators, and the general public.

We begin in Chapter Six by exploring the foundational model of data processing upon which the GDPR's accountability framework was developed. The growth of Data Protection Law did not occur in isolation, rather it followed the establishment of various national and international instruments. By scrutinising a selection of these laws and their accountability models a more comprehensive understanding of the 'controller' and 'processor' concepts can be attained. Following this work, we turn our focus to the evolving complexities that have arisen since the mid-1990s, challenging the traditional model. These challenges have been further complicated by recent rulings of the CJEU in the cases of *Wirtschaftsakademie*, *Jehovan todistajat*, *Fashion ID*, *NVSC*, *Belgian State*, and *IAB Europe*. An analysis of these cases and the implications of the Court's rulings is thus undertaken.

In Chapter Seven we outline the core complications stemming from the Court's rulings namely:

1. The lack of a conceptual framework onto which the Court's innovations can be applied.

2. The weakening of legal certainty in data processing relationships as actors, their responsibilities, and liabilities cannot be easily identified.
3. The undermining of consent as a lawful basis for processing personal data.
4. The violation of the Data Protection Principles of 'Fairness' and 'Transparency'.
5. The obscuring of data commodification as a societal issue.
6. The limiting of individual and regulatory control of personal data through opaque data sharing relationships.

Chapter Seven concludes by assessing the cumulative impact of these issues on the Court's aspiration of providing 'complete and effective' protection of individuals.

Following this analysis we provide two illustrations of *the Problem of Control* as it manifests in reality. The first, outlined in Chapter Eight, is the disappearance of the home as a place of physical and legal sanctuary as a result of smart home devices. This example is worthy of study because of its significant implications on established law. The exemption of the home from both interference and legal obligations is a settled issue in Privacy and Data Protection Law. Nevertheless, *the Problem of Control* manifests in this area all the same.

Conversely, Chapter Nine provides an exploration of a relatively untested domain for Data Protection Law, the case of AI Service Chains. Supply chains in AI Services are intricate with the creation, deployment, and use of technologies spread across many interconnected stakeholders. As such nowhere are the limits of the accountability framework of Data Protection Law challenged as much as in the case of AI Services. At the onset of this Introduction we queried whether the ambitions of Data Protection Law can still be met with the tools which have thus

far been developed to achieve them. Exploring this domain allows us to analyse whether the controller-based accountability model first established in the 1980s is now anachronistic.

4.4 Part III: Recommendations and Conclusion

In Part III focus is given to the question of how to mitigate *the Problem of Control*. Recommendations as found in literature will be presented and critically examined including: (I) extending responsibilities for processors; (II) applying a non-controller-based accountability model; (III) moving to a *de minimis* threshold for control in the form of orchestration; and (IV) allowing ‘site level flexibility’ in judicial and regulatory action.

Finally, this thesis offers one immediate mitigation to *the Problem of Control* by providing a defined taxonomy of data processing relationships. Smaller companies and private individuals are often left to decipher complex data processing chains on their own, or else must lean on the knowledge of professional consultants. Such a requirement for expertise may be seen as a regressive form of taxation whereby the cost of compliance for all businesses dealing with data is sufficiently high to stifle innovation for all but the largest firms. This itself undermines the legislative ambition of stimulating the digital market for all, which led to the adoption of the GDPR.³⁴

Access to a well-defined taxonomy of data control relationships can empower those attempting to fulfil their obligations under the GDPR. Moreover, having clearly demarcated models of all parties present in common personal data sharing

³⁴ Lynskey, *The Foundations of EU Data Protection Law* (n 7) 46–88. The goals of the GDPR will be explored in depth in [Chapter Three, Section 3. The Ambitions of the EU Data Protection Regime](#).

scenarios may offer substantial practical advantages for researchers, regulators, technology creators, and private citizens.

4.5 Methodology

The primary methodology of this thesis will be doctrinal while other approaches will be employed at different times. Doctrinal research assigns to the legal scholar and practitioner the responsibility of interpreting authoritative texts to apply them correctly in legal reasoning. This form of research is characteristically argumentative, with the primary objective of constructing approaches founded on sound legal rationale.³⁵ The primary sources of analysis shall be the text of legal instruments along with (i) their recitals and preparatory works; (ii) the case law of the CJEU and ECtHR, (iii) Guidance issued by the Article 29 Working Party ('WP29'),³⁶ the European Data Protection Board ('EDPB'),³⁷ and the Supervisory Authorities ('SAs') of EU Member States;³⁸ and (iv) scholarly writings.

However, legal research is not limited solely to doctrinal methods. It can also encompass non-doctrinal research, which takes a more problem-oriented, policy-driven, and law reform-focused approach. For instance, this approach might involve identifying flaws in existing policy regarding its effectiveness or implementation and subsequently proposing necessary legal reforms. This process often necessitates consideration of the social contexts underpinning the

³⁵ Sanne Taekema, 'Relative Autonomy, A Characterisation of the Discipline of Law' in Bart van Klink and Sanne Taekema (eds), *Law and method: interdisciplinary research into law* (Mohr Siebeck 2011).

³⁶ See [Chapter Four, Section 8, The EDPB and Cross Border Cooperation](#) for an overview of this body.

³⁷ See [Chapter Four, Section 8, The EDPB and Cross Border Cooperation](#) for an overview of this body.

³⁸ See [Chapter Four, Section 7. Supervisory Authorities](#) for an overview of Supervisory Authorities.

law and an assessment of how the current legal framework impacts various social constructs in practice. As a result, a space is opened for the incorporation of empirical legal research, enriching the understanding of law through its practical application and societal effects.³⁹ In this thesis this will be achieved through explanatory illustrations of the *Problem of Control* in action in Chapters Eight and Nine.

Additionally, in reviewing underlying philosophical conceptions attention will be given to the 'Cambridge School' of intellectual history.⁴⁰ In this regard the work of John Dunn⁴¹ and Quentin Skinner⁴² are of particular importance. This approach maintains that an understanding of the social, political, and historical context of a particular work enhances understanding.⁴³ This method is not to be confused with biographic speculation. Rather arguments are to be understood through the clear intent of their author. This may only be achieved through a comprehension of the political and philosophical climate of the time of the work's composition, in addition to an analysis of the meaning of key terms and language utilised by a thinker.⁴⁴

³⁹ Ian Dobson and Francis Johns, 'Legal Research as Qualitative Research' in Mike McConville and Wing Hong Chui (eds), *Research Methods For Law* (2nd edn, Edinburgh University Press 2017).

⁴⁰ Lawrence Hamilton, 'The Power of the Past: The Future of Intellectual History in South Africa' in Peter Vale, Lawrence Hamilton, and Estelle Prinsloo (eds), *Intellectual Traditions in South Africa: Ideas, Institutions and Individuals* (University of KwaZulu-Natal Press 2014) 6.

⁴¹ John Dunn, 'The Identity of the History of Ideas', *Political Obligation in its Historical Context: Essays in Political Theory*, edited by J. Dunn (Cambridge University Press 1980); John Dunn, 'Practising History and Social Science on "Realist" Assumptions:', *Political Obligation in its Historical Context: Essays in Political Theory*. (Cambridge University Press 1980); John Dunn, *The History of Political Theory and Other Essays*. (Cambridge University Press 1996).

⁴² Quintin Skinner, 'Meaning and Understanding in the History of Ideas', *Visions of Politics Volume I: Regarding Method*, edited by Q. Skinner. (Cambridge University Press 2002).

⁴³ Hamilton (n 40).

⁴⁴ *ibid* 8.

Furthermore, in deciphering the content and distinguishing features of the rights to privacy and data protection we will utilise an ‘essence’ study of the two rights.⁴⁵ A natural reading of the essence of a right is of finding the heart of a right within its larger body. Similarly, we may be drawn to metaphors from physical science and conceive of the essence as the nucleus around which its structure is formed.

González Fuster notes that the case law of the CJEU shows that, in reality, the Court appeals to the essence requirement even in the absence of a clear conception of what defines a right’s core.⁴⁶ This may be the result of the difficulty of the task itself. Indeed, Advocate General Pitruzzella argues that pinpointing the essence of a fundamental right is an exceedingly complex undertaking and at times it may be ‘almost impossible to do so’.⁴⁷ Perhaps because of this difficulty, Lock notes that where the CJEU ‘has found the essence of a right to have been infringed, it has done so largely apodictically without much discussion’.⁴⁸ As such, González Fuster maintains that the essence requirement should be seen more as a judicial tool for determining the unlawfulness of certain rights limitations, rather than as a directive to precisely delineate a right’s core area.⁴⁹ Accepting these limitations

⁴⁵ See Maria Grazia Porcedda, ‘On Boundaries. Finding the Essence of the Right to the Protection of Personal Data.’ in: Leenes, Van Brakel, De Hert and Gutwirth, *Privacy and Data Protection: The Internet of Bodies*, (Hart Publishing 2018) and *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis* (Hart 2023) 111–128.

⁴⁶ Gloria González Fuster, ‘Study on the Essence of the Fundamental Rights to Privacy and to the Protection of Personal Data’ 16.

⁴⁷ *Case C-817/19 Ligue des droits humains ASBL v Conseil des ministres* [2022] EU:C:2022:491 *Opinion of AG Pitruzzella* at [92].

⁴⁸ Tobias Lock, ‘Articles 51-54’, in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds.), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, (Oxford University Press 2019) 2251.

⁴⁹ González Fuster (n 46) 17.

we may still use an essence study of the right to privacy to gain deeper insight into its respective distinguishing components.

5. Limitations of this Study

This thesis does not act as a defence for the rights to privacy and data protection. Instead, we proceed from the reality that both are entrenched in the Charter of Fundamental Rights of the European Union. As such, our attention is focused upon the legislative frameworks which have been employed to protect these rights and the accountability models used to uphold them.

Furthermore, this thesis does not aim to provide a systemic history of technology or of surveillance. Certain moments are highlighted as vital for the development of both Privacy and Data Protection Law. These are explored in order to deliver vital context for the origins and limitations of the tools which we have to safeguard rights.

Additionally, while the experience of alienation through surveillance is heightened and taken to new limits through the advancing technologies outlined in this thesis. It would, however, be incorrect to imply that such alienation is itself a novel experience. A review of history may sometimes lead us to romanticise a more humane bygone era. The advent and implications of modern algorithmic decision-making, while unique in their scope and potential hazards, continue a long-standing tradition of impersonal bureaucracies employing quantitative analysis. This tradition, as illuminated by Foucault,⁵⁰ Browne,⁵¹ and Muhammad⁵²

⁵⁰ Michel Foucault, *Discipline and Punish: The Birth of the Prison* (2nd ed, Vintage Books 1995).

⁵¹ Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Duke University Press 2015).

⁵² Khalil Gibran Muhammad, *The Condemnation of Blackness: Race, Crime, and the Making of Modern Urban America* (Harvard University Press 2019).

traces back to the early 19th century. These scholars reveal a deep-rooted history of quantifying human beings in various social and institutional contexts, including education, racial categorisation, colonialism, enslavement, military service, poverty, mental health, and imprisonment, showcasing a continuum of attempts to order and categorise people through numbers. It is drawing on this work that we opened this chapter by comparing the experience of today's data subject to that of life in the colonies of the past.

Moreover, as is suggested at different points throughout this thesis, technologies of surveillance from the first censuses to the algorithmic supply chains of today do not simply record a population. Instead, they are by their very nature 'constitutive' of the surveyed public. That is to say, they help form the notion of a collective as a 'people'. The works of Igo,⁵³ Didier,⁵⁴ Bouk,⁵⁵ and Merchant⁵⁶ are instructive in this field. While Murphy provides a valuable study on the connection between language, power, surveillance, and privacy.⁵⁷ However, a deeper engagement with this historical understanding is beyond the scope of this thesis.

Finally, it must be noted that the controller-based accountability model is not used exclusively within Europe. Its origins can be directly traced to the 1980 OECD

⁵³ Sarah E Igo, *The Averaged American: Surveys, Citizens, and the Making of a Mass Public* (Harvard University Press 2008); Sarah E Igo, *The Known Citizen* (Harvard University Press 2018).

⁵⁴ Emmanuel Didier, Theodore M Porter and Priya Vari Sen, *America by the Numbers: Quantification, Democracy, and the Birth of National Statistics* (The MIT Press 2020).

⁵⁵ Daniel B Bouk, *How Our Days Became Numbered: Risk and the Rise of the Statistical Individual* (Paperback edn, University of Chicago Press 2018).

⁵⁶ Emily Klancher Merchant, *Building the Population Bomb* (Oxford University Press 2021).

⁵⁷ Maria H Murphy, *Surveillance and the Law: Language, Power, and Privacy* (Routledge, Taylor & Francis Group 2020).

Guidelines⁵⁸ and the Council of Europe's Convention 108.⁵⁹ As the OECD represents more than European states and Convention 108 was open to ratification by states outside of Europe it stands to reason that a host of other national and regional laws place key responsibilities on controllers.⁶⁰

Additionally, starting in 2018 numerous US Privacy Laws have been passed at the state level. Twelve of these employ the controller as the key responsible entity.⁶¹ However, these will not be examined in this thesis as our remit is limited to the European Data Protection Regime. In time a comparative study of these laws may provide a valuable counterpart to this initial research.

Case law and legislation referred to in this thesis date to 30 September 2024.

⁵⁸ Organisation for Economic Co-operation and Development ('OECD'), 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris.' (1980).

⁵⁹ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) 1981 108.

⁶⁰ See for example Personal Information Protection Act 2011 (as amended in 2023) (South Korea); Bill 87/2023 Bill for the Protection of Personal information 'Proyecto de Ley de Protección de Datos Personales' (2023) (Argentina); Law No. 18331 on the Protection of Personal Data and Habeas Data Action (Uruguay).

⁶¹ See SB21-190, Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1303; SB 6, Connecticut Personal Data Privacy and Online Monitoring Act Public Act No. 22-15(2022) § 1(25); HB 154, Delaware Personal Data Privacy Act (2023); SB 5, Indiana Consumer Data Protection Act (2023); SF 262, Iowa Consumer Data Protection Act (2023); SB 384, Montana Consumer Data Protection Act (2023); SB 332, New Jersey Data Privacy Law (2024); SB 619, Oregon Consumer Privacy Act (2023); HB1181, Tennessee Information Protection Act (2023); HB 4, Texas Data Privacy and Security Act (2023); SB 227, Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101(29)(b) (2022); Virginia Consumer Data Protection Act Code § 59.1-571 (2021).

PART I: STATE OF THE ART

'Privacy is a distinctly modern product, one of the luxuries of civilization'

E. L. Godkin, 1890

In the 1440s Johannes Gutenberg, utilised contemporary knowledge of screw-pressing to develop a new method for reproducing written work.⁶² The impact of Gutenberg's printing press was revolutionary. More books were produced in the fifty years following Gutenberg's invention than had been written out by scribes in the one thousand years which had preceded it.⁶³

New trades, professions, and realms of law developed in the wake of these advancements.⁶⁴ Prior to the printing press the process of copying written work was almost as laborious as creating the original itself. However, the potential for identical duplication altered the relationship between author and their work. Thus, new forms of legal protection in an expanded model of intellectual property ownership became necessary.

Similarly, the rights to privacy and data protection have developed as a result of radical shifts in the individual's understanding of herself and her world. These correspond to very real innovations in technology and the relationship between the state and individuals. This insight is not revolutionary. Its roots may be found in Alexis de Tocqueville's definition of modernity as a change in the self-

⁶² Elizabeth Eisenstein, *The Printing Revolution in Early Modern Europe* (Cambridge University Press 1993) 15.

⁶³ Cullen Murphy, 'Anyone Who Thinks We've Now Grasped What the Internet Has in Store for Us Should Revisit What the Printing Press Unleashed.' (2020) January *The Atlantic* 4. See also Yascha Mounk, *The People vs. Democracy* (Harvard University Press 2018) 149.

⁶⁴ John Naughton, *From Gutenberg to Zuckerberg* (Quercus 2012) 14.

understanding of individuals *vis-a-vis* society following the American and French Revolutions.⁶⁵

The pattern of technological innovation leading to societal concern beyond the grasp of available legal remedies is central to this thesis. Two key examples are highlighted in this section with emphasis placed upon the emergence of the legal rights to privacy and data protection. Both rights have been given distinct standing with the arrival of the Charter of Fundamental Rights of the European Union in 2000.

⁶⁵ Alexis de Tocqueville, *Ancien Regime and the Revolution*. Translated by G. Bevan (Penguin 2008[1856]). See also Raf Geenens, 'Modernity Gone Awry: Lefort on Totalitarian and Democratic Self-Representation' (2012) 13 *Critical Horizons* 74, 86; Dana Jalbert Stauffer, 'Tocqueville on the Modern Moral Situation: Democracy and the Decline of Devotion' (2014) 108 *The American Political Science Review* 772.

Chapter Two: The Foundations of Data Protection

1. Introduction

Within the EU framework, the right to data protection under the Charter holds a prominent status. The CJEU interprets this right stringently, affording it significant importance when weighed against other rights and interests. Although the Charter positions data protection alongside the more established right to privacy, it is noteworthy that the GDPR explicitly emphasises the right to data protection as its basis rather than its more traditional counterpart.

Article 7 of the Charter outlines the right to privacy in terms similar to those found in the Universal Declaration of Human Rights ('UDHR')⁶⁶ and the European Convention on Human Rights ('ECHR').⁶⁷

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

While Article 8 of the Charter provides a new right to the 'protection of personal data' not mentioned in either the UDHR or the ECHR.

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

⁶⁶ Universal Declaration of Human Rights (UDHR). Resolution 217, 10 December 1948.

⁶⁷ Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No 1-16), ETS No 005, 4 November 1950.

3. Compliance with these rules shall be subject to control by an independent authority.

In this chapter we seek to understand the origins, conceptual underpinnings, and essential components of the right to data protection under the Charter. Thereafter we will delve into the nature of the relationship between the two and ask how the right to data protection is to be distinguished from the right to privacy? This question is complicated by ambiguity over the content of the new right to data protection. As Dalla Corte explains there is no ‘univocal, authoritative conception of what constitutes the right to data protection’.⁶⁸

The first part of this chapter will explore these two rights, focusing upon their origins, conceptual underpinnings, and essential components in case law. Thereafter we will examine three possible readings of the relationship between the two rights. Attention will be given to the case law of both the CJEU and European Court of Human Rights (‘ECtHR’) throughout this analysis.

2. From Privacy to Data Protection

2.1 Early Formulations

The roots of the modern right to privacy can be traced back to the very foundations of the Western canon. Already in the 4th century BCE, Aristotle drew a distinction between the household and the public square in book I of his *Politics*.⁶⁹ The political sphere of a city, the ‘*Polis*’ is contrasted to the domestic realm of the home and domestic life, the ‘*Oikos*’. Correspondingly Roman law recognised a closed

⁶⁸ Lorenzo Dalla Corte, “A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection Hart Publishing”, *Dara Hallinan, Ronald Leenes, Serge Gutwirth and Paul De Hert (eds.), Data Protection and Privacy: Data Protection and Democracy* (Hart Publishing 2020) 28.

⁶⁹ Aristotle, *Aristotle’s Politics Translated and with an Introduction, Notes, and Glossary* by Carnes Lord (Carnes Lord tr, 2nd edn, University of Chicago Press 2013).

domestic sphere.⁷⁰ Nevertheless, it is from the eighteenth century onward, that the nascent rights from which contemporary privacy guarantees are derived began to emerge in both civil and common law jurisdictions. These early formulations laid the foundation for the modern conception of privacy rights.

Societal upheaval (the Reformation, the Enlightenment, and the Peace of Westphalia) precipitated by technological change had led to a new conception of the state, as well as individual autonomy within it.⁷¹ Constitutional developments in the French Revolution marked an initial step towards establishing a distinct right to privacy.⁷² The Constitution of 1791, the first comprehensive revolutionary framework, introduced protections against privacy infringements.⁷³ However, the emergence of privacy rights in a stable and recognisably modern form in French law can be traced to the introduction of statutory provisions governing the press in the nineteenth century. The definitive emergence of a right to privacy in French law can be attributed to the landmark decision in *Dumas v Liébert*.⁷⁴ In this case, the well-known author Alexandre Dumas had been photographed with both his wife and mistress. When the photographer subsequently reproduced these images for public sale, Dumas successfully sought an injunction against their distribution in the Parisian court. The ruling was significant in establishing that the subject of

⁷⁰ Larry Siedentop, *Inventing the Individual: The Origins of Western Liberalism* (Belknap Press of Harvard University Press 2014) 7–33.

⁷¹ Christian Reus-Smit, *Individual Rights and the Making of the International System* (Cambridge University Press 2013) 68–106. See also Claude Lefort, *Democracy and Political Theory*. Trans. D. Macey. (Polity Press 1988) 19. Richard Falk, ‘Revisiting Westphalia, Discovering Post-Westphalia’ (2002) 6 *The Journal of Ethics* 311; Mathias Risse, ‘What to Say About the State’ (2006) 32 *Social Theory and Practice* 671.

⁷² James Q Whitman, ‘The Two Western Cultures of Privacy: Dignity versus Liberty’ (2003) 113 *Yale Law Journal* 1151.

⁷³ Constitution of 3 September 1791, *Constitution du 3 septembre 1791*, tit. III, ch. V, art. 17. ‘Les calomnies et injures contre quelques personnes que ce soit relatives aux actions de leur vie privée, seront punies sur leur poursuite.’

⁷⁴ *Dumas v Liébert Cour de Paris* (25 mai 1867) *Ann Prop Ind*.

such images retained an ongoing right to withdraw consent for publication. Moreover, the court asserted that 'private life is walled off in the interest of the individual,' thereby implying a concern for the individual's ability to 'safeguard his dignity' through control over his image.⁷⁵ This ruling prefigured several themes that would become prominent in subsequent privacy jurisprudence, including the concept of personal control over one's image and information, and the recognition of potential moral harm resulting from unauthorised public exposure.⁷⁶

A comparable approach was evident during the same period in the United Kingdom through the English Common Law injunction against breach of confidence.⁷⁷ In the case of *Abernethy v. Hutchinson*⁷⁸ Lord Eldon prohibited the publication of unwritten lecture notes, basing his decision on the understanding that the information was intended solely for student education. The *Prince Albert v Strange*⁷⁹ case further extended this principle, prohibiting not only the reproduction of personal etchings but also their description or listing. This ruling parallels the French decision recognizing legal remedies for unauthorised disclosure of personal information. However, *Strange* left many questions unanswered regarding the precise nature and scope of this legal protection, despite affirming the principle of confidentiality.

⁷⁵ This decision was reinforced in *Bonnet v Société Olibet Trib Comm Seine* (13 juin 1882) *Ann Prop Ind*. While a similar judgment precedes the *Dumas* case in *Félix v O'Connell, Trib Civ Seine* (16 juin 1858) *DP* although there the Court made no reference to privacy. See Róisín Á Costello, *Privacy Law in Ireland* (Bloomsbury Publishing 2023) para 1.11; Megan Richardson, *The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea* (Cambridge University Press 2017) 148; Whitman (n 72) 1176.

⁷⁶ Costello, *Privacy Law in Ireland* (n 75) para 1.12.

⁷⁷ *ibid* 1.20-1.25; Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 207-210.

⁷⁸ *Abernethy v Hutchinson* [1825] 47 ER 1313 (*High Court of Chancery*).

⁷⁹ *Prince Albert v Strange* [1849] 2 De G & Sm 652, [1849] 64 ER 293 (*High Court of Chancery*).

Despite these developments the right to privacy's arrival in popular legal parlance is most often traced to a single article written by two American jurists at the end of the 19th century.⁸⁰ The need for such a defence emerged as Samuel Warren and Louis Brandeis noted a newly felt trespass into the personal sphere of individuals.

By the close of the 19th century technological innovation had placed a greater premium on the sanctuary of the home. A rapid wave of inventions, each changing the nature of physical and informational space, entered public life with the introduction of the commercial telegraph in 1874. This invention was quickly overshadowed by the first telephonic conversation in 1876. Likewise, the typewriter (1874), microphone (1876), and dictaphone (1889) were all to be found before Brandeis and Warren penned their article and brought the right to privacy into legal discourse.⁸¹ The true object of their ire, however, was the snap camera.⁸² The invention of the 'snap' camera in 1888 fundamentally changed photography making it a far less onerous process.⁸³ Early photography could not easily take place without the willing consent and attentive cooperation of the subject. Now such assent was no longer required.⁸⁴ The pairing of this new invasive technology

⁸⁰ Dorothy J Glancy, 'The Invention of the Right to Privacy' (1979) 21 *Arizona Law Review* 1, 1. For a detailed discussion of the right's origins see Róisín Áine Costello, *Privacy Law in Ireland* (Bloomsbury Publishing 2023) Section I.

⁸¹ *ibid* 25; Seipp (n 55) 105; Alfred W McCoy, *Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State* (University of Wisconsin Press 2009) 21–23. See also Friedrich A Kittler, *Gramophone, Film, Typewriter* (Stanford University Press 1999).

⁸² Róisín Á Costello, 'Warren and Brandeis and the Right to Privacy's Hollow Core.' [2015] *Kings Inns Law Review* 3 <<https://ssrn.com/abstract=3059762>> accessed 10 March 2024.

⁸³ Miles Orvell, *American Photography* (Oxford University Press 2003) 35. See also Reese V Jenkins, 'Technology and the Market: George Eastman and the Origins of Mass Amateur Photography' (1975) 16 *Technology and Culture* 1; Richard S Tedlow, 'The Beginning of Mass Marketing in America: George Eastman and Photography as a Case Study' (1997) 17 *Journal of Macromarketing* 67.

⁸⁴ The lack of consent required was a point emphasised in advertisements for a variety of new cameras, which were shaped to resemble other objects including hip flasks and binoculars Igo (n 53) 30.

with tabloid journalism, which had already been accused of breaching the confines of decency, threatened to override considerations of private sanctity entirely.⁸⁵

Warren and Brandeis employed the term the ‘right to be let alone’ to explain the meaning of privacy. This phrasing was borrowed from Thomas Cooley, Chief Justice of the Michigan Supreme Court. In Cooley’s rendering ‘The right to one’s person may be said to be a right of complete immunity: to be let alone’.⁸⁶ Warren and Brandeis maintained that privacy is not to be conceived of as a property right. Rather, the concept is to be understood as a right that enables people to create the space in which they can formulate, develop, and exercise the personal thoughts, ideas, and beliefs which they might not otherwise wish to be made public.⁸⁷ This articulation can be likened to the German constitutional concept of *Persönlichkeitsrecht*⁸⁸ – the right to develop one’s identity and personality, or as Warren and Brandeis put it, the principle of ‘an inviolate personality’.⁸⁹

2.2 20th Century Developments

While a right to privacy had at last been articulated by the close of the 1800s, it would only arrive in legal application decades into the next century, following a

⁸⁵ Irwin R Kramer, ‘The Birth of Privacy Law: A Century since Warren and Brandeis’ (1989) 39 Catholic University Law Review 703, 710; Ben Bratman, ‘Brandeis and Warren’s the Right to Privacy and the Birth of the Right to Privacy’ (2001) 69 Tenn. L. Rev. 623, 629.

⁸⁶ Thomas M Cooley, *A Treatise on the Law of Torts, or the Wrongs Which Arise Independently of Contract* (3rd Edition, Callaghan & company 1906) 33.

⁸⁷ Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford Law Books 2010) 19. See also Glancy (n 80); Igo (n 53) 38.

⁸⁸ Jens Kremer, ‘On the End of Freedom in Public Spaces: Legal Challenges of Wide-Area and Multiple-Sensor Surveillance Systems’, *Surveillance, counter-terrorism and comparative constitutionalism* (Routledge 2014); Bart Van Der Sloot, ‘Privacy as Personality Right: Why the ECtHR’s Focus on Ulterior Interests Might Prove Indispensable in the Age of “Big Data”’ (2015) 31 Utrecht Journal of International and European Law 25.

⁸⁹ Warren and Brandeis (n 24) 205.

wave of technological and societal innovation. More significantly large-scale loss of civilian life in World War II led to a dramatic reinterpretation of the role of states *vis-à-vis* the individual. The 1945 Nuremberg trials of Nazi war criminals ended the hitherto accepted notion of virtually limitless state sovereignty which had been entrenched by the 1648 Treaty of Westphalia.⁹⁰ Instead an increasing acknowledgement of individual rights defined the latter half of the 20th Century in Europe.⁹¹

The centrality of the rights-based order is exhibited by the adoption of the United Nations' Universal Declaration of Human Rights ('UDHR') in 1948. Although never intended to bind states,⁹² the Declaration was to serve as 'a jurisprudential underpinning for political or philosophical assertions of the dignity of the individual irrespective of local, domestic laws'.⁹³

The inclusion of a right to privacy in the UDHR reflects the success of Warren and Brandeis' theoretical approach. The right found its guarantee in the Declaration through Article 12:

⁹⁰ Izidor Janžekovič, 'The Balance of Power from the Thirty Years' War and the Peace of Westphalia (1648) to the War of the Spanish Succession and the Peace of Utrecht (1713)' (2023) 49 *History of European Ideas* 561.

⁹¹ RI Rotbert, 'Deterring Mass Atrocity Crimes: The Cause of Our Era,' *Rotberg, R.I. (ed.), Mass Atrocity Crimes: Preventing Future Outrages* (Brookings Institution Press 2010) 1. Igo (n 53) 144. A Hehir, 'The Responsibility to Protect in International Political Discourse: Encouraging Statement of Intent or Illusory Platitudes?' (2011) 15 *The International Journal of Human Rights*, 72. Don Hubert, 'The Responsibility to Protect: Preventing and Halting Crimes Against Humanity' in Robert I Rotbert (ed), *Mass Atrocity Crimes: Preventing Future Outrages* (Brookings Institution Press) 89.

⁹² Samuel Moyn, *The Last Utopia: Human Rights in History* (Harvard University Press 2012) 44–85.

⁹³ Elizabeth Borgwardt, *A New Deal for the World: America's Vision for Human Rights* (Harvard University Press 2007) 242. See also Mark Bradley, *The World Reimagined: Americans and Human Rights in the Twentieth Century* (Cambridge University Press 2016); Raddivari Revathi, 'Evolution of Privacy Jurisprudence – A Critique' (2018) 60 *Journal of the Indian Law Institute* 189; O Diggelmann and MN Cleis, 'How the Right to Privacy Became a Human Right' (2014) 14 *Human Rights Law Review* 441.

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.⁹⁴

Here, privacy is rendered in line with Warren and Brandeis' articulation of the 'right to be let alone'. As in the case of the lawyers' conception, Article 12 of the UDHR provides only a vague understanding of what the content of privacy is in reality.

Igo notes that despite the heavy scrutiny which the Declaration received there was silence when it came to the right to privacy.⁹⁵ Instead 'privacy was taken to be part of an assumed bundle of protections concerning people, their dwellings, and their papers.' Its roots were understood to be tied to 'a line of distinguished documents, from the French Declaration of Human Rights (1789, 1793) and the United States Bill of Rights (1791) to the Atlantic Charter (1941) and Bogota Declaration (1948)'.⁹⁶ Despite this level of agreement, there was very little in the way of tangible gains found through the incorporation of privacy into the Declaration. As a non-binding document its concerns quickly fell away when balanced against the practical considerations of Cold-War fears.⁹⁷

⁹⁴ The UDHR's formulation was almost entirely reused in the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 lays out the right to privacy:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

⁹⁵ Igo (n 53) 145.

⁹⁶ *ibid.* See also Moyn (n 195) 44–83; Diggelmann and Cleis (n 93).

⁹⁷ Bradley (n 93).

2.3 European Incorporation

Arriving five years after the UDHR, the European Convention on Human Rights (‘ECHR’) entered into force on 3 September 1953. This legal instrument bound all members of the newly formed Council of Europe.⁹⁸ Once more a right to private life was articulated in Article 8 of the ECHR:

- 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
- 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Already an expansion to the content of the UDHR’s corresponding right may be seen. There, only ‘arbitrary interference’ with the right to privacy was prohibited. While in the case of Article 8 of the ECHR a number of conditions are required for any interference *whatsoever* by the state.

Arriving nearly fifty years later, the CFEU retained an almost identical articulation of the right to privacy as reflected in *Table 1* below.

Table 1. Comparison: Article 7 of CREU and Article 8(1) ECHR

Article 7, CFREU	Article 8(1), ECHR

⁹⁸ Sian Rudgard, ‘Origins and Development of European Data Protection Law’ in Eduardo Ustaran (ed), *European Data Protection* (2nd edn, IAPP Publications 2019).

Everyone has the right to respect for his or her private and family life, home and communications.⁹⁹

Everyone has the right to respect for his private and family life, his home and his correspondence.¹⁰⁰

Aside from the change to more gender inclusive language, the substance of the text remains the same. Three of the four protected elements (private life, family life, and home) are identical. While the final element has been changed from ‘correspondence’ to ‘communications.’ We may understand this alteration to be a natural linguistic adaptation reflecting the impacts of fifty years of technological change on speech.¹⁰¹ Beyond the correspondence of the two texts, the Explanations which accompany the Charter clarify that Article 7 ‘corresponds’ to the ECHR’s rendering of the right.¹⁰²

Moreover, per Article 52(3), rights within the Charter that are derived from the ECHR should be interpreted in harmony with the case law of the ECtHR.¹⁰³ In *La Quadrature du Net*, the CJEU explained the purpose of Article 52(3) to be ensuring ‘the necessary consistency between the rights contained in the Charter and the corresponding rights guaranteed in the ECHR.’¹⁰⁴ This is to be achieved without compromising the independence of EU law and the jurisdiction of the CJEU. The

⁹⁹ Emphasis added.

¹⁰⁰ Emphasis added.

¹⁰¹ Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 71.

¹⁰² Explanation on Article 7, Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/17.

¹⁰³ Costello, *Privacy Law in Ireland* (n 75) para 4.04.

¹⁰⁴ *Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others v Premier ministre and Others* [2020] EU:C:2020:791 at [124].

Court further noted that when interpreting the Charter, the corresponding rights of the ECHR should be considered as the minimum level of protection.¹⁰⁵

This threshold provides the CJEU with an extensive basis from which to begin its own analysis. Indeed, the ECtHR has addressed over 6 000 cases relating to Article 8 of the ECHR, a figure that significantly surpasses the more infrequent case law of the CJEU on Article 7 of the Charter. The ECtHR's body of case law is not only more extensive but also broader in scope compared to that of the CJEU. This is because, unlike the Charter, which is applicable within the specific context of EU law, the ECHR operates under a distinct legal framework established by the Treaty of London and is not confined to the legal order of the EU.¹⁰⁶

The ECtHR has applied Article 8 ECHR expansively, covering areas far beyond those which could have been contemplated at the time of its adoption. This includes aspects such as collective health protection,¹⁰⁷ personal data processing,¹⁰⁸ and environmental conservation.¹⁰⁹

In responding to the ECtHR's extensive Article 8 case law, the CJEU has thus far either interpreted these matters independently or drawn broad analogies to the

¹⁰⁵ *ibid.*

¹⁰⁶ Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 72.

¹⁰⁷ See *Vavříčka v The Czech Republic* Application nos 47621/13, 3867/14, 73094/14, 19298/15 19306/15, and 43883/15 [2021] CE:ECHR:2021:0408JUD004762113.

¹⁰⁸ See Registry of the European Court of Human Rights (ECtHR), 'Guide to the Case-Law of the of the European Court of Human Rights - Data Protection (Last Updated on 31 August 2022)' <https://www.echr.coe.int/documents/d/echr/Guide_Data_protection_ENG> accessed 10 March 2024.

¹⁰⁹ See *López Ostra v Espagne* Application no 16798/90 [1994] CE:ECHR:1994:1209JUD001679890. *Çiçek and Others v Turkey* no 44837/07 [2020] CE:ECHR:2020:0204DEC004483707; *Hatton v the United Kingdom* [GC] Application no 36022/97 [2003] CE:ECHR:2003:0708JUD003602297.

ECtHR's jurisprudence.¹¹⁰ Importantly some aspects of the ECtHR's jurisprudence on Article 8(1) in fact relate to other rights in the Charter. An individual's right to physical and psychological integrity is protected by Article 3 of the Charter and would not be decided under the right to privacy in Article 7. Similarly, the right to environmental protection is covered by Article 37 of the Charter.¹¹¹ Thus we must conclude that the right to privacy under Article 7 of the Charter protects a narrower set of interests than its corresponding provision in Article 8 of the ECHR.¹¹²

3. The Emergence of Data Protection

3.1 Technological and Societal Context

An important factor in the evolution of Privacy and Data Protection Law throughout the 20th century was the administrative state which grew in its capacity following the global financial crash of 1929.¹¹³ As Wiggins and Jones explain, '[f]rom the 1930s, government statisticians introduced techniques of representative sampling to make novel claims about the nation as a whole.'¹¹⁴ Once more the individual was forced to reimagine her relationships to others, especially the state which had previously left her with far greater anonymity. Albeit this anonymity had been the natural result of governmental disinterest and neglect.

¹¹⁰ Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 73. See also Costello, *Privacy Law in Ireland* (n 75) ch 4.

¹¹¹ See *Case C-28/09 Commission v Austria* [2011] EU:C:2011:854.

¹¹² Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 75.

¹¹³ Igo (n 53) 56; Stephen Skowronek, *Building a New American State: The Expansion of National Administrative Capacities, 1877-1920* (Cambridge University Press 1982); Gary Lawson, 'The Rise and Rise of the Administrative State' (1994) 107 *Harvard Law Review* 1231; Eliza Wing-yee Lee, 'Political Science, Public Administration, and the Rise of the American Administrative State' [1995] *Public Administration Review* 538.

¹¹⁴ Chris Wiggins and Matthew L Jones, *How Data Happened: A History from the Age of Reason to the Age of Algorithms* (First edition, W W Norton & Company 2023) 74.

The introduction of a social welfare system propped up with citizen identifiers found darker reflections in the emergence of the totalitarian states of the USSR under Stalin and Nazi Germany under Hitler.¹¹⁵ These regimes were defined by the absolute unification of all elements of society under the party – an entity which is present at every level of the public body. In Hannah Arendt’s famous rendering ‘[b]y pressing men against each other, total terror destroys the space between them.’¹¹⁶

For leading scholars this new form of state was seen as fundamentally linked to the rise of technology and modern life.¹¹⁷ Raymond Aron and Hannah Arendt both understood totalitarianism as representing modernity’s drive for technical mastery reflected in society. This is described by Raymond Aron as the ‘promethean ambition’ of humanity to respond to the ever-increasing demands of mechanisation. Similarly, Arendt framed totalitarianism as modernity ‘writ large’.¹¹⁸ As such the increase of state knowledge, even in Western Europe and the USA was to be treated with suspicion towards a naturally centralising tendency.

This greater state role also came with an increased cost. As Newman explains, in the post-World War II era, the scope of central government responsibilities, encompassing areas from economic regulation to national security, expanded significantly. From 1950 to 1970, government spending in the United States experienced a notable increase of 7 percent, escalating from 21 to 28 percent of the

¹¹⁵ Adam Tooze, *Statistics and the German State, 1900-1945: The Making of Modern Economic Knowledge* (Cambridge University Press 2001). See also Igo (n 53) 55–59.

¹¹⁶ Hannah Arendt, *The Origins of Totalitarianism* (Kindle edn, Penguin 2017) 612.

¹¹⁷ Raf Geenens, ‘Modernity Gone Awry: Lefort on Totalitarian and Democratic Self-Representation’ (2012) 13 *Critical Horizons* 74, 80.

¹¹⁸ Bernard Flynn, *The Philosophy of Claude Lefort: Interpreting the Political* (Northwestern University Press 2005) 259.

Gross Domestic Product (GDP). Welfare spending also saw a major surge from under \$1 billion in 1950 to an excess of \$36 billion by 1970. This pattern was not exclusive to the United States, instead it reflected a broader trend across the advanced industrial democracies. As the complexity of governance intensified, public administrators actively sought out new tools to enhance economic strategy formulation and streamline government operations.¹¹⁹

The drive for extensive data gathering was paralleled by the creation of systems that facilitated the automated processing of this information, exemplified by the early Hollerith punched card machines.¹²⁰ Tooze suggests that through these machines ‘bureaucrats were inspired to dreams of omniscience’ as it ‘became possible to conceive of an entire nation recorded in a single database instantly accessible by means of mechanical handling equipment.’¹²¹

From the outset this growth of computing in public life was met with concern over its potential impact on privacy.¹²² Two US Congressional hearings were held on *The Computer and Invasion of Privacy* in 1965,¹²³ while further Senate hearings took

¹¹⁹ Abraham L Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Cornell University Press 2008) 43.

¹²⁰ Steven Lubar, ‘“Do Not Fold, Spindle or Mutilate”: A Cultural History of the Punch Card’ (1992) 15 *Journal of American Culture* 43. George Strawn, ‘Masterminds of Punched Card Data Processing: Herman Hollerith and John Billings’ (2023) 25 *IT Professional* 90.

¹²¹ Tooze (n 115) 24.

¹²² A significant contribution in this field is *Databanks in a Free Society*, a seminal work on the rise of automated computing and the resultant impact on civil rights which was published in 1972 by Alan Westin and Michael Baker. Alan F Westin and Michael A Baker, *Databanks in a Free Society* (Quadrangle Books 1972).

¹²³ United States House of Representatives, ‘The Computer and Invasion of Privacy: Hearings before a Subcommittee on Government Operations, House of Representatives, Eighty-Ninth Congress, First Session, July 2, 3, 4, 7, 23 and September 23. Part 1 and Part 2, 1965.’ <<https://babel.hathitrust.org/cgi/pt?id=uc1.a0000162578&seq=5>> accessed 29 July 2023.

place in 1967¹²⁴ and 1971.¹²⁵ Additionally, the Rand Corporation would publish numerous studies of their own on the issue of automated databanks.¹²⁶ Despite this US focus, it was ultimately in Europe that the first laws addressing concerns over data processing emerged.

3.2 European Developments

When charting the evolution of European Data Protection Law, we can pinpoint three distinct eras: (i) the initial phase of crafting national data protection laws during the 1970s, (ii) the period of internationalisation in the early 1980s, and (iii) the ongoing era of European harmonisation that began in 1995.¹²⁷

In the 1970s, various European countries began to implement provisions regulating the automated processing of data. Pioneers in this legislative activity included the German federal state of Hesse, as well as Sweden and France, which were among the first in Europe to adopt legal acts concerning the processing of information related to individuals. These acts marked the beginning of an initial wave of regulatory activity starting in 1970. These laws generally took two forms: ad-hoc acts or constitutional-level provisions. Each approach advanced a distinct legal framework for protecting individuals against automated data processing,

¹²⁴ United States Senate, 'Computer Privacy. Hearings, Ninetieth Congress, First Session, Pursuant to S. Res. 25. March 14 and 15, 1967.'
<<https://babel.hathitrust.org/cgi/pt?id=osu.32437121556241&seq=7>> accessed 29 July 2023.

¹²⁵ United States Senate, 'Federal Data Banks, Computers, and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-Second Congress, February 23-25, and March 2-15 and 17, 1971.'
<<https://babel.hathitrust.org/cgi/pt?id=uc1.c051765460&seq=11>> accessed 29 July 2023.

¹²⁶ Paul Armer, 'Computer Aspects of Technological Change, Automation, and Economic Progress, Paper P-347'; Jay John Hellman, 'Privacy and Information Systems: An Argument and an Implementation',.

¹²⁷ Brendan van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia 2019) 151.

often employing varied terminology and differing perspectives on the rights and freedoms involved. Few of these early laws directly referred to what we now understand as data protection, and even fewer associated their provisions explicitly with privacy.¹²⁸

Following the first wave of legislation three European states – Portugal,¹²⁹ Spain,¹³⁰ and Austria¹³¹ – chose to include data protection provisions within their constitutions by the end of the 1970s.¹³² Mirroring these first attempts at a national level; regional and international efforts to balance technological growth with concern for individual freedom led to new legal measures. The 1980s began with two significant multi-national instruments to strengthen data protection. In 1980 the OECD released its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,¹³³ while the Council of Europe introduced Convention 108 in 1981.¹³⁴ Both Convention 108 and the OECD Guidelines sought to create a harmonised approach to Data Protection Law. The primary contribution of the OECD Guidelines lies in the set of principles which they introduced.¹³⁵ These serve as the basis for contemporary Data Protection Law.¹³⁶ Convention 108 mirrors

¹²⁸ Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer International Publishing 2014) 55.

¹²⁹ Constitution of Portugal, Constituição Da República Portuguesa 1976. Article 35.

¹³⁰ Constitution of Spain, Constitución Española, 1978. Article 18(4).

¹³¹ Federal Act of 18 October 1978 on the protection of personal data, Bundesgesetzblatt für die Republik Österreich 1978 (Austria).

¹³² González Fuster (n 128) 68–70.

¹³³ Organisation for Economic Co-operation and Development ('OECD') (n 58).

¹³⁴ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

¹³⁵ Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma', (2013) 126 Harvard Law Review 1880, 1882.

¹³⁶ Newman (n 119) 25.

these principles,¹³⁷ while also supplying special rules on transborder data flows,¹³⁸ and mechanisms for mutual assistance.¹³⁹

In particular, the European Commission viewed Convention 108 as a chance to lay down unified rules within the European Community. It issued a recommendation for Member States to ratify Convention 108 by 1982's end, keeping the option to introduce legislation if non-compliance persisted.¹⁴⁰ However, this subtle bid to unify national legislation did not meet success. By 1990, only seven Member States had given approval to Convention 108, and their enacted laws varied considerably. Furthermore, the discretion given to the interpretation of the principles instead led to a data protection regime which differed from country to country. Thus, despite the Commission's inclination for a natural evolution of uniform national data protection laws, it was compelled to actively intervene to align national laws.¹⁴¹

Seeking to redress this imbalance, the European Commission proposed a data protection law in 1990.¹⁴² The framework of data protection principles served as the basis of this new approach. The result was the 1995 Data Protection

¹³⁷ Convention 108, Chapter II.

¹³⁸ *ibid.* Chapter III.

¹³⁹ *ibid.* Chapter IV.

¹⁴⁰ European Commission, 'Recommendation of 29 July 1981 Relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [1981] OJ L246/31.'

¹⁴¹ Orla Lynskey, *The Foundations of EU Data Protection Law* (First edition, Oxford University Press 2015) 48; Sian Rudgard, 'Origins and Development of European Data Protection Law', in: *Ustaran, Eduardo et al. European Data Protection* (Second Edition, IAPP Publications 2019). Section 1.4

¹⁴² 'Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM (90) 314 Final – SYN 287' Official Journal of European Communities.

Directive.¹⁴³ Significantly the passing of the Directive marked the passing of data protection leadership to the EU from the Council of Europe following the inadequacies of Convention 108. The Directive sought to supplement Convention 108 by providing high level requirements for the protection of personal data which were to be implemented at national level by member states.¹⁴⁴ The key regime of the Data Protection Directive has been incorporated directly into the GDPR and expanded within it.

With the inception of the Charter in 2000, the right to data protection was given standing, independent of the right to privacy. However, this is not the only articulation of the right to data protection to have emerged through the Lisbon Treaty.¹⁴⁵ Article 16 of the amended Treaty of the Functioning of the European Union ('TFEU') reasserts a right to data protection.¹⁴⁶

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

¹⁴³ González Fuster (n 128) 125.

¹⁴⁴ In contrast to a European Commission Regulation, a European Commission Directive is not automatically applicable within the member states of the European Union. Instead a Directive is binding upon member states, but leaves to 'national authorities the choice of form and methods' for implementation.

¹⁴⁵ Consolidated versions of the Treaty on European Union ('TEU') and the Treaty on the Functioning of the European Union ('TFEU') [2016] OJ C202/1, 7 June 2016 ('Lisbon Treaty').

¹⁴⁶ *ibid.*

While Article 39 of the Treaty of the European Union¹⁴⁷ further expands upon the operationalisation of the right to Data Protection.

In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

Article 16 of the TFEU and Article 39 of the TEU hold a two-fold function. First, they validate the status of the right to data protection. Additionally, they assign the task of further fleshing out this right to secondary legislation.¹⁴⁸ Both Articles mandate a concrete responsibility on the legislative body to introduce new regulations associated with the 'protection of individuals in relation to the processing of personal data' as well as the unimpeded movement of such data.¹⁴⁹ It is in this secondary legislation that the boundaries, and content of the right to data protection is firmly established.

4. Conceptual Foundations

4.1 Privacy's Conceptual Disarray

In understanding the conceptual foundations of Data Protection we may first begin by analysing the wider debates which surround the right to privacy more

¹⁴⁷ Consolidated versions of the Treaty on European Union ('TEU') and the Treaty on the Functioning of the European Union ('TFEU') [2016] OJ C202/1, 7 June 2016 ('Lisbon Treaty').

¹⁴⁸ Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 98–102.

¹⁴⁹ *ibid* 99.

generally. The pursuit of a universally accepted and satisfactory definition of privacy has proven to be an arduous task. We are faced with addressing what Costello refers to as ‘privacy’s hollow core’.¹⁵⁰ The multifaceted nature of privacy, encompassing informational, decisional, physical, and proprietary dimensions, often presents competing and even contradictory aspects that resist singular characterisation. Key accounts include:

1. **Limited Access to the Self** – the ability to shield oneself from unwanted access by others. The ‘Access Account’ has been developed by Thomson,¹⁵¹ Gavison,¹⁵² Bok,¹⁵³ O’Brien,¹⁵⁴ Allen,¹⁵⁵ van den Haag,¹⁵⁶ and Macnish¹⁵⁷ among others. An early articulation of this argument is made by E.L. Godkin in the late 19th century, who argues that ‘nothing is better worthy of legal protection than private life.’ This protection of private life translates into the ‘right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion.’¹⁵⁸

¹⁵⁰ Costello, ‘Warren and Brandeis and the Right to Privacy’s Hollow Core.’ (n 82) 2.

¹⁵¹ Judith Jarvis Thomson, ‘The right to privacy’ (1975) 4 *Philosophy and Public Affairs* 295.

¹⁵² Ruth Gavison, ‘Privacy and the Limits of Law’ (1980) 89 *The Yale Law Journal* 421.

¹⁵³ Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Vintage Books 1989).

¹⁵⁴ David M O’Brien, *Privacy, Law, and Public Policy* (Praeger 1979).

¹⁵⁵ Judith Wagner DeCew and Anita L Allen, ‘Uneasy Access: Privacy for Women in a Free Society.’ (1992) 101 *The Philosophical Review* 709; Anita L Allen, *Why Privacy Isn’t Everything: Feminist Reflections on Personal Accountability*, vol 21 (Rowman & Littlefield Publishers 2003).

¹⁵⁶ Ernest van den Haag, ‘On Privacy’ (1971) 13 *Nomos: Yearbook of the American Society for Political and Legal Philosophy* 149.

¹⁵⁷ Kevin Macnish, ‘Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World’ (2018) 35 *Journal of Applied Philosophy* 417.

¹⁵⁸ EL Godkin, ‘Libel and Its Legal Remedy’ [1880] *The Atlantic* <<https://www.theatlantic.com/magazine/archive/1880/12/libel-and-its-legal-remedy/632214/>> accessed 8 July 2023.

2. **Secrecy**—the concealment of certain matters from others. This perspective suggests that privacy is breached when previously hidden information is made public. Noteworthy exponents of this account include Posner¹⁵⁹ and Jourard.¹⁶⁰ Privacy as secrecy can be perceived as a specific variant of the Access Account. In Solove's wording '[s]ecrecy of personal information is a way to limit access to the self.'¹⁶¹ The clandestine nature of personal information represents one method of self-access limitation. This perception is more confined than the broad conceptualizations of the Access Account since confidentiality pertains solely to the hiding of personal details.¹⁶²

3. **Privacy as Control** – This rendering finds its roots in Alan Westin's *Privacy and Freedom*. Here, Westin defines privacy as the 'claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'¹⁶³ Beyond Westin's formulation the control account has been developed by Fried,¹⁶⁴ Gross,¹⁶⁵

¹⁵⁹ Richard A Posner, *The Economics of Justice* (Harvard University Press 2003) 271.

¹⁶⁰ Sidney M Jourard, 'Some Psychological Aspects of Privacy' (1966) 31 *Law and Contemporary Problems* 307, 307.

¹⁶¹ Daniel J Solove, *Understanding Privacy* (Harvard University Press 2010) 22.

¹⁶² *ibid* 21.

¹⁶³ Alan F Westin, *Privacy and Freedom* (Scribner 1967) 7.

¹⁶⁴ Charles Fried, 'Privacy' (1968) 77 *The Yale Law Journal* 475.

¹⁶⁵ Hyman Gross, 'Privacy and Autonomy' (1971) 13 *Nomos: Yearbook of the American Society for Political and Legal Philosophy* 169.

Altman,¹⁶⁶ Parent,¹⁶⁷ Bezanson,¹⁶⁸ and Inness,¹⁶⁹ among others.¹⁷⁰ In Fried's rendering '[p]rivacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.' Thus, the loss of control over personal information equates to a decrease in privacy.¹⁷¹

4. **Personhood**—the protection of one's personality, individuality, and dignity. The 'Personhood Account' diverges from the previously mentioned models as it hinges on a normative goal of privacy—safeguarding personality integrity. Drawing on Warren and Brandeis' concept of 'inviolate personality' Freund introduces the term 'personhood'.¹⁷² Benn too, puts forward a personhood perspective on privacy, characterising privacy as acknowledgement for individuals as decision-makers.¹⁷³ As Murphy explains, 'while an individual may not always need to keep secrets in order to be autonomous, the possession of the ability to keep secrets is vital if individuals are to make truly autonomous choices.'¹⁷⁴ This conception is not mutually exclusive with the others cited in

¹⁶⁶ Irwin Altman, 'Privacy: A Conceptual Analysis' (1976) 8 *Environment and Behavior* 141.

¹⁶⁷ WA Parent, 'Privacy, Morality, and the Law' (1983) 12 *Philosophy and Public Affairs* 269.

¹⁶⁸ Randall P Bezanson, 'The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990' (1992) 80 *California Law Review* 1133.

¹⁶⁹

¹⁷⁰ See Richard Parker, 'A Definition of Privacy' (1974) 27 *Rutgers Law Review* 275; Thomas Scanlon, 'Thomson on Privacy' (1975) 4 *Philosophy and Public Affairs* 315; Stephen T Margulis, 'Conceptions of Privacy: Current Status and Next Steps' (1977) 33 *Journal of Social Issues* 5; Allen (n 100); Beate Rossler, *The Value of Privacy* (Polity Press 2005); M. Ryan Calo, 'The Boundaries of Privacy Harm' (2011) 86 *Indiana Law Journal* 1131.

¹⁷¹ Macnish (n 157) 419; Björn Lundgren, 'A Dilemma for Privacy as Control' (2020) 24 *The Journal of Ethics* 165.

¹⁷² Paul Freund, 'Address at the American Law Institute, 52nd Annual Meeting 42-43'.

¹⁷³ Stanley I Benn, 'Privacy, Freedom, and Respect for Persons' in Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy* (1st edn, Cambridge University Press 1984).

¹⁷⁴ Murphy, *Surveillance and the Law* (n 57) 9.

this chapter. Rather, it is frequently invoked alongside them to expound on the significance of privacy, the facets of the self that should be restricted, or the information over which we should exercise control.

5. **Privacy as Intimacy** – ‘Intimacy Accounts’ maintain that privacy is vital not only for the formation of the individual self, but also for fostering human connections. This theory identifies the worth of privacy in the nurturing of personal relationships.¹⁷⁵ We establish relations with varying depths of intimacy and self-disclosure, and we appreciate privacy so that we can uphold the preferred levels of intimacy for each of these relationships. Gerstein posits that ‘intimate relationships would cease to exist if we did not persistently demand privacy for them.’¹⁷⁶

Each of these accounts holds limitations. For instance Intimacy Accounts are often labelled as excessively expansive, as they fail to aptly delineate the scope of ‘intimacy.’ They can likewise be overly restrictive as they concentrate too intensely on personal relationships and the specific emotions evoked by them. Although trust, love, and intimacy are nurtured by privacy, these are not the sole objects to be protected by it. As DeCew notes, data regarding our finances is private but not intimate.¹⁷⁷

In a similar vein the Access Account is unable to provide a classification of the private realm itself. In reality, not every instance of access to an individual

¹⁷⁵ Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (1st Vintage Books ed, Vintage Books 2001) 8.

¹⁷⁶ Robert S Gerstein, ‘Intimacy and Privacy’ in Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press 1984) 265.

¹⁷⁷ Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press 1997) 56.

infringes upon their privacy. Instead, a privacy violation would only result from access to certain aspects of the individual or particular information and affairs. The Access Account does not provide clarity on the extent of the access which equates to a privacy violation. Within the spectrum from no access whatsoever to complete access, the crucial task is determining the boundary line.

Similarly, Control Accounts present a conception that is too wide-ranging. Gerety argues that Control Accounts encompass ‘complete control over all data about oneself, one’s group, and one’s institutions. Undoubtedly, in both law and personal experience, privacy should amount to significantly less than this.’¹⁷⁸ Furthermore, Hartzog criticises the Control Model as illusory, overwhelming, and myopic, instead advocating for design rules and a more effective structural allocation of power.¹⁷⁹

The breadth of privacy as a concept as well as the shortcomings of individual conceptions have led scholars to question the feasibility of seeking a comprehensive definition.¹⁸⁰ In response to this difficulty, Solove put forth an alternative approach through numerous writings in the first decade of the 2000s.¹⁸¹ Rather than attempting to distil privacy into a single, all-encompassing definition,

¹⁷⁸ Tom Gerety, ‘Redefining Privacy’ (1977) 12 Harvard Civil Rights and Civil Liberties Law Review 262–263.

¹⁷⁹ Woodrow Hartzog, *Privacy’s Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018); Woodrow Hartzog, ‘The Case Against Idealising Control’ (2018) 4 European Data Protection Law Review <<https://doi.org/10.21552/edpl/2018/4/5>>.

¹⁸⁰ Maria P Angel and Ryan Calo, ‘Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy’ (2024) 124 Columbia Law Review 507, 519. See in particular Daniel J Solove, ‘Conceptualizing Privacy’ (2002) 90 California Law Review 1087, 1125; Woodrow Hartzog, ‘What Is Privacy? That’s the Wrong Question’ (2021) 88 University of Chicago Law Review 1677; Robert C Post, ‘Three Concepts of Privacy’ (2001) 89 The Georgetown Law Journal 2087; Thomson (n 151).

¹⁸¹ Solove, ‘Conceptualizing Privacy’ (n 180); Daniel J Solove, ‘A Taxonomy of Privacy’ (2006) 154 University of Pennsylvania Law Review 477; Solove, *Understanding Privacy* (n 161).

Solove proposed a taxonomy of activities that give rise to privacy concerns. In his words, '[p]rivacy is not one thing, but a cluster of many distinct yet related things.'¹⁸²

This approach recognises that the myriad of invasions falling under the umbrella of privacy may differ from one another in their specific manifestations, yet share sufficient commonalities to be considered part of the same conceptual family. These activities exhibit what philosopher Ludwig Wittgenstein termed a 'family resemblance', impinging upon individuals in related ways and constituting a cluster of related privacy problems.¹⁸³ Wittgenstein introduced the notion of family resemblance to describe the way in which various uses of a term or concept may be related, not by a single common feature, but by a network of overlapping similarities.

To identify and classify these privacy-related activities, Solove employed the criterion of 'social recognition'. By examining the extent to which society acknowledges and responds to various privacy harms, Solove identified a total of 16 harmful activities under four overarching categories, (I) information collection, (II) information processing, (III) Information dissemination, and (IV) Invasion. The full division is represented in *Table 2* below:

Table 2. Solove's Taxonomy of Privacy

Overarching Group	Activities
Information Collection	• Surveillance • Interrogation
Information Processing	• Aggregation

¹⁸² Solove, *Understanding Privacy* (n 161) 40.

¹⁸³ Ludwig Wittgenstein, *Philosophical Investigations* (Basil Blackwell 1968) ss 66–67.

	• Identification • Insecurity • Secondary Use • Exclusion
Dissemination of Information	• Breach Of Confidentiality • Disclosure • Exposure • Blackmail • Appropriation • Distortion
Invasion	• Intrusion • Decisional Interference

This division is only one of the possibilities available. Costello for instance identifies three ‘genres’ of privacy: relational, spatial, and informational.¹⁸⁴ While, González Fuster begins her account of the evolution of the Right to Data Protection by ‘mapping’ privacies,¹⁸⁵ Calo focuses on different types of privacy harms.¹⁸⁶

Calo has been a consistent critic of Solove’s approach arguing that it lacks both a limiting principle and a rule of recognition.¹⁸⁷ In 2024 a renewed debate over the value of Solove’s approach and accompanying taxonomy emerged with Angel and Calo arguing against what they consider arbitrary criteria for selecting what falls within the canon of privacy scholarship and Solove defending the value of

¹⁸⁴ Costello, *Privacy Law in Ireland* (n 75) para 3.56-3.131.

¹⁸⁵ González Fuster (n 128) 21–49. It is notable that cartographical metaphors are common in this area, with Solove commenting noting that he original intended to label his taxonomy as ‘A Cartography of Privacy’ Daniel J Solove, ‘Against Privacy Essentialism’ [2024] SSRN Electronic Journal 9 <<https://www.ssrn.com/abstract=4826385>> accessed 25 July 2024.

¹⁸⁶ M. Ryan Calo (n 170).

¹⁸⁷ *ibid* 1139–42.

his original articulation.¹⁸⁸ However, we may note the primary value of this approach in shifting the focus from a search for a universal definition to a more pragmatic examination of the concrete ways in which privacy is threatened and violated in contemporary society.

4.2 Data Protection and Informational Self-Determination

The right to data protection is commonly linked to the conception of Informational Self-Determination as first developed by the Federal Constitutional Court of Germany in its 1983 *Census Decision*.¹⁸⁹ The decision represents a vital development in the evolution of European Data Protection Law as Thouvenin suggests that '[i]nformational self-determination may well be the underlying rationale of the fundamental right to the protection of personal data.'¹⁹⁰

The origins of informational self-determination are rooted in the 1982 census law, unanimously passed by the German parliament. This law permitted the state to amass extensive demographic data about its citizens via a questionnaire comprising over 160 questions.¹⁹¹ Parliamentary debates on the law skirted data protection concerns, focusing instead on financial implications. This legislative calm was in stark contrast to societal uproar as citizens worried about their privacy and the potential risks tied to the expanding role of computers in public administration. Concerns were compounded by the inclusion of code numbers on

¹⁸⁸ Angel and Calo (n 180); Solove, 'Against Privacy Essentialism' (n 185).

¹⁸⁹ BVerfG, *Order of the First Senate of 15 December 1983 [1983] 1 BvR 209/83 (German Federal Constitutional Court)*. See Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 *Computer Law & Security Review* 84. For a description of the case in English.

¹⁹⁰ Florent Thouvenin, 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?' (2021) 12 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 246.

¹⁹¹ Hornung and Schnabel (n 189) 85.

forms intended for lengthy retention, and the vast network of 600 000 census takers tasked with data collection under local authority oversight. Controversy was also ingrained in the broader unease about escalating surveillance and the pervasive digitisation of public administration.¹⁹²

The Census Act faced legal scrutiny at the *Bundesverfassungsgericht*, where the Court decreed that the census, in its intended format, infringed upon the right to ‘informational self-determination’. This right was extracted from the German constitutional concept of *Persönlichkeitsrecht* or ‘right to personality,’ anchored on the right to safeguard human dignity,¹⁹³ as well as the right to personal liberty.¹⁹⁴ The aim of the right to personality is to secure the ability of each individual to freely shape their own personality.¹⁹⁵

The right to informational self-determination is defined as ‘the power of the individual to decide, based on the principle of self-determination, when and to what extent information about his private life should be disclosed to others.’¹⁹⁶ Thus, the court maintained that personal data processing should be rooted in an individual’s consent.

The concept of informational self-determination is deeply embedded in the discussions prevalent in German legal literature at the time, suggesting that the court's deliberations were influenced by this academic discourse. Scholars

¹⁹² *ibid.*

¹⁹³ German Constitution Article 1(1).

¹⁹⁴ *ibid.* Article 2(1).

¹⁹⁵ Hornung and Schnabel (n 189) 86.

¹⁹⁶ *Census Decision C.II* quoted in René Mahieu, ‘The Right of Access to Personal Data: A Genealogy’ (2021) 2021 *Technology and Regulation* 62, 68.

including Podlech¹⁹⁷ and Pohle¹⁹⁸ note that the court particularly drew from sociological systems theory and the works of Niklas Luhmann.¹⁹⁹ This theory emphasises the role of functional differentiation in society and the importance of distinct societal subsystems, each governed by its own set of norms and interactions. According to Luhmann, the coherence of an individual's personality relies on navigating these subsystems through varied roles, underscoring the societal dependency on individuals' capacity to maintain a consistent self-identity.

Luhmann's analysis extends to the function of fundamental rights, including dignity and freedom, in facilitating individuals' ability to present themselves as unique personalities within society's complex structure. This perspective on fundamental rights posits that they serve to maintain the distinct functions of society's various subsystems. Privacy, particularly, is pivotal for safeguarding an individual's unique identity, which depends on the clear demarcation between these subsystems. Privacy and informational self-determination act as gatekeepers, ensuring that sensitive information from one realm does not seep into another. This containment is crucial for individuals to shape their identities freely and autonomously, which, in turn, underpins a free and democratic order. Informational self-determination, derived from these theoretical underpinnings, is thus seen as crucial for enabling individuals to be aware of and control the information others have about them, which is fundamental for personal freedom and dignity.²⁰⁰

¹⁹⁷ Adalbert Podlech, 'Die Begrenzung Staatlicher Informationsverarbeitung Durch Die Verfassung Angesichts Der Möglichkeit Unbegrenzter Informationsverarbeitung Mittels Der Technik: Zur Entscheidung Des Bundesverfassungsgerichts Über Das Volkszählungsgesetz 1983' (1984) 12 *Leviathan* 85. Quoted in Mahieu (n 175) 68.

¹⁹⁸ Jörg Pohle, 'Datenschutz und Technikgestaltung' 144 <<https://edoc.hu-berlin.de/handle/18452/19886>> accessed 3 February 2024. Quoted in Mahieu (n 196) 68.

¹⁹⁹ Mahieu (n 196) 68; Hornung and Schnabel (n 189) 85.

²⁰⁰ Hornung and Schnabel (n 189) 85–86.

Informational self-determination draws parallels to the Control Account of Privacy. However, Schwartz argues that informational self-determination transcends the mere control over personal data, advocating instead for a framework that limits, clarifies, and aligns data processing with the necessities of a free and democratic society. It is a right that facilitates individuals' ability to develop their personalities freely, by ensuring that data flows remain transparent and restricted to what is essential for societal progress.²⁰¹ In this way, informational self-determination is also reminiscent of Warren and Brandeis' appeal to 'inviolate personality' and the Personhood Account.

If individuals lack control over who accesses their personal information within their social sphere, it can stifle their exercise of freedom. The spectre of constant surveillance may deter them from engaging in any non-conforming actions to avoid drawing scrutiny. In a state with omniscient tendencies, true freedom of expression and choice are essentially nullified. Thus, informational self-determination serves a dual purpose. In the first instance, (I) it provides a sanctuary for personal autonomy. Simultaneously, (II) it is necessary to allow the free and active involvement of citizens in a constitutional democracy.²⁰² This dual rendering is reminiscent of the Civic Republican model of Rousseau's *The Social Contract*, where it is maintained that it is only through entering society that one can gain the 'moral freedom, which alone renders man truly master of himself.'²⁰³

²⁰¹ Paul Schwartz, 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination' (1989) 37 *The American Journal of Comparative Law* 675, 90.

²⁰² Hornung and Schnabel (n 189) 86. A necessary corollary is that encroachments upon the right to informational self-determination are only justifiable when public interest demonstrably supersedes the individuals.

²⁰³ Jean-Jacques Rousseau, *The Social Contract* (Wordsworth Classics 1762) 28. See also Nicholas Dent, *Rousseau* (Routledge 2008) 129; Olga Stuchebrukhov, "'Ridiculous" Dream versus Social

Ultimately, informational self-determination may be seen as a conception which unites the Control and Personhood accounts in services of individual, societal, and democratic interests.

5. The ‘Essence’ of Data Protection

Porcedda²⁰⁴ and González Fuster²⁰⁵ work to distil the essence of the right to data protection under Article 8 of the Charter. To grasp the significance of defining a right’s essence, one can look to Article 52(1) of the Charter. This clause acts as an ‘overarching provision’ governing permissible restriction to all qualified rights inscribed in the Charter, such as the right to personal data protection.

Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms.

According to the *Explanations* which accompany the Charter, limitations on rights and freedoms should be read with a restricted viewpoint and cannot result in ‘disproportionate and unreasonable interference that undermines the fundamental substance of those rights.’²⁰⁶ As such, despite some latitude, the preservation of the essence of the right is deemed non-negotiable. Essentially, an infringement of this core aspect of the right would be unacceptable, contravening the rule of law which underpins both the Charter and EU public policy.²⁰⁷

Contract: Dostoevskij, Rousseau, and the Problem of Ideal Society’ (2007) 59 *Studies in East European Thought* 101, 106.

²⁰⁴ Porcedda, ‘On Boundaries. Finding the Essence of the Right to the Protection of Personal Data.’ (n 45). And Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 111–128.

²⁰⁵ González Fuster (n 46).

²⁰⁶ *Case C- 292/97 Karlsson and Others*, [2000] EU:C:2000:202.

²⁰⁷ Porcedda, ‘On Boundaries. Finding the Essence of the Right to the Protection of Personal Data.’ (n 45) 3.

Brkan argues that the threshold for 'interference with the fundamental right' is one which in fact 'calls into question the existence of the fundamental right' itself.²⁰⁸ Brkan similarly differentiates between essence interferences and 'serious' or 'particularly serious' limitations of rights. Indeed, it is possible for rights to undergo significant limitations while still being considered as upholding their 'essence'. Conversely, limitations that preserve the 'essence of a right' may be characterised as 'less intense' compared to situations where the essence is breached.²⁰⁹

Moreover, understanding the essence of these rights is not a matter for the Courts alone. Reference to the essence requirement in the Standard Contractual Clauses issued by the European Commission in June 2021,²¹⁰ indicates that not only legislators and judiciary bodies, but also data controllers and processors, are expected to recognise and address any breaches of the essence of EU fundamental rights.²¹¹

²⁰⁸ Maja Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core' (2018) 14 European Constitutional Law Review 332, 363. Quoted in

²⁰⁹ González Fuster (n 46) 14–15. See also Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779, 784.

²¹⁰ Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council [2021] OJ L 199/31. See in particular Par. 19 and Clause 14(a). The latter of which requires the parties to warrant that the 'laws and practices' of a country outside of the EEA where personal data is transferred 'respect the **essence** of the fundamental rights and freedoms'. (emphasis added)

²¹¹ González Fuster (n 46) 5–6. See also Laura Drechsler and Irene Kamara, 'Essential Equivalence as a Benchmark for International Data Transfers After Schrems II', in Eleni Kosta, Ronald Leenes, and Irene Kamara (eds.), *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022) 17–18.

It is noteworthy that to date, the CJEU has never made a ruling that a limitation on the right to data protection is unlawful because of a failure to respect the essence of the right.²¹² Moreover, the jurisprudence itself does not provide for an easy identification of the essence of the right to privacy itself. Moore notes the lack of ‘a common thread...that would identify the essence of the rights to private life and data protection.’²¹³ The closest instance is to be found in the *Schrems* Judgments²¹⁴ where it is in fact the undermining of the essence of the Article 47 right to effective judicial protection which is used as the basis for invalidation. In *Schrems II*, the CJEU found that the United States did not provide adequate judicial protection for European residents whose personal data was transferred into its jurisdiction.²¹⁵ This finding may be seen as linked to the wording of Article 8(3) of the Charter which states that the right itself ‘shall be subject to control by an independent authority.’ However, this is not the language chosen by the Court, which instead chose to frame its ruling on Article 47 alone.

Porcedda²¹⁶ explains that ‘[i]f the right to the protection of personal data were an absolute right, its entire definition would correspond to the essence.’ However, as Article 8 of the Charter frames the right to protection of data in ‘qualified’ terms it is necessary to understand the ‘boundaries’ of the right. Unpacking the provisions of the right to data protection in Article 8 of the Charter reveals three distinct

²¹² See González Fuster (n 47) 31–32.

²¹³ Dominique Moore, ‘Article 23 – Restrictions’, in Christopher Kuner, Lee Bygrave, Christopher Docksey and Laura Drechsler (eds.), *The EU General Data Protection Regulation: A Commentary*. (Oxford University Press 2020) 554.

²¹⁴ *Case C-362/14 Schrems v Data Protection Commissioner (“Schrems I”)* [2015] EU:C:2015:650; *Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (“Schrems II”)* [2020] EU:C:2020:559.

²¹⁵ *Schrems II* at 187.

²¹⁶ Porcedda, ‘On Boundaries. Finding the Essence of the Right to the Protection of Personal Data.’ (n 45) 7.

components. First (I), it sets out principles that must be adhered to during data processing. Secondly (II), the provision endows the data subject with specific rights, including the right to access personal data collected about them and the right to request corrections to that data. Finally (III), it mandates the establishment of an independent authority to ensure compliance with these data processing rules and principles.²¹⁷

This three-part structure is deeply ingrained within the history of data protection. Already in 1980 Hondius had noted that a 'tripartite structure' was to be found in the emerging field of EU Data Protection Law. Specifically, all data protection regulations then in place within Europe (a) imposed obligations on those using data, (b) conferred rights on individuals and (c) placed on government the duty to supervise compliance.²¹⁸

5.1 Article 8 (1) of the Charter

Everyone has the right to the protection of personal data concerning him or her.

Article 8(1) and Article 16(1) TFEU collectively establish that every individual has the right to personal data protection. This provision is universal, applying to anyone under EU law's jurisdiction, regardless of their nationality or residence.

From a human rights standpoint, 'protection' implies both a negative obligation to avoid infringing on the right and a positive duty to uphold it, as highlighted by Articles 16 TFEU and 39 TEU. These articles emphasise that the focus of protection

²¹⁷ González Fuster (n 46) 17.

²¹⁸ Frits W Hondius, 'Data Law in Europe' (1980) 16 Stanford Journal of International Law 87, 95. Quoted in González Fuster (n 46) 18.

is on individuals concerning the processing of their data, encompassing both vertical and horizontal duties.²¹⁹

Article 8's emphasis on 'protection' and the lack of clarification in its Explanation suggest that 'protection' refers to a system or architecture safeguarding personal data. The GDPR's Recital 11 outlines three key aspects of effective protection: rights of data subjects, obligations of processors, and powers for ensuring rule compliance and imposing sanctions. These aspects align with Articles 8(2) and 8(3) of the Charter.

5.2 Article 8(2) of the Charter

Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Article 8's second paragraph outlines the prerequisites for personal data processing and provides data subjects with a range of rights. It stipulates that personal data must be processed in a fair manner, for specific purposes, and be lawful either through consent or another basis. Additionally, Article 8(2) of the EU Charter delineates two fundamental rights crucial to data protection. Firstly, it confers on data subjects the right of access. This right allows individuals to verify if their personal data is being processed, to obtain a free copy of such data and to receive additional information about the processing. In his advisory opinion in *Rijkeboer*, Advocate General Ruiz-Jarabo Colomer frames the right to access as the

²¹⁹ Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 115.

‘true subjective dimension’ of Data Protection Law. As it is only through this right that individuals may ‘react in defence of their interests’.²²⁰

Secondly, Article 8(2) grants data subjects the right to prompt rectification of inaccurate personal data. This right is foundational for the principle of accuracy, which mandates that data should be precise and updated when necessary. Efforts must be made to promptly correct or delete inaccurate data in light of the processing purposes. The significance of rectification and maintaining accuracy is linked to the personal aspect of data protection, as it respects and reflects an individual's unique identity.²²¹

Overall, the second limb of Article 8(2) of the Charter is manifested in the control exerted by individuals over their personal data.²²² This control translates into at least six rights under the GDPR.²²³ These rights vary in intensity and function as complementary steps in a strategy for managing personal data and mitigating potential harms.

5.3 Article 8(3) of the Charter

Compliance with these rules shall be subject to control by an independent authority.

Here once more appeal is made to the notion of *control*, albeit of a different actor. Article 8, paragraph 3 of the EU Charter requires that compliance with data protection rules be overseen by an independent authority. This obligation

²²⁰ Case C-553/07 *College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer* [2008] EU:C:2008:773, *Opinion of AG Ruiz-Jarabo Colomer* at [29].

²²¹ Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 122.

²²² González Fuster (n 128) 205.

²²³ These rights are outlined in Chapter 3 of the GDPR encompassing Articles 12 to 23.

underscores the vital role of a supervisory authority in safeguarding individuals' rights in the context of personal data processing. This provision contributes additional depth to the concept of protection by implying both an obligation to shield and to enforce rights.²²⁴

The notion of 'control' is expected to ensure 'effective protection from violations of data subjects' fundamental rights'.²²⁵ This includes preventing tactics like 'forum shopping' that are designed to bypass these rights and ensuring the practical enforcement of provisions that uphold these rights. Control in this sense is intertwined with the notion of independence. This aspect of Article 8 suggests a need for human involvement in data processing decisions, potentially emerging as an implicit, yet essential component of the right to data protection.²²⁶ We must note a third appeal to the role of *control* in data protection law is present. We may ask who is to hold *control* over data processing operations. If neither data subjects themselves nor all controllers can yield command over data processing, is it still available to supervisory authorities?

The components amounting to the essence of the right to data protection, as identified by Porcedda²²⁷ through analysis of CJEU case law and secondary law, are represented in *Table 3* below.

Table 3. Essential Elements of the Right to Data Protection per Porcedda

²²⁴ Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014).

²²⁵ *Case C-645/19 Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit* [2021] EU:C:2021:483 at [68].

²²⁶ Bygrave (n 224).

²²⁷ Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 125–129.

Essential Component	Description	Essence (CJEU)
Protection	In the broad sense, the system or architecture of personal data protection comprising principles, rights and duties. In a more restrictive sense, the principles and related technical and organisational measures to protect individuals against harms that may derive from data processing operations. Examples are data minimization and integrity and confidentiality.	(a contrario) The provision of security safeguards in the legal basis.
Fairness, lawfulness and purpose limitation (legitimate processing)	The expectation for data subjects that the processing must be legitimate, which refers to three interrelated principles stemming from the rule of law: • Fairness (includes transparency); • Purpose limitation (could include storage limitation); • Lawful legal basis.	The provision of purpose limitation in the legal basis.
Data Subject Rights	Data subjects' control over their personal data, enabling them to intervene in the processing. It includes: (i) accessing the data and	

	obtaining a copy; and (ii) rectifying inaccurate data. It supports a range of options available to the data subject specified in the applicable law. Currently this includes objecting to processing, including profiling; restricting the processing of one's personal data; erasing data; and transferring one's data.	
Independent control (human oversight)	The availability of oversight concerning data processing and the respect of the principles relating to the processing of personal data. Expresses the rule of law principle of access to justice, entitling individuals to claim without hindrance the intervention of an authority for the protection of his or her right. It can implicitly command human involvement in the processing and that a human being must be involved in the process (also drawn from data subject rights).	

6. The Relationship Between Privacy and Data Protection

In reality, even the CJEU does not consistently emphasise the unique standing of the two rights. In assessing compliance with the essence requirement, it has at times differentiated the application of this requirement between the right to respect for private life and the right to the protection of personal data.²²⁸ On other occasions it has instead treated them interchangeably.²²⁹

Nevertheless, the relationship between the rights to data protection and privacy can be generally envisioned in three manners: (i) data protection and privacy function as complementary rights; (ii) data protection operates as a component within the right to privacy; and (iii) data protection stands as an autonomous right, serving various roles including, but not confined to, the safeguarding of privacy.²³⁰ These models are explored in the following subsections.

6.1 Model 1: Separate Rights Complementing Each Other

The first understanding suggests a complementary relationship between data protection and privacy, both acting as intermediary tools with the ultimate goal of ensuring respect for human dignity. This model is represented in *Figure 1* below.

²²⁸ For a separate treatment of Articles 7 and 8 of the Charter see *Joined Cases C-293/12 and C-594/12 Digital Rights Ireland* [2014] EU:C:2014:238 at [39-40]; *Opinion 1/15 of 26 July 2017 pursuant to Article 218(11) TFEU* [2017] EU:C:2017:592 at [151].

²²⁹ For a treatment of Articles 7 and 8 of the Charter together see *Case C-291/12 Schwarz v Stadt Bochum* [2013] EU:C:2013:6 at [39]; *Case C-817/19 Ligue des droits humains ASBL v Conseil des ministres* [2022] EU:C:2022:491 *Opinion of AG Pitruzzella*. (n 70) at [120]; and *Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson* [2016] EU:C:2016:970. (n 28) at [99-101].

²³⁰ Lynskey, *The Foundations of EU Data Protection Law* (n 7) 90.

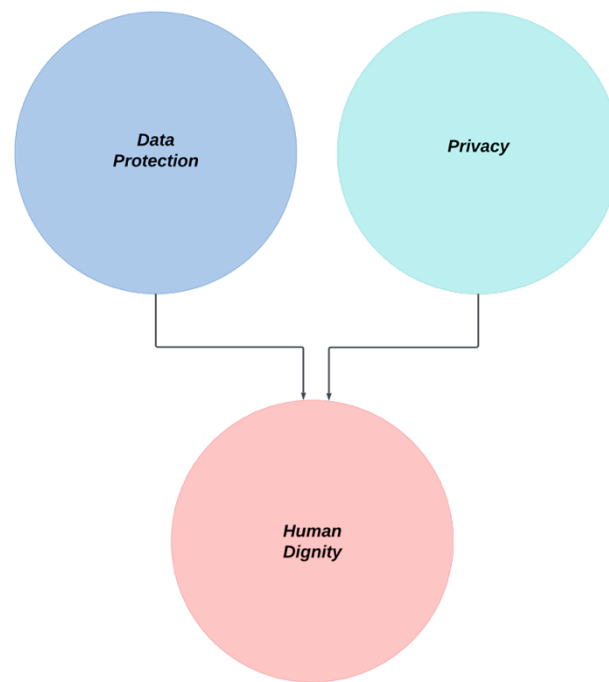


Figure 1. Relationship Between Privacy and Data Protection (Model 1)

Human dignity frequently serves as the underlying basis for various fundamental rights, shaping their scope and limitations. This principle potentially lays the foundation for data protection rights as well.²³¹ This view is supported by Porcedda who argues that both rights ‘exist morally as enablers of the development and preservation of one’s personality and identity in autonomy.’ As such they are to be understood as ‘facets of dignity highly prized in a democracy to which autonomous individuals contribute.’²³²

This connection was prominently highlighted in the 1983 *Census Decision*,²³³ of the German Federal Constitutional Court as discussed earlier in this chapter.²³⁴ This

²³¹ *ibid* 94.

²³² Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 13–14.

²³³ *BVerfG, Order of the First Senate of 15 December 1983 [1983] 1 BvR 209/83 (German Federal Constitutional Court)* (n 189). See Hornung and Schnabel (n 189). For a description of the case in English.

²³⁴ See [Chapter Two, Section 4.2 Data Protection and Informational Self-Determination](#).

perspective supports the theory that data protection rights have their origins, albeit indirectly, in the right to human dignity. Echoing this, Rouvroy and Pouillet reference this judgment to affirm that data protection and privacy collectively support individual self-development and the autonomous capacity for action and cooperation—elements intrinsically tied to human dignity.²³⁵ Bognetti further emphasises the necessity to regulate data collection activities by all entities, even when data subjects 'voluntarily agree to accept their degradation', reinforcing the imperative to uphold human dignity.²³⁶

There are several objections to the idea that data protection exclusively serves human dignity purposes within the EU framework. Firstly, there is a lack of consensus among EU member states about the specific nature of the right to human dignity. Despite its presence in various constitutional orders, there is no uniform constitutional tradition of human dignity to underpin data protection rights. In its ruling in *Evans v UK*, the ECtHR highlighted the diversity of national moral and cultural views. The court went on to emphasise the considerable discretion held by member states in how they protect human dignity, especially when balancing private and public interests.²³⁷

Secondly, the notion of human dignity is used to bolster various philosophical beliefs, which limits its utility in guiding or justifying data protection law. For instance, while EU data protection law might be seen as upholding human dignity

²³⁵ Antoinette Rouvroy and Yves Pouillet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 47.

²³⁶ Giovanni Bognetti, 'The Concept of Human Dignity in European and US Constitutionalism' in Georg Nolte (ed), *European and US Constitutionalism* (1st edn, Cambridge University Press 2005) 91. Quoted in Lynskey (n 1) 95.

²³⁷ *Evans v the United Kingdom Application no 6339/05* [2007] CE:ECHR:2007:0410JUD000633905 at [77]-[81].

by preventing complete alienation of individual rights, an opposing viewpoint may argue that human dignity necessitates allowing individuals to fully control their rights including the ability to relinquish them. This interpretation suggests that any prohibition in data protection laws could infringe on human dignity by transferring control over an individual's rights from the person to the legislature.²³⁸

A third argument concerns the structure of the Charter itself. Human dignity rights, including the right to life, integrity of the person, and prohibitions on torture and slavery, are in the 'Dignity' chapter, whereas data protection and privacy rights are placed under the chapter on 'Freedoms'.²³⁹ This categorisation indicates that the Charter's drafters did not view data protection as solely or primarily based on human dignity. Moreover, early drafts of the Charter, which proposed formulations of data protection rights similar to the German concept of informational self-determination, were eventually discarded.

6.2 Model 2: Data Protection as a Component of Privacy

A second reading of the relationship between the two rights is understanding the right to data protection as simply a component of the larger right to privacy. This model is reflected in *Figure 2* below. Here the sphere of data protection is entirely subsumed by the larger sphere of privacy.

²³⁸ Lynskey, *The Foundations of EU Data Protection Law* (n 7) 100.

²³⁹ *ibid.*

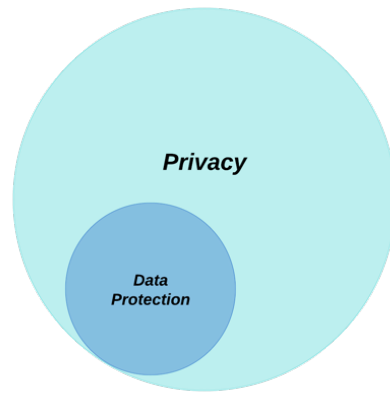


Figure 2. Relationship Between Privacy and Data Protection (Model 2)

Viewed through this lens, privacy was initially understood as ‘seclusion’ or the ‘right to be let alone’, it has since expanded to include aspects of controlling information. This evolution is seen as a response to the growth of digital records, giving rise to a multitude of new issues related to informational privacy. According to this model, the right to data protection does not fulfil any separate goals beyond those addressed by the right to privacy. In essence, every component of data protection law is underpinned by concerns related to privacy.²⁴⁰

A clear articulation of this argument is also made by Solove in the US context where he maintains that ‘the constitutional right to information privacy has emerged in the courts as a spin-off of the regular constitutional right to privacy’.²⁴¹ Supporting this view is the 2007 Advisory Opinion of Advocate General Kokott in *Promusicae*, who maintains that data protection legislation was ‘based on the fundamental right to private life.’²⁴²

²⁴⁰ *ibid* 102.

²⁴¹ Daniel J Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press 2004) 75. Quoted in Lyskey, *The Foundations of EU Data Protection Law* (n 7) 102.

²⁴² *Case C-275/06 Promusicae* [2007] EU:C:2007:454 *Opinion of AG Kokott* at [51]. Importantly this Advisory Opinion was delivered on 18 July 2007, prior to the signing of the Treaty of Lisbon on 13 December 2007. As such Advocate General Kokott’s framing could not yet rely upon the Charter, which had not yet been given legal application.

However, under this model we are forced to question why a separate right to data protection has been included in the Charter and TFEU. One possible explanation is proposed by de Hert and Gutwirth who posit that the introduction of the right to data protection within the Charter specifically aimed to enhance the legitimacy of the EU's data protection framework.²⁴³ Lynskey questions the validity of this explanation stating that 'the suggestion that a new right was recognised in the EU legal order to provide ex post legitimacy to existing legislation seems intuitively unsatisfactory.'²⁴⁴ Moreover, in 2016 the CJEU clearly asserted the independence of the right to data protection and the right to privacy, 'Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR.'²⁴⁵

6.3 Model 3: Data Protection as a Right which serves purposes beyond Privacy

Our third model is of data protection as a right which does overlap with privacy, but also serves further purposes. This is represented in *Figure 3* below:

²⁴³ Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009).

²⁴⁴ Lynskey, *The Foundations of EU Data Protection Law* (n 7) 91.

²⁴⁵ *Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post och telestyrelsen and Secretary of State for the Home Department v Tom Watson* [2016] EU:C:2016:970 at [129].

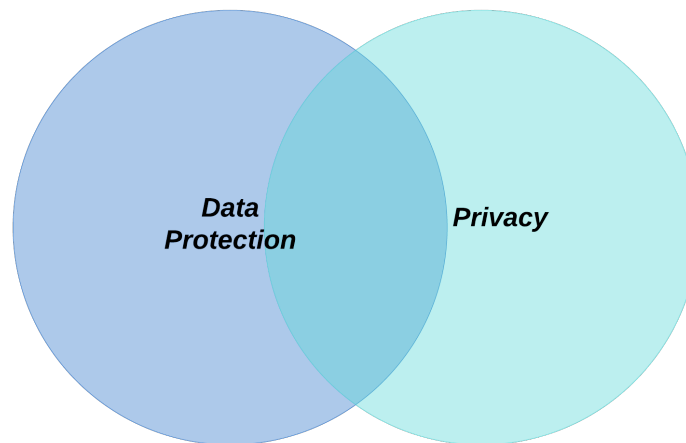


Figure 3. Relationship Between Privacy and Data Protection (Model 3)

In this framework, data protection and privacy share significant common ground, However, data protection fulfils various roles that go beyond the realm of privacy, and similarly, privacy has its own unique aspects not covered by data protection.²⁴⁶ This perspective sheds light on why privacy law does not cover all facets of data protection. The elements of data protection law that do not align with the right to privacy cater to other objectives unrelated to privacy. Furthermore, this model pays greater homage to the varying constitutional traditions of EU Member States. These traditions are referred to by the Court of Justice when delineating general principles of EU law.²⁴⁷

Supporting this view is the Advisory Opinion of Advocate General Cruz Villalón in *Digital Rights Ireland*. Here it is maintained that ‘Article 8 of the Charter enshrines the right to the protection of personal data as a right which is distinct from the right to privacy’, however even if ‘subject to an autonomous regime...data protection seeks to ensure respect for privacy.’²⁴⁸

²⁴⁶ Lynskey, *The Foundations of EU Data Protection Law* (n 7) 103.

²⁴⁷ *ibid* 104.

²⁴⁸ *Joined cases C-293/12 and C-594/12 Digital Rights Ireland* [2013] EU:C:2013:845, *Opinion of AG Cruz Villalón* at [55].

Ultimately, Lynskey notes the absence of an unambiguous explanation for the interaction between data protection and privacy, acknowledging the contribution each model brings to ongoing discussions on the topic.

7. Conclusion

7.1 Legal Response to Technological Innovation

In this chapter we have highlighted privacy and data protection as legal rights which have evolved in response to technological and societal change. By the close of the 19th Century the promise of isolation and confidentiality in one's home had been undermined by the stirrings of surveillance. With the advent of photographic tabloid journalism, the physical walls of the past had become transparent. In response Warren and Brandeis penned their famed article 'the Right to Privacy'.

In contrast, by the 1960s new concerns underpinned the formation of data protection law within Europe. The shadow of the totalitarian regimes of the Third Reich and the USSR combined with significant technological advances in automated data processing invoked a new fear of centralised state knowledge and control.

Yet a similar lacuna separates the emerging challenges of the 2020s from the context of Hesse in 1970 and even those leading to the adoption of the Data Protection Directive in 1995. The rise of multinational 'tech-giants', the emergence of an industry of extractive AdTech, and 'surveillance capitalism'²⁴⁹ have complicated the relationship between actors and potential harms to fear in

²⁴⁹ See Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

hitherto inconceivable ways. The primary concerns of today are no longer centred upon state control alone.

7.2 Key Elements of the Right Data Protection

Since the arrival of the Charter in 2000, the relationship between privacy and data protection has become more complex with both rights now given distinct standing. However, the content of the new right to data protection under Article 8 of the Charter is unclear as is its relationship with the right to privacy in Article 7.

In our analysis of the right to data protection under Article 8 of the Charter the following key elements have been identified:

1. Protection

- **Broad Reading:** the very architecture of personal data protection including a framework of principles, rights, and obligations.
- **Narrow Reading:** principles and associated technical and organisational strategies aimed at shielding individuals from potential damages arising from data processing activities. Key examples of such protective measures include the reduction of data collected to the minimum necessary and ensuring data integrity and confidentiality.

2. Legitimacy of Processing:

the anticipation that personal data will be handled in a legitimate manner. This expectation is rooted in three interconnected principles derived from the rule of law:

- A legal basis for processing of data.
- Transparency of and fairness in processing.

- Purposes specification for data use and the prohibition of further processing in a way that is incompatible with those original purposes.
3. **Data Subject Rights:** Individuals are given controlling rights to oversee their personal data and take action regarding its use. This encompasses: (i) the ability to access one's data and receive a copy thereof; and (ii) the power to correct any inaccuracies. These rights facilitate a suite of legal options for individuals.
 4. **Independent Control:** the provision of attentive oversight over data handling practices and adherence to personal data processing principles. This reflects the rule of law's tenet of unobstructed access to legal redress, empowering individuals to seek the engagement of a regulatory body to safeguard their rights. Implicitly, it demands the participation of judgement in data-related activities, ensuring that a human agent plays a role in the process, a notion also inferred from the rights granted to data subjects.

7.3 The Relationship Between the Two Rights

We have seen three possible models to define the relationship between the two rights. The initial interpretation posits that data protection and privacy operate in tandem ultimately converging in their shared objective to uphold the principle of human dignity. The second perspective views data protection as an integral element of the broader right to privacy. In this view, data protection falls completely within the scope of privacy, without distinct boundaries. The third understanding posits that while data protection and privacy considerably intersect, data protection extends into additional domains. This model acknowledges that data protection not only upholds privacy but also addresses concerns that privacy alone does not encompass, just as there are aspects of privacy that data protection does not specifically address.

Model 1 underscores the significance of human dignity in the realm of data protection rules, offering a potential insight into why the processing of personal data can be detrimental, regardless of its connection to material harm.

With Model 2, the capacity of privacy law to encompass data protection elements is demonstrated. Nonetheless, since not all data protection rules fall under its umbrella, it implies these rules either hold no weight or serve alternate functions, similar to those hinted at in Models 1 and 3. Model 3 proposes a separation between data protection and privacy, albeit with considerable overlap. This separation mirrors the diverse constitutional traditions among Member States and aligns with Data Protection Laws' objective to 'protect fundamental rights, in particular privacy.' However, it also emphasises the yet-to-be-defined independent roles of data protection, beyond the boundaries of privacy, reinforcing its multifaceted importance in safeguarding various rights and interests.²⁵⁰

7.4 Appeals to Control

It is clear that the right to privacy as defined by the Charter and given meaning through case law amounts to a conception that stretches beyond the confines of the perspective offered by Warren and Brandeis. Notwithstanding, it remains challenging to pinpoint a single, unifying foundational account of privacy that serves as the basis for this right. Its content at times seems to align with the control or access accounts while at others it would appear that the understanding of privacy as personhood or informational self-determination is more appropriate. As such we must accept our inability to identify an overriding conception of the

²⁵⁰ Lynskey, *The Foundations of EU Data Protection Law* (n 7) 104–105.

right to privacy under Article 7 of the Charter. Instead, we may embrace Solove's notion of a family resemblance approach which states that 'privacy is better understood as drawing from a common pool of similar characteristics.'²⁵¹

However, we find greater clarity in terms of Article 8 of the Charter. Here we find a strong appeal to informational self-determination and control as the central basis for EU Data Protection Law. The limits of this appeal to control and autonomy will be explored in the next chapter. Moreover, we shall demonstrate that individual control is entirely dependent upon the role of data controllers for actualisation. As such in the absence of precision in the accountability mechanisms of the GDPR, individual self-determination simply cannot be achieved.

What is more, Article 8(3) of the Charter outlines a further appeal to the ideal of control, stipulating that regulatory bodies should exercise *control* over data processing activities. This regulatory oversight is intended to provide 'effective protection from violations of data subjects' fundamental rights. Such protection encompasses preventing strategies like forum shopping' which aim to circumvent these rights, as well as ensuring the practical enforcement of provisions that uphold them. In this context, the notion of control is intrinsically linked to the principle of oversight and regulatory independence. This aspect of Article 8 implies a necessity for human involvement in data processing decisions, potentially emerging as an implicit yet crucial element of the right to data protection. Furthermore, it raises the question of who should ultimately hold control over data processing operations. If neither data subjects themselves nor all controllers can exert complete command over data processing, we might consider whether such control is achievable for supervisory authorities. Furthermore,

²⁵¹ Solove, 'Conceptualizing Privacy' (n 180).

without clear demarcation of the role of *controller*, the autonomy of individuals is stymied while the powers of regulators are likely to be misdirected.

Chapter Three: Data Protection's Nature and Ambitions

1. Introduction

The GDPR represents a significant evolution in the field of data protection, building upon decades of legal development while introducing novel concepts and strengthening existing protections. At its core, the Regulation embodies a balance between two seemingly divergent goals: the protection of fundamental rights and freedoms and the facilitation of economic growth and market integration within the EU. This duality reflects the complex role that personal data plays in modern society, serving both as a deeply personal asset requiring robust safeguards and as a valuable economic resource driving innovation and commerce.

As we examine the nature of the GDPR, we will explore the tension between these dual objectives and how they shape the Regulation's approach to data protection. Additionally, we will consider the historical context of EU data protection law, tracing the shift from a primarily market-oriented focus to an increasing emphasis on fundamental rights protection. This evolution mirrors broader societal changes and the growing recognition of data protection as a distinct fundamental right within the EU legal framework.

Central to our discussion will be an analysis of two contrasting paradigms in data protection: the Individual Control Model and the Societal Protection Model. These approaches represent different philosophical underpinnings for data protection, with significant implications for how regulations like the GDPR are structured and implemented. By examining the GDPR through these lenses, we aim to provide

insight into the regulation's underlying assumptions, strengths, and potential limitations.

Throughout this chapter, we will critically assess the GDPR's approach to balancing individual empowerment with broader societal protections. Ultimately, however, both ambitions will be shown to rely upon effective and clear accountability mechanisms and as such are impacted by *the Problem of Control*.

2. Context of the GDPR: The Need for New Legislation

By 2003 with the publication of the first report of the European Commission on the 1995 Directive²⁵² it had become clear that the goals of harmonisation and consistency were not being met. The national laws passed to give meaning to the Directive in member states had already diverged to the point where its aims had been undermined. Notably, the report found that such discrepancies occurred with even the most specific sections of the Directive.²⁵³

Moreover, certain divergences undermined the goals of facilitating the free flow of personal data in a regulated environment. An example is requirements for businesses to notify Data Protection Authorities of processing activities. As these differed from member state to member state, a greater bureaucratic and financial burden was placed on businesses seeking to operate in multiple EU jurisdictions.²⁵⁴

²⁵² 'First Report on the Implementation of the Data Protection Directive (95/46/EC)', <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=EN>> accessed 27 September 2023.

²⁵³ *ibid.*

²⁵⁴ *Ibid.*

Thus in 2010 the Commission introduced a strategy to reform the European Data Protection Regime.²⁵⁵ Two years later, the European Commission published its proposal for a comprehensive reworking of the Data Protection Directive, which ultimately led to the passing of the GDPR.

The Recitals which accompany the GDPR describe the issues which led to the need for a new legal instrument. It is explained that the principles and aims of the Directive 'remain sound' but these have been undermined through a fragmented system of implementation. This in turn had undermined the goal of allowing for the free and safe flow of personal data across the EU with economic consequences.²⁵⁶ The introduction of a new data protection law at an EU level was thus seen as necessary. The GDPR was published in the Official Journal of the European Union in May 2016, becoming fully enforceable on 25 May 2018.

3. The Ambitions of the EU Data Protection Regime

A recurring motif in EU Data Protection Law is a dichotomy of articulated goals. In the first instance policy makers aim to protect fundamental rights and freedoms. At the same time a strong focus is placed upon economic and market supporting goals.²⁵⁷

This tension is already clear from the 1980 OECD Guidelines²⁵⁸ which delineate several intertwined objectives: (i) the establishment of acceptance for certain

²⁵⁵ European Commission, 'A Comprehensive Approach on Personal Data Protection in the European Union', Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions'.

²⁵⁶ The GDPR, Recital 9.

²⁵⁷ See Lynskey, *The Foundations of EU Data Protection Law* (n 7) 46–88. Lynskey devotes a chapter to the interplay between the goals of rights protection and economic stimulation.

²⁵⁸ See [Chapter Two, Section 3. The Emergence of Data Protection.](#)

minimal standards for the protection of personal data privacy; (ii) minimisation of variances between pertinent domestic rules and practices across OECD members; (iii) the prevention of undue interruption to the movement of personal data amongst OECD member countries; and (iv) the elimination of objections to transborder data flows. The intention behind these Guidelines was to ensure that the evolution of national data protection laws would not pose a hindrance to cross-border data flows, thereby ensuring smooth international trade. Despite this, the non-binding nature of these Guidelines posed a challenge, as their efficacy was constrained, allowing discrepancies to continue in national laws.²⁵⁹

EU Data Protection Law has consistently followed these dual goals. One objective is economic, aiming to enhance the establishment of the internal market, while the other is rights-based, focusing on safeguarding fundamental rights during personal data processing. *Table 4* outlines this recurring tension in digitally focused EU law.

Table 4. Dualism of Goals in Digitally Focussed EU Legislation

Legal Instrument	Rights Preserving Goals	Market Supporting Goals
1995 Data Protection Directive	Article 1(1): Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.	Article 1(2): Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the

²⁵⁹ Lynskey, *The Foundations of EU Data Protection Law* (n 7) 47–48.

		protection afforded under paragraph 1.
GDPR	Article 1(2): This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.	Article 1(3): The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.
AI Act	Article 1 (1): The purpose of this Regulation is...ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union	Article 1 (1): The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI)...and supporting innovation.
Digital Services Act	Article 1 (1): The aim of this Regulation is to contribute to the proper functioning of the internal market for	Article 1 (1). The aim of this Regulation is to <u>contribute to the proper functioning of the internal</u>

	intermediary services by setting out harmonised <u>rules for a safe, predictable and trusted online environment</u> that facilitates innovation and <u>in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected.</u> ²⁶⁰	<u>market for intermediary services</u> by setting out harmonised rules for a safe, predictable and trusted online environment that <u>facilitates innovation</u> and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected. ²⁶¹

Regarding its rights protecting emphasis, it is undoubtedly true that GDPR is primarily concerned with the right to protection of one's personal data. Yet the intention of the GDPR goes further as is outlined in Article 1(2) wherein the right to data protection is highlighted, but included among a broader aim of respecting fundamental rights and freedoms:

This Regulation protects **fundamental rights and freedoms of natural persons** and in particular their right to the protection of personal data.²⁶²

This emphasis is reiterated in Recital 2(1):

²⁶⁰ Emphasis added to highlight rights-based aspects of text.

²⁶¹ Emphasis added to highlight market and innovation aspects of text.

²⁶² Emphasis added.

The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, **respect their fundamental rights and freedoms**, in particular their right to the protection of personal data.²⁶³

This is further emphasised in Recital 4:

This Regulation respects all **fundamental rights and observes the freedoms and principles** recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.²⁶⁴

EU data protection legislation unifies national laws, ensuring a consistent level of rights protection across all Member States, thereby eliminating objections to cross-border data flows on the basis of human rights. Nevertheless, clear strain exists between the GDPR's economic and rights-based focuses.

In his Advisory Opinion in *Google v CNIL*, Advocate General Szpunar noted that the GDPR goes beyond the internal-market approach of the 1995 Data Protection Directive, aiming to establish a comprehensive system of personal data protection across the EU.²⁶⁵ This view was supported by the CJEU's ruling in the case, where it recognised GDPR's goal of ensuring a high level of personal data protection EU-wide.²⁶⁶

²⁶³ Emphasis added.

²⁶⁴ Emphasis added.

²⁶⁵ *Case C-507/17 Google LLC v CNIL* [2019] EU:C:2019:15, *Opinion of AG Szpunar* at [77].

²⁶⁶ *Case C-507/17 Google LLC v CNIL* [2019] EU:C:2019:772 at [76].

Prior to the GDPR, this tension was intensified given the EU's inability to pass fundamental rights legislation when the Directive was enacted. A circumstance that only changed with the enactment of the Lisbon Treaty in December 2009. Lynskey makes the compelling argument that as a result of the EU's inability to enforce fundamental rights legislation, the CJEU initially prioritised data protection's market integration goal, while cautiously approaching its fundamental rights aspect. However, recent developments showcase a shift towards a balanced view.²⁶⁷ This transition underscores a significant divergence between past and present data protection. While Data Protection Law continues to fulfil its market function, its fundamental rights objective now receives greater attention.

4. Data Protection: Individual Control v Societal Protection

From the emergence of Data Protection Law two distinct impulses have developed. The first is a desire to protect society through regulatory control. This corresponds to Article 8(3) of the CFREU which states that '[c]ompliance with these [data protection] rules shall be subject to *control* by an independent authority. The second is the development of a regime of data subject rights to ensure individual *control*. Two such rights, access and rectification, are included in Article 8(2) of the CFREU. We may label these two contrasting paradigms as the 'Individual Control Model' and the 'Societal Protection Model'.²⁶⁸

²⁶⁷ Lynskey, *The Foundations of EU Data Protection Law* (n 7) 47.

²⁶⁸ In this regard we largely follow the naming conventions of Solove and Hartzog. Daniel J Solove and Woodrow Hartzog, 'Kafka in the Age of AI and the Futility of Privacy as Control' (2024) 104 Boston University Law Review 1024.

3.1 The Individual Control Model

The idea of control as the underpinning rationale has already been referenced in this thesis. In Chapter Two we outlined the conception of privacy defined by the control held by individuals over their information,²⁶⁹ as well as the notion of informational self-determination.²⁷⁰ Both of these understandings seek to empower individuals by granting them authority over their personal information. From this viewpoint, an individual's privacy rights hinge on their control or lack thereof over these private matters. Thus, the loss of control over personal information equates to a decrease in privacy and data protection.²⁷¹ The Individual Control Model is the operationalising mechanism behind these two understandings.

The appeal to individual control is one which may be seen as emerging from the zeitgeist of the early 2000s and 2010s. Allusion has been given to the Control Account of Privacy by industry leaders and ultimately policy makers. An example of the former category – in January 2002, Bill Gates sent an email to every full-time employee at Microsoft, laying out the company's new strategy and emphasising security in its products.²⁷² Under the heading 'Privacy', Gates wrote:

Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It

²⁶⁹ See [Chapter Two, Section 4.1 Privacy's Conceptual Disarray](#).

²⁷⁰ See [Chapter Two, Section 4.2 Data Protection and Informational Self-Determination](#).

²⁷¹ Macnish (n 157) 419; Lundgren (n 171).

²⁷² The full email was reproduced by *Wired* on 17 January 2002. Bill Gates, 'Bill Gates: Trustworthy Computing' [2002] *Wired* <<https://www.wired.com/2002/01/bill-gates-trustworthy-computing/>> accessed 7 July 2023.

should be easy for users to specify appropriate use of their information including controlling the use of email they send.²⁷³

Similarly, in a 2018 interview with WIRED's Nicholas Thompson, Twitter founder Jack Dorsey explained:

I do believe that individuals should own their data and should have the right to have the controls over how a company might utilise that and how a service might utilise that and be able to pull it immediately.²⁷⁴

While, in his 2018 written testimony to the US House of Representatives, Facebook founder Mark Zuckerberg attested on behalf of his organisation:

We believe strongly in providing meaningful privacy protections to people. This is why we work hard to communicate with people about privacy and build controls that make it easier for people to control their information on Facebook.²⁷⁵

Hartzog notes that the word 'control' is used over one thousand times in this testimony.²⁷⁶

This appeal to control is realised by bestowing individuals with a range of privacy rights designed to facilitate their control over personal data.²⁷⁷ Another key feature of this model is the reliance on consent requirements. In the United States, the predominant approach has been one of 'notice-and-choice', whereby organisations provide privacy notices detailing their data practices, and

²⁷³ Emphasis added.

²⁷⁴ Nicholas Thompson, 'Jack Dorsey on Twitter's Role in Free Speech and Filter Bubbles' *Wired* <<https://www.wired.com/story/jack-dorsey-twitters-role-free-speech-filter-bubbles/>> accessed 7 July 2023 (emphasis added).

²⁷⁵ Emphasis added.

²⁷⁶ Hartzog, 'The Case Against Idealising Control' (n 179) 424.

²⁷⁷ Daniel J Solove, 'The Limitations of Privacy Rights' (2023) 98 *Notre Dame Law Review* 975, 977.

individuals are given the option to opt-out if they object. This approach has been widely derided by commentators, who argue that it is ineffective due to the fact that most people do not read privacy notices and remain oblivious to how their data is being used. Richards and Hartzog maintain that ““notice” often means little more than burying data practices in the fine print of a dense privacy policy, while “choice” means choosing to use a service with its non-negotiable data practices as a take-it-or-leave-it option.”²⁷⁸

In the EU’s Data Protection Regime, consent must be explicit and affirmative (opt-in), reflecting a higher standard than the notice-and-choice approach. While express consent is generally considered superior, it still places a heavy burden on individuals to make informed decisions about the collection and use of their data. Regardless of the stringency of consent requirements, whether opt-in or opt-out, the concept of consent remains fundamentally tied to the notion of individual control.²⁷⁹

3.2 The Societal Protection Model

The Societal Protection Model²⁸⁰ posits that privacy and data protection are not solely, or even primarily, individual concerns. Instead, it argues that they should be safeguarded to promote broader societal values such as democracy, freedom,

²⁷⁸ Neil M Richards and Woodrow Hartzog, ‘Privacy’s Constitutional Moment’ (2020) 61 Boston College Law Review 1687.

²⁷⁹ Solove and Hartzog (n 268) 1026.

²⁸⁰ Approaches following this model are also referred to as structural or paternalistic models. See Felix Bieker, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law* (Asser Press 2022); Katherine Nolan, ‘The Individual in EU Data Protection Law (PhD Thesis; LSE Law School)’ (PhD Thesis, LSE Law School 2023) ch Five <<https://etheses.lse.ac.uk/4596/>>.

creativity, health, as well as intellectual and emotional flourishing.²⁸¹ Scholars including Paul Schwartz,²⁸² Oscar Gandy,²⁸³ Julie Cohen,²⁸⁴ Joel Reidenberg,²⁸⁵ Spiros Simitis,²⁸⁶ and Priscilla Regan²⁸⁷ have consistently emphasised the importance of viewing privacy as a societal value rather than merely an individual interest. This perspective conceptualises privacy and data protection rights primarily in terms of power dynamics and the role of human information in its creation, deployment, and distribution. It asserts that privacy protection necessitates an architecture that structures power and a regulatory framework governing information dissemination, collection, and networking.²⁸⁸

De Hert and Papakonstantinou argue for a focus beyond individual rights models, characterising such perspectives as inadequate for addressing the collective issues posed by big data and its associated analytics.²⁸⁹ Hirsch articulates the impetus for societal protection rather than individual control in the context of increased algorithmic surveillance:

²⁸¹ This is a key theme of the ideal of Informational Self-Determination discussed in [Chapter Two, Section 3.2 Data Protection's Conceptual Underpinnings](#).

²⁸² Paul M Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review 1607, 1647–1658.

²⁸³ Oscar H Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Oxford University Press 2021).

²⁸⁴ Julie E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373.

²⁸⁵ Joel R Reidenberg, 'Privacy Wrongs in Search of Remedies' 54 Hastings Law Journal 877.

²⁸⁶ Spiros Simitis, 'Reviewing Privacy In an Information Society' (1987) 135 University of Pennsylvania Law Review 707.

²⁸⁷ Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (The University of North Carolina Press 2000).

²⁸⁸ Solove, *The Digital Person* (n 241) 101.

²⁸⁹ Paul De Hert and Vagelis Papakonstantinou, 'Framing Big Data in the Council of Europe and the EU Data Protection Law Systems: Adding "Should" to "Must" via Soft Law to Address More than Only Individual Harms' (2021) 40 Computer Law & Security Review 105496.

In order to protect people in the algorithmic economy, privacy law must shift from a liberalist legal paradigm that focuses on individual control, to one in which public authorities set substantive standards that defend people against algorithmic threats.²⁹⁰

This sentiment is echoed by Smuha, who raises concerns about the capacity of legal systems primarily focused on individual control to effectively address societal harms associated with artificial intelligence.²⁹¹

In the specific context of genetic data, Costello²⁹² as well as Kuru and Beriain²⁹³ have independently scrutinised the appropriateness of individualised approaches. Their work highlights the unique challenges posed by genetic information, which inherently involves data pertaining to multiple individuals, thus complicating traditional notions of individual data ownership and control.

3.3 Defining the GDPR

Article 8(3) of the Charter clearly links the right to data protection to the societal protection model by insisting that '[compliance] with these rules shall be subject to *control* by an independent authority.' Furthermore there is a key linguistic connection to this model, as Nolan notes, the very term 'data protection' serves as a concise representation of 'the protection of natural persons with regard to the processing of personal data.'²⁹⁴ Unsurprisingly then, the GDPR does incorporate

²⁹⁰ Dennis Hirsch, 'From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics' (2020) 79 Maryland Law Review 439.

²⁹¹ Natalie A Smuha, 'Beyond the Individual: Governing AI's Societal Harm' 10 Internet Policy Review.

²⁹² Róisín Á Costello, 'Genetic Data and The Right to Privacy: Towards a Relational Theory of Privacy?' (2022) 22 Human Rights Law Review 1.

²⁹³ Taner Kuru and Iñigo De Miguel Beriain, 'Your Genetic Data Is My Genetic Data: Unveiling Another Enforcement Issue of the GDPR' (2022) 47 Computer Law & Security Review 105752.

²⁹⁴ Nolan (n 280) 122.

elements of societal protection, such as requirements for justifying data processing, minimising data collection and use, conducting Data Protection Impact Assessments, and implementing data protection by design and default. However, these structural elements are often perceived as insufficient, with a disproportionate reliance on individual control mechanisms. Many of these structural measures lack robustness, potentially falling short in terms of accountability and thoroughness.²⁹⁵ Similarly, Waldman argues that compliance measures can devolve into superficial, performative exercises that fail to achieve meaningful protection. The structural elements of the GDPR often lack the same rigour and enforceability as its individual control provisions. For instance, requirements for privacy impact assessments and data protection by design and default are criticised for their lack of specificity and accountability, potentially allowing organisations to fulfil these obligations in a perfunctory manner.²⁹⁶

In reality, the GDPR still predominantly relies on individual control. This conclusion is directly supported by Recital 7 of the GDPR which explicitly states that ‘natural persons should have control of their own personal data’. While Recital 68 states that the right to data portability expressed under Article 20 explicitly aims to ‘further strengthen the control’ one has ‘over his or her own data’. Moreover, early drafts of the Charter proposed formulations of data protection rights similar to the German concept of informational self-determination.²⁹⁷

²⁹⁵ Margot E Kaminski, ‘Binary Governance: Lessons from the GDPR’s Approach to Algorithmic Accountability’ (2019) 92 Southern California Law Review 1529.

²⁹⁶ Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge University press 2021) 9–10.

²⁹⁷ Lynskey, *The Foundations of EU Data Protection Law* (n 7) 100.

The GDPR emphasises individual control by permitting a wide range of data processing through consent and placing significant emphasis on individual rights in both organisational compliance efforts and external enforcement. In Nolan's articulation '[a]s the protected subject of this regime—the "data subject"—the individual is central to the logic and functioning of this legislative scheme.'²⁹⁸

Purtova underscores that while there is broad agreement on the significance of individual control as 'a matter of wide consensus', data protection laws seldom encapsulate this concept in a single, distinct provision, or name it as 'the principle of control'.²⁹⁹ Despite debate regarding the universal acknowledgment of the importance of individual control it is undeniable that no unified principle of control is present within EU data protection legislation. Instead, the EU legal framework on data protection outlines various distinct rights, providing individuals the opportunity to exercise control over their personal data, rather than consolidating all aspects under a single 'principle of control'.³⁰⁰

Van Ooijen and Vrabec³⁰¹ present a breakdown of the manner in which the GDPR seeks to realise the ambition presented in Recital 7. In order to do so the authors divide the processing of personal data into three distinct states: (1) information reception; (2) approval and primary use; and (3) data secondary use (reuse). These are presented in *Figure 4 below*:

²⁹⁸ Nolan (n 280) 35.

²⁹⁹ Nadezhda Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table ... and Back on Again?' (2014) 30 Computer Law & Security Review 6, 12.

³⁰⁰ Lynskey, *The Foundations of EU Data Protection Law* (n 7) 180.

³⁰¹

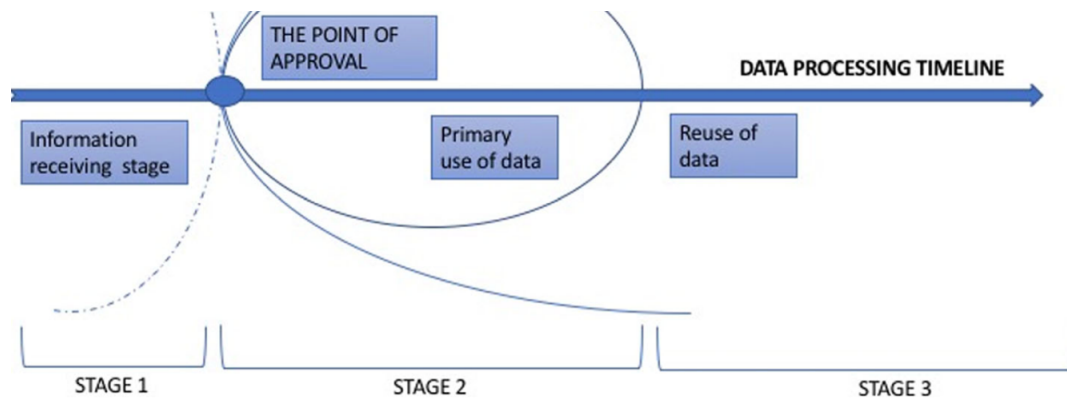


Figure 4. *Stages of Data Processing Timeline per Van Ooijen and Vrabec*³⁰²

At the first stage of information reception are provisions aimed at enhancing an individual's control through the right to information provision. Prior to any data processing activity, a data subject must be made aware of several matters including, the intentions for data processing, the identity of the controller, the recipients of their personal data, and the data storage period.³⁰³ Additionally, the GDPR mandates that a controller should also disclose the occurrence of 'automated decision-making, including profiling', and provide significant information about the logic involved, as well as the importance and anticipated consequences of such cases. At the initial stage, the key to enhanced control lies in comprehending the information provided. Only when an individual is cognisant of the data processing and corresponding decision-making actions, and can grasp the potential outcomes, does she hold control over the processing of her personal data.³⁰⁴

³⁰² I Van Ooijen and Helena U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 *Journal of Consumer Policy* 91, 93.

³⁰³ GDPR, Articles 13 and 14.

³⁰⁴ Van Ooijen and Vrabec (n 302) 96–97.

In the second and third stages of this processing cycle, the GDPR strengthens individual control of personal data through a combination of elements including a higher threshold for consent,³⁰⁵ higher transparency standards,³⁰⁶ and a host of detailed rights to be applied within the context of personal data processing.³⁰⁷ It is noteworthy that Lynskey refers to these as ‘control rights’.³⁰⁸ These rights include that of data portability,³⁰⁹ restriction of processing,³¹⁰ and the much-discussed right of erasure,³¹¹ known as the ‘right to be forgotten’. At the same time, the existing rights established under the 1995 Data Protection Directive remain including the right to access one’s personal data,³¹² the right of rectification for incorrect personal data,³¹³ and the right to object to data processing.³¹⁴

Within the GDPR, the concept of protection has become intricately linked with the notion of control, reflecting the central role that control over data and autonomy play in data protection and information privacy theory. However, the GDPR’s approach extends beyond individual control or choice in many circumstances.³¹⁵ Instead, it incorporates a range of regulatory approaches to legitimise data

³⁰⁵ GDPR, Article 7.

³⁰⁶ *ibid.* Recital 37, 58 Articles 5(1), 13-14.

³⁰⁷ *ibid.* Articles 15-22.

³⁰⁸ Orla Lynskey, ‘Deconstructing Data Protection: The “Added-Value” of a Right To Data Protection in the EU Legal Order’ (2014) 63 *International and Comparative Law Quarterly* 569. And Lynskey, *The Foundations of EU Data Protection Law* (n 7).

³⁰⁹ GDPR, Article 20.

³¹⁰ *ibid.* Article 18.

³¹¹ *ibid.* Article 17.

³¹² GDPR, Article 15

³¹³ *ibid.* Article 16

³¹⁴ *ibid.* Article 21

³¹⁵ Nolan (n 280) 122.

processing. This multifaceted approach results in a legal framework that balances the safeguarding of individual choice with the Societal Protection Model.

Ultimately however, both models rely upon a clear accountability system to ensure their realisation. Individuals seeking to exercise control over their personal data must do so by employing their rights against controllers. This crucial relationship between data subjects and controllers lies at the heart of the European Data Protection Regime, which seeks to empower individuals and ensure the responsible handling of their information. However, the effectiveness of this system is contingent upon a clear and unambiguous demarcation of the role of controller.

Similarly, independent Supervisory Authorities ('SAs')³¹⁶ tasked with overseeing the application and enforcement of data protection law, levy their powers against actors according to the level of responsibility placed upon them by the law, specifically controllers. These authorities play a vital role in ensuring compliance, investigating breaches, and imposing sanctions where necessary. Yet, their ability to carry out these functions effectively is predicated on a precise understanding of who qualifies as a controller in any given data processing scenario.

The lack of clarity in defining the role of controller has far-reaching consequences for both individual autonomy and the efficacy of regulatory oversight. When the boundaries of controllership are blurred, data subjects are left uncertain as to whom they should direct their requests and complaints, hindering their ability to exercise their rights and maintain control over their personal information. This

³¹⁶ See [Chapter Four, Section 7. Supervisory Authorities](#).

ambiguity creates a significant barrier to individual empowerment, undermining the very purpose of the data protection framework.

Moreover, without a clear demarcation of the role of controller, the powers of SAs risk being misdirected or ineffectively deployed. These authorities may find themselves pursuing the wrong actors or struggling to allocate responsibility in complex data processing chains. This not only wastes valuable resources but also erodes public trust in the regulatory system, as individuals perceive a lack of effective enforcement and accountability.

The importance of defining the role of controller extends beyond the operational aspects of Data Protection Law. It is a matter of fundamental rights and the balance of power in the digital age. By failing to provide a clear and consistent understanding of controllership, we risk creating a landscape in which individuals are disempowered, and regulators are hamstrung in their efforts to protect the privacy and autonomy of citizens.

5. Conclusion

The GDPR stands as the pivotal piece of legislation in the evolving landscape of EU Data Protection Law. At its core, the GDPR embodies a duality of purpose that has long characterised EU data protection efforts. On one hand, it aims to safeguard fundamental rights and freedoms, with a particular focus on privacy and data protection. On the other, it seeks to foster economic growth and market integration within the EU. This balance between rights protection and market facilitation is not merely a legislative quirk but a reflection of the multifaceted role that data plays in modern society – as both a personal asset to be protected and an economic resource to be leveraged.

Notably, the GDPR represents a shift in emphasis compared to earlier data protection initiatives. While previous efforts often prioritised market integration, recent developments, including the GDPR, have placed greater weight on fundamental rights protection. This evolution aligns with the recognition of data protection as a distinct fundamental right within the EU Charter of Fundamental Rights, signalling a growing awareness of the critical importance of data privacy in an increasingly digital world.

In this chapter we have identified two contrasting paradigms which have emerged in the field of data protection: the Individual Control Model and the Societal Protection Model. The Individual Control Model emphasises empowering individuals to make informed decisions about their personal data, reflecting concepts like informational self-determination. In contrast, the Societal Protection Model views privacy and data protection as collective issues that require broader structural safeguards to address power imbalances and systemic risks in data processing.

While the GDPR incorporates elements of both models, it leans heavily towards the Individual Control Model. This preference is evident in several aspects of the regulation, from the explicit statement in Recital 7 that ‘natural persons should have control of their own personal data’ to the emphasis on consent mechanisms and individual rights throughout the text. The structure of data processing stages and corresponding control mechanisms identified by Van Ooijen and Vrabec further illustrates this individual-centric approach.

However, we have also highlighted growing criticism of an over-reliance on individual control mechanisms, particularly in the face of complex technological challenges like big data and artificial intelligence. Critics argue that individual-centric approaches may be inadequate to address collective harms and the

profound power imbalances that characterise the modern digital economy. These concerns raise important questions about the long-term effectiveness of the GDPR's approach in an era of rapid technological change. Where the GDPR does include societal protection measures, such as data minimisation principles and impact assessments, these are often perceived as less robust or enforceable compared to the regulation's individual rights provisions. This disparity suggests that finding the right balance between individual empowerment and societal safeguards remains an ongoing challenge in Data Protection Law.

Furthermore, the effectiveness of both individual control and societal protection ultimately depends on clear accountability structures. This underscores the critical importance of precisely defining key roles within the data protection framework, particularly that of the 'controller' in data processing scenarios. Ambiguity in these definitions will undermine the practical implementation of data protection principles and hinder the ability of individuals to exercise their rights effectively.

Chapter Four: Key Elements of the Data Protection Regime

1. Introduction

The European Data Protection Regime of the 2020s differs from its precedents both in terms of its breadth and depth. In terms of breadth, the EU's Data Protection Regime is only a part of its larger regulatory framework for online services, markets, and data sharing. What is more, the definitions, roles, and responsibilities first brought into EU Law through the 1995 Directive have been expanded dramatically through case law. As such the expansive Data Protection Regime of the 2020s is a product of both legislative action and judicial interpretation as will be explored in the next chapter.

In terms of depth, the provisions of the GDPR and complementary legislation go far beyond the requirements of the 1995 Data Protection Directive. As the GDPR forms the basis of contemporary Data Protection Law and this thesis, this chapter will be devoted to its provisions. At the outset we will examine key definitions, as well as the GDPR's material and territorial scope. As the central concern of this thesis is the controller-based accountability model of Data Protection Law, this is reviewed in depth. In order to understand the implications of the roles of controllers, processors, and joint-controllers, attention is also given to GDPR's most significant obligations. The GDPR may be described as both a principle and risk based legal instrument – both aspects will be explored in this chapter.

2. Key Definitions

2.1 Personal Data and the Data Subject

The application of the GDPR hinges on the classification of data as 'personal'. This necessitates a precise definition of personal data to delineate the boundaries of legal applicability.³¹⁷ The definition of 'personal data' is given in Article 4(1) of the GDPR '

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

From here the definition of 'data subject' is drawn to be the identified or identifiable natural person to whom personal data pertains.

2.1.1 Key Elements

The definition of personal data supplied is comprehensive and malleable with the goal of providing technologically neutral protection as envisioned by Recital 15 of the GDPR.³¹⁸ It is composed of four elements that collectively define its scope and application.³¹⁹ Firstly, (I) the term 'any information' underscores the expansive nature of personal data, encompassing a wide array of information types, from

³¹⁷ Lynskey, 'Complete and Effective Data Protection' (n 32) 302.

³¹⁸ Purtova (n 31) 44; Paul M Schwartz and Daniel J Solove, 'Reconciling Personal Information in the United States and European Union' (2014) 102 California Law Review 877.

³¹⁹ Lee A Bygrave and Luca Tosoni, 'Article 4(1): Personal Data' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020) 109.

textual data to photographs, and sound recordings. This broad interpretation reflects the legislature's intent to provide comprehensive protection to individuals' data, irrespective of its form or sensitivity.³²⁰

Secondly, (II) the notion of 'relating to' establishes the link between the information and the data subject. Information is deemed to 'relate' to an individual when it is inherently connected to that person, either through its content, purpose, or effect. This connection can be direct, as in the case of information specifically about an individual, or indirect, such as when data pertains to an object closely associated with a person. Moreover, information used to evaluate, influence, or impact an individual's rights and interests also falls within the compass of 'relating to' an individual.³²¹ Much like the notion of identifiability, the interpretation of 'relating to' a natural person is subject to both broad and narrow constructions, inviting a nuanced assessment of the nature and extent of the relationship between the information and the individual, as well as the presence of this relationship under particular circumstances. The absence of clear guidance regarding the interpretation of 'relating to' further compounds the challenges faced by those seeking to navigate this complex legal landscape.³²²

Thirdly, (III) the requirement of an 'identified or identifiable' person is central to the applicability of EU Data Protection Law. An individual is considered 'identifiable' when they can be singled out whether directly or indirectly. Recital 26 of the GDPR provides guidance on the threshold for the possibility of identification. The mere hypothetical possibility of identification is not sufficient

³²⁰ *Case C-434/16 Nowak v Data Protection Commission* [2017] EU:C:2017:994 at [34].

³²¹ van Alsenoy (n 127) 25–26; Purtova (n 31) 42–43.

³²² See Purtova (n 70); and Orla Lynskey, 'Complete and Effective Data Protection' (2023) 76 *Current Legal Problems* 297.

to meet the standard of ‘identifiable’ and thus does not constitute personal data under the GDPR.³²³ Rather, the term ‘identifiable’ is limited to ‘all the means reasonably likely to be used.’ However, there is no requirement that all the information enabling the identification of the data subject be held by the same individual or entity.³²⁴

Finally, the scope of personal data, as defined by the GDPR, is confined to information pertaining to natural persons, thereby generally excluding data related to legal entities from its protective sphere.³²⁵ The GDPR's silence on the definition of a natural person is a deliberate choice, leaving the interpretation of this concept to the discretion of individual member states. This approach reflects the balance between the need for harmonised data protection standards across the EU and the recognition of the diverse legal and cultural landscapes that shape the understanding of personhood within each jurisdiction.³²⁶ However, the GDPR does provide some guidance on the time-based boundaries of its provisions. Recital 27 explicitly states that the regulation does not extend its safeguards to the personal data of deceased individuals. This exclusion reflects the common understanding that the right to data protection, as a fundamental human right, is inherently linked to the life of the natural person and ceases upon their demise.³²⁷

³²³ Mac Macmillan, ‘Data Protection Concepts’ in Eduardo Ustaran (ed), *European Data Protection* (3rd edn, IAPP Publications 2023).

³²⁴ *Case C-582/14 Breyer v Bundesrepublik Deutschland* [2016] EU:C:2016:779 at [43].

³²⁵ This exclusion is not absolute, as various legal instruments, including the ePrivacy Directive, national data protection laws, and constitutional provisions, may extend alternative safeguards to information concerning legal persons.

³²⁶ Bygrave and Tosoni (n 319) 111.

³²⁷ Michèle Finck and Frank Pallas, ‘They Who Must Not Be Identified — Distinguishing Personal from Non-Personal Data under the GDPR’ (2020) 10 *International Data Privacy Law* 11, 13.

2.1.2 Anonymous and Pseudonymous Data

The dichotomy between anonymous and personal data is a fundamental distinction in the realm of Data Protection Law. Anonymous data pertains to information that bears no connection to an identified or identifiable individual. It encompasses data that has been ‘rendered anonymous in such a manner that the data subject is not or no longer identifiable.’³²⁸ Anonymous data, stripped of personal identifiers, does not fall within the purview of the GDPR. In contrast pseudonymous data, though disguised, retains its link to an identifiable person and, consequently, remains subject to the provisions of Data Protection Law. True anonymity requires rendering data subjects unidentifiable, permanently severing all connections to individuals. Only then does information leave the purview of Data Protection Law.³²⁹

Already prior to the advent of the GDPR, the CJEU had ruled that dynamic IP devices can constitute personal data in *Breyer*.³³⁰ While in its 2017 decision in *Nowak*,³³¹ the Court maintained that exam scripts corresponding to an individual also constitute identifiable personal data.

However, the broad and flexible definition of data is not without its challenges. The interpretive leeway granted can lead to inconsistency in the application of Data Protection Law. The determination of what constitutes a reasonable possibility of identification or a sufficient nexus between information and an

³²⁸ Purtova (n 31) 44–45.

³²⁹ Recital 26, GDPR; ‘pseudonymisation’ means ‘the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person’ (Article 4(5) GDPR).

³³⁰ Case C-582/14 *Breyer v. Bundesrepublik Deutschland* [2016] EU:C:2016:779 (n 324).

³³¹ Case C-434/16 *Nowak v Data Protection Commission* [2017] EU:C:2017:994 (n 320).

individual is often subjective and context-dependent as shall be explored further in Chapter Five.³³²

2.2 Special Category Data

Beyond the class of personal data, a secondary classification of ‘special category data’ is laid out in Article 9 of the GDPR. These are personal data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership. Additionally special category data include genetic or biometric data; data concerning health; and data concerning a natural person’s sex life or sexual orientation. Special category data carries a higher duty of care and the lawful bases which can be relied upon to process it are more restrictive.³³³

2.3 Processing

As with the definition of personal data, the category of ‘processing’ is intentionally far-reaching. The GDPR, defines ‘processing’ as ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.’³³⁴ A long, but not exhaustive list of activities which meet this definition is provided. Processing includes the recording of personal data, its consultation, use, transmission, publication, and even its destruction. This list of operations underscores the legislature's intent to create a technologically neutral

³³² See [Chapter Five, Section 3.1 The Expanded Scope of Personal Data](#).

³³³ Ludmila Georgieva and Christopher Kuner, ‘Article 9: Processing of Special Categories of Personal Data’ in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020) 365–384.

³³⁴ GDPR, Article 4(2).

framework that can withstand the test of time and prevent attempts at circumvention.³³⁵

3. Actors and Accountability

The system of accountability under the GDPR follows a tradition formalised in the 1980s and 1990s.³³⁶ The primary actor in data processing is the controller. The definition of a controller is given in Article 4(7) of the GDPR:

‘[C]ontroller’ means the natural or legal person, public authority, agency or other body which, *alone or jointly with others*, determines the purposes and means of the processing of personal data.³³⁷

In every circumstance of data processing there is at least one data subject and one controller.³³⁸ Those who make the decision to process data must ascertain whether it contains personal information and, if that is the case, determine what their obligations are under GDPR.

The GDPR stipulates that data should be gathered for defined, clear, and legitimate objectives, and should not be processed further in a manner that is incompatible with these goals. Therefore, defining the ‘objectives’ of the processing and the ‘methods’ to accomplish them is of significant importance.³³⁹ The controller is the actor who decides why and how data processing will take

³³⁵ Luca Tosoni and Lee A Bygrave, ‘Article 4(2): Processing’ in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020) 117.

³³⁶ See [Chapter Six, Section 2. Controller Based Accountability: Historical Origins](#).

³³⁷ Emphasis added.

³³⁸ Michèle Finck, ‘Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law’ (2021) 11 *International Data Privacy Law* 333.

³³⁹ European Data Protection Board, ‘Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021’ (2021).

place. Any natural or legal entity that exerts such control over the processing of personal data participates in deciding the objectives and methods of that processing.³⁴⁰ However, it is noteworthy that an entity will be categorised as a controller even if it does not intentionally target personal information or has inaccurately concluded that it is not dealing with personal data.³⁴¹

The role of controller may be held by either a natural person or a legal entity. The EDPB³⁴² explains that even where a specific individual within an organisation is given responsibility for data compliance, they will not be considered to be a controller. Instead, they act on behalf of the legal entity which is itself the controller and holder of obligations under data protection law.³⁴³ The same is true of a division within a legal entity, such as the marketing team of a company. The legal entity itself (the company) and not the division (the marketing team) will still be the controller for this act of data processing.³⁴⁴

Controllers may appoint a processor to carry out the data processing operation. The definition of processor is given in Article 4(8) of the GDPR:

‘[P]rocessor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

A processor may commission further sub-processors if the terms governing the controller-processor agreement so allow. These sub-processors are bound by

³⁴⁰ Case C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* (‘Jehovan todistajat’) [2018] EU:C:2018:551 (n 21). At par. 68

³⁴¹ European Data Protection Board, ‘Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021’ (n 339) 15.

³⁴² See [Chapter Four, Section 8, The EDPB and Cross Border Cooperation](#) for an overview of this body.

³⁴³ *ibid.* 10.

³⁴⁴ *ibid.*

scope and terms of the original agreement. This relationship is represented in *Figure 5* below.

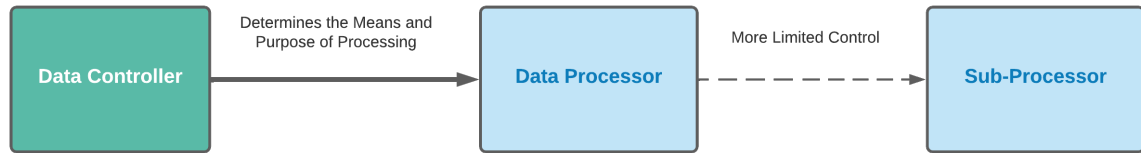


Figure 5. Controller, Processor, and Sub-Processor Relationship

A central question pertains to determining the boundary between decisions that should be made by the controller and those that can be left to the processor's discretion. Decisions regarding the purpose of the processing are invariably under the jurisdiction of the controller. When it comes to defining the means of processing, a clear distinction can be drawn between means that are essential and non-essential. 'Essential means' are intimately tied to the purpose and extent of the processing and are inherently the responsibility of the controller. Such essential means include the type of personal data to be processed, the processing duration, the categories of recipients, and the categories of data subjects. On the other hand, 'non-essential means' refer to the more practical aspects of implementation, such as the selection of a specific type of hardware or software or detailed security measures, which can be left to the processor to decide.³⁴⁵

All roles under Data Protection Law are determined through factual control in determining 'the purposes and means of the processing of personal data.' The EDPB³⁴⁶ explains that the categories of controller and processor are 'functional

³⁴⁵ European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339) 14.

³⁴⁶ See [Chapter Four, Section 8, The EDPB and Cross Border Cooperation](#) for an overview of this body.

concepts' in that 'they aim to allocate responsibilities according to the actual roles of the parties.' Consequently, the formal designation of controller or processor roles is immaterial if the true relationship is different. These actual roles stem 'from the concrete activities' of each party in clear contexts and are 'not negotiable.'³⁴⁷

Finally, it is also possible for more than one party to share the role of controller, thus forming a joint controller relationship. A joint controller relationship is defined in Article 26 of the GDPR 'Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.' This relationship in its simplest form is represented in *Figure 6* below.

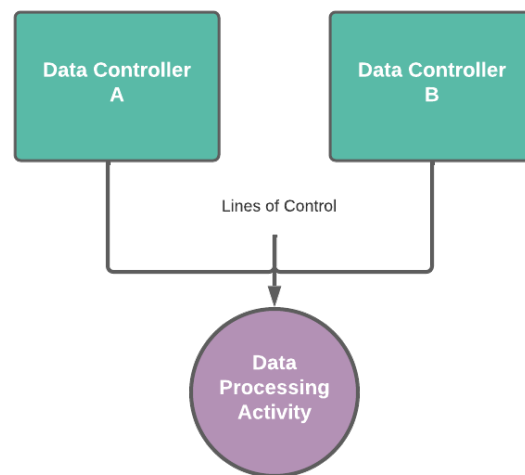


Figure 6. Joint Controller Relationship

Joint controllers are required to determine their 'respective responsibilities for compliance' with the GDPR.³⁴⁸ This arrangement must be transparent and its essence must be made available to data subjects.³⁴⁹ Importantly, data subjects may

³⁴⁷ *ibid.* 9 [12]

³⁴⁸ GDPR, Article 26(1).

³⁴⁹ *ibid.* Article 26(2).

exercise their rights 'in respect of and against each of the [joint] controllers' regardless of the way the joint controllers have decided to divide responsibility.³⁵⁰

Generally, joint controllership pertains to a specific data processing activity where multiple parties collaboratively decide on its purpose and means. The term itself implies that the decision-making is shared or not solely attributed to one entity. The evaluation of joint controllership is grounded on a factual analysis, considering the actual influence over the purpose and means of processing, rather than a formal enquiry. This requires a careful review of all current or planned agreements and comparing them with the actual circumstances of the data processing involved. A mere formal designation is insufficient for at least two reasons. First, (I) parties might lack a formal agreement on joint controllership by law or contract. In other cases, (II) the formal assignment might not mirror the reality of the arrangements, potentially delegating the role of controller to an entity that lacks the ability to determine the processing's purposes and means.

The distinction between data processing roles is not firm. The straightforward differentiation between processors and controllers has been criticised for being overly simplistic and described as a 'broken binary'.³⁵¹ In reality, it is possible to hold multiple roles as controller, processor, or joint controller for various acts of data processing even within a defined contractual relationship between two entities. In all cases the true test for determining the nature of the role is a factual question of control in deciding the means and purposes of processing. The complexity of these relationships and the continued validity of these roles is the central concern of this work

³⁵⁰ *ibid.* Article 26(3).

³⁵¹ van Alsenoy (n 127) 7. See also Patrick Van Eecke and Maarten Truyens, 'Privacy and Social Networks' (2010) 26 *Computer, Law & Security Review* 535.

4. Scope of Application

In order to comprehend the duties incumbent upon controllers, joint-controllers, and processors, the scope of application of the GDPR must be understood. In this section we review the GDPR's material and territorial scope.

4.1 Material Scope

The material scope of the GDPR is given in Article 2(1):

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

The GDPR applies to both automated data processing as well as the manual processing of data as long as the data 'form part of a filing system or are intended to form part of a filing system.' The definition of a 'filing system' has been clarified at the CJEU in the case of *Jehovan todistajat*. The Court found that it is not necessary for the 'filing system' to 'include data sheets, specific lists or other search methods.' Instead the key determining factor is that personal data is kept in a manner which enables it to be retrieved for subsequent use.³⁵²

However, a number of exceptions to this material scope are listed in Article 2(2): including processing which falls outside the scope of Union law, processing carried out in the context of law enforcement, and processing carried out for a purely personal or household use. Most important for this thesis is the household exemption. Under Article 2(2)(c) data which is processed in the context of 'purely'

³⁵² Case C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyyskunta* ('*Jehovan todistajat*') [2018] EU:C:2018:551 (n 21). at [62].

personal or household activities is exempt from the GDPR. As such personal messages, letters and address books are not subject to the obligations of Data Protection Law. This does not extend to actors which provide the means for this processing, such as the manufacturer of a cell phone.³⁵³ The household exemption is discussed in greater detail in Chapter Eight.³⁵⁴

4.2 Territorial Scope

The GDPR applies both to actors ‘established’ in the EU as well as to data processing operations when the data subject is based within the EU.³⁵⁵

4.2.1 EU Established Controllers and Processors

In the first instance a question over the definition of ‘establishment’ arises. Recital 22 gives the term a broad meaning:

[E]stablishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

Furthermore, the concept of establishment has been tested in the CJEU case of *Weltimmo*.³⁵⁶ This case dealt with the question of activities which met the definition of establishment. Weltimmo, a company incorporated in Slovakia, advertised properties in Hungary. In response to complaints laid with the Hungarian Data

³⁵³ Herke Kranenborg, ‘Article 2: Material Scope’ in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020).

³⁵⁴ See [Chapter Eight, Section 6. The Smart Home and the Household Exemption](#).

³⁵⁵ GDPR, Article 3.

³⁵⁶ *Case C-230/14 Weltimmo s.r.o v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] EU:C:2015:639.

Protection Authority, Weltimmo maintained that Hungarian authority was not applicable and that only the Slovakian DPA held jurisdiction.

In its ruling, the CJEU held that a broad interpretation was to be given to the concept of establishment. Contrary to the argument made by Weltimmo, the Court instead ruled that the threshold for establishment could be met where an entity exercises 'through stable arrangements in the territory of that member state...a real and effective activity even a minimal one.'³⁵⁷ As such the presence of even a single representative may be enough to meet the threshold for establishment. In this case Weltimmo could be said to be established in Hungary, even though it was incorporated in Slovakia.

In its *Guidelines 3/2018*, the EDPB³⁵⁸ also makes it clear that the appointment of a processor based in the EU is not in itself sufficient to make GDPR applicable to the controller who has appointed them.³⁵⁹ Beyond simply being established within the EU, the second element of Article 3(1) of GDPR requires that the processing of personal data take place 'In the context of the activities of an establishment of a controller or a processor in the Union.' The EDPB explains that the processing activity concerned must be 'inextricably linked' to the EU Establishment.³⁶⁰

³⁵⁷ *ibid.* at [41].

³⁵⁸ See [Chapter Four, Section 8, The EDPB and Cross Border Cooperation](#) for an overview of this body.

³⁵⁹ European Data Protection Board, 'Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)' (2018) 11. The example is given of a Mexican company which offers products only in Mexico but decides to appoint a processor based in the EU. As neither the controller (the Mexican company) nor the data subjects (Mexican clients) are based in the EU, the GDPR is not applicable to the controller in this case. However, it is still applicable to the EU based processor who must comply with processor obligations.

³⁶⁰ *ibid* 10.

This issue was clarified by the CJEU in *Google Spain*.³⁶¹ A significant preliminary concern in the case was whether the activities of Google Spain in selling advertising within Spain were significantly linked to the search functionality of Google Incorporated. Importantly, Google Spain did not itself provide the search functionality in question, which was carried out by Google Inc. outside of the EU. However, the CJEU found sufficient connection between the activities of Google Spain and the search functionality in question to connect the two. As such the search functionality of Google Inc. was deemed to be within the jurisdiction relevant for the decision to be made.³⁶²

It is important to note that nationality and residence of the data subjects in question are not determinative. Instead, the GDPR will still apply to the processing of data of non-EU residents whenever the controller is based within the EU.

4.3 Application of the GDPR to Non-EU based Controllers and Processors

Article 3(2) of GDPR further extends the applicability of GDPR to non-EU based controllers and processors when are involved in:

- (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

³⁶¹ *Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, González [2014] EU:C:2014:317* (n 33). This case established the ‘right to be forgotten’ under EU Law.

³⁶² *ibid.* at [56].

Recital 23 of GDPR provides some clarity in understanding whether goods or services are in fact being ‘offered’ to data subjects within the EU:

In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union.³⁶³

Boardman and Fenelon³⁶⁴ explain that it thus follows that the inadvertent selling of a good or service to an individual within the EU does not of necessity meet the threshold of ‘envisioning’ laid out by Recital 23. The EDPB lists factors which are to be considered relevant in deciding whether the threshold has been met.³⁶⁵ These include: naming the EU or member states in reference to the goods or services; the use of an EU language; referencing travel instructions from the EU; paying a search engine to facilitate access by individuals in the EU; and the use of EU specific domain names.

Beyond offering goods or services, the monitoring of EU based individuals will also trigger the application of GDPR for non-EU based controllers or processors. Recital 24 of the GDPR clarifies that monitoring includes ‘profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.’ Importantly, the EDPB has noted that it is not necessary for this monitoring to take

³⁶³ Emphasis added.

³⁶⁴ Ruth Boardman and James Fenelon, ‘Territorial and Material Scope of the General Data Protection Regulation’ in Eduardo Ustaran (ed), *European Data Protection* (2nd edn, IAPP Publications 2019).

³⁶⁵ European Data Protection Board, ‘Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)’ (n 359) 15–16.

place intentionally.³⁶⁶ It also provides list of example activities which are to be considered 'monitoring':

- Behavioural advertisement
- Geo-localisation activities, in particular for marketing purposes
- Online tracking through the use of cookies or other tracking techniques such as fingerprinting
- Personalised diet and health analytics services online
- CCTV
- Market surveys and other behavioural studies based on individual profiles
- Monitoring or regular reporting on an individual's health status.³⁶⁷

5. Data Protection Principles

In order to comprehend the duties incumbent upon controllers and joint-controllers we must detail the core principles of the GDPR. These are to be applied by data controllers in all processing of personal data. These principles are: (i) Lawfulness, Fairness, and Transparency; (ii) Purpose Limitation; (iii) Data Minimisation; (iv) Accuracy; (v) Storage Limitation; (vi) Integrity and Confidentiality; and (vii) Accountability.³⁶⁸ We will examine each in the following subsections.

³⁶⁶ *ibid* 18.

³⁶⁷ *ibid*.

³⁶⁸ GDPR, Article 5.

5.1 Principle 1: Lawfulness, Fairness, and Transparency

Lawfulness

All processing of personal data requires a lawful basis which is identified and laid out clearly. The lawful bases for processing are (i) consent, (ii) performance of a contract, (iii) compliance with a legal obligation, (iv) protection of the vital interests of a natural person, (v) public interest, and (vi) protecting the legitimate interests of a controller or third party.³⁶⁹

In the case of 'special category' data more a restricted basis for data processing is required. Article 9 provides the lawful bases for processing special category data. These are:

- Explicit consent
- Employment, social security, and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies using member's data for political, philosophical and religious purposes.
- Data made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research, and statistics (with a basis in law).

Fairness

In addition to having a lawful basis for processing personal data, the processing in question must be carried out in a manner which is deemed to be 'fair'. Fairness

³⁶⁹ *ibid.* Article 6.

may be seen as an overarching value of Data Protection Law.³⁷⁰ The EDPB explains that the core of the requirement for fairness mandates that ‘personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject.’³⁷¹ The EDPB goes on to list a number of sub-principles which stem from fairness including respect for autonomy, truthfulness, non-discrimination, ethical use of data processing, and strengthening consumer choice. Fairness also necessitates an assessment of the negative impact of the data processing on the individual and others. Disproportionately negative impacts will not be justified and thus the processing involved will not be lawful under the GDPR.³⁷²

Transparency

The Principle of Transparency places an obligation on controllers to communicate information about data processing to data subjects. It may be seen as the logical extension to the obligation to process personal data ‘lawfully’ and ‘fairly.’³⁷³ Article 12(1) mandates that information must be communicated ‘in a concise, transparent, intelligible and easily accessible form, using clear and plain language.’³⁷⁴ Moreover, information must be provided both before the processing

³⁷⁰ European Data Protection Board, ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’ (2020) 17. See also Lee A Bygrave, ‘Core Principles of Data Protection’ (2001) 7 Privacy Law and Policy Reporter 169, 58.

³⁷¹ European Data Protection Board, ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’ (n 370) 17–18.

³⁷² *ibid.* 18.

³⁷³ Brendan Van Alsenoy, ‘Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation’ (2016) 7 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 271, 34.

³⁷⁴ The information to be shared with data subjects is clarified through Articles 12(1), 13, 14, 15, 19 and 22(3) of the GDPR.

takes place³⁷⁵ and after the operations have begun.³⁷⁶ These requirements are even more stringent for any information addressed specifically to a child.

The Transparency Principle additionally requires that data subjects are made aware of and empowered to use their rights under Articles 15 to 22.

5.2 Principle 2: Purpose Limitation

The GDPR requires that personal data must be used only for ‘specified, explicit and legitimate purposes’ and not be used in ‘a manner that is incompatible with those purposes.’³⁷⁷ Two requirements emanate from this principle. First, (I) controllers must clearly articulate the purposes for which personal data is being used at the moment of collection. Furthermore, (II) controllers must refrain from using this personal data in any way that is not compatible with the purpose defined at the moment of collection. Any subsequent use requires a separate lawful basis.³⁷⁸

5.3 Principle 3: Data Minimisation

The corresponding principle under the 1995 Directive required that data be ‘adequate, relevant and not excessive’ in relation to the purposes for which it was collected.³⁷⁹ The GDPR further restricts processing by requiring the data collected to be ‘limited to what is necessary’ to achieve the purposes of the processing. This

³⁷⁵ GDPR, Articles 13 and 14.

³⁷⁶ *ibid.* Article 15.

³⁷⁷ *ibid.* Article 5(1)(b).

³⁷⁸ Mariel Filippidis, ‘Data Processing Principles’ in Eduardo Ustaran (ed), *European Data Protection* (2nd edn, IAPP Publications 2019). see also Bygrave (n 370). and Van Alsenoy (n 373) 34.

³⁷⁹ Article 6(1)(c).

principle is thus closely linked to that of Purpose Limitation, without this specification an appropriate limit cannot be placed upon the data collection.

5.4 Principle 4: Accuracy

All controllers are obligated to ensure the accuracy of the personal data which they process. This translates to an *ex-ante* obligation to ensure that data is correct at the time of collection as well as an ongoing requirement to keep data up to date.³⁸⁰

Recital 39 of the GDPR explains that all reasonable steps be taken to delete or rectify inaccurate data promptly. This principle is also connected to the data subject's right to rectification of inaccurately recorded data under Article 16 of the GDPR.

5.5 Principle 5: Storage Limitation

Directly flowing from the Principle of Data Minimisation is that of Storage Limitation. Under this provision personal data may not be kept in a form which permits identification of data subjects for longer than necessary to realise the purposes for which the data were collected.³⁸¹

5.6 Principle 6: Integrity and Confidentiality

The GDPR states that personal data must be 'processed in a manner that ensures appropriate security of the personal data.'³⁸² The twin objectives of the Integrity and Confidentiality Principle are (a) to ensure that no unauthorised access to the

³⁸⁰ Filippidis (n 378).

³⁸¹ Cécile de Terwangne, 'Article 5: Principles Relating to Processing of Personal Data' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020) 318.

³⁸² The GDPR, Article 5(1)(f).

personal data takes place, and (b) to ensure that the data itself is protected from unauthorised alteration or destruction. The EDPB³⁸³ explains:

The security of personal data requires appropriate measures designed to prevent and manage data breach incidents; to guarantee the proper execution of data processing tasks, and compliance with the other principles; and to facilitate the effective exercise of individuals' rights.

As such controllers are required to implement appropriate 'technical and organisational measures' in proportion 'appropriate to the risk' involved.³⁸⁴

5.7 Principle 7: Accountability

Under the Accountability Principle a new obligation to 'demonstrate compliance' with all the principles outlined in Article 6 is placed upon the controller.³⁸⁵

This emphasis upon Accountability is further amplified by the requirements of Data Protection by Default and Design.³⁸⁶ This translates to privacy and data protection as *ex ante* considerations which must be incorporated into the creation and implementation of technologies and policies. Other obligations arising from the Principle of Accountability under the GDPR include:

- The obligation to bind processors to their legal obligations.³⁸⁷
- The obligation to keep records of all personal data processing activities.³⁸⁸

³⁸³ European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (n 370) 26.

³⁸⁴ GDPR, Article 32 (1)

³⁸⁵ de Terwangne (n 381) 318–319.

³⁸⁶ GDPR, Article 25.

³⁸⁷ *ibid.*, Article 28(3).

³⁸⁸ *ibid.*, Article 30.

- The responsibility to inform supervisory authorities and in some cases data subjects when a breach has taken place.³⁸⁹
- The responsibility to conduct Data Protection Impact Assessments ('DPIAs') for high-risk processing of personal data.³⁹⁰

6. Risk Assessment

In 2014, the Article 29 Working Party asserted that risk-based assessment has always been a component of EU Data Protection Law.³⁹¹ A key example is the CJEU's judgment in *Worten*,³⁹² where it highlighted the obligation for the controller to establish 'appropriate technical and organisational measures' as being based upon assessment of proportionality in combating risks.

The emphasis upon risk assessment and mitigation has been bolstered by the GDPR. Under its provisions data controllers must undertake risk assessments when ensuring the security of data processing,³⁹³ as well as when deciding whether data breaches must be reported to Supervisory Authorities and data subjects.³⁹⁴ However, the clearest example of risk considerations is within the requirement to conduct Data Protection Impact Assessments ('DPIAs').³⁹⁵

³⁸⁹ *ibid.*, Articles 33-34.

³⁹⁰ *ibid.*, Article 35.

³⁹¹ Article 29 Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks, Adopted on 30 May 2014 (WP218)' 2.

³⁹² *Case C-342/12 Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT)* [2013] EU:C:2013:355.

³⁹³ *ibid.* Article 32.

³⁹⁴ *ibid.* Article 33-34.

³⁹⁵ *ibid.* Article 35.

Article 35 of the GDPR mandates that a DPIA must be undertaken where processing is likely to result in a ‘high risk to the rights and freedoms’ of natural persons. Going further, Article 35 (3) outlines a non-exhaustive list of processing activities which require a DPIA.

A data protection impact assessment referred to in paragraph 1 shall *in particular* be required in the case of:

- (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
- (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- (c) a systematic monitoring of a publicly accessible area on a large scale.³⁹⁶

The non-exhaustive nature of this list has been reinforced by the Article 29 Working Party 29 (‘WP29’).³⁹⁷ As is explicitly made clear in its *Guidelines* ‘the words ‘in particular’ in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. There may be ‘high risk’ processing operations that are not captured by this list, but yet pose similarly high risks.’³⁹⁸

³⁹⁶ Emphasis added.

³⁹⁷ See [Chapter Four, Section 8, The EDPB and Cross Border Cooperation](#) for an overview of this body.

³⁹⁸ Article 29 Working Party (‘WP29’), ‘Guidelines on Data Protection Impact Assessment (DPIA) WP248. Endorsed by the European Data Protection Board on 25 May 2018’ (2018).

As such the EDPB³⁹⁹ outlines nine criteria which signal high risks and thus require a full assessment. These are derived from Article 35 of GDPR along with recitals 71, 75 and 91, and a review of the phrasing ‘likely to result in a high risk’ throughout the Regulation. The criteria are:

- Evaluation and scoring.
- Automated decision making.
- Systemic monitoring.
- Processing of sensitive data or data of a highly personal nature.
- Data processed at a large scale.
- Matching and combining datasets.
- Data concerning vulnerable data subjects.
- Innovative use of technology or applying new technological or organisational solutions
- When the processing in its own right prevents data subjects from exercising a right or using a service or a contract.⁴⁰⁰

The Supervisory Authorities⁴⁰¹ within EU member states have built upon this guidance requiring the completion of Article 35 impact assessments when processing meets certain requirements.⁴⁰²

From the onset, Article 35 of GDPR makes it clear that the concern to be resolved by a DPIA is not limited to privacy or data protection rights. Instead, Article 35 (1)

³⁹⁹ See [Chapter Four, Section 8, The EDPB and Cross Border Cooperation](#) for an overview of this body.

⁴⁰⁰ Article 29 Working Party (‘WP29’) (n 398) 9–10.

⁴⁰¹ See next section for an overview of Supervisory Authorities.

⁴⁰² See for instance CNIL, ‘Délibération N° 2018-326 Du 11 Octobre 2018 Portant Adoption de Lignes Directrices Sur Les Analyses d’impact Relatives à La Protection Des Données (AIPD) Prévu Par Le Règlement Général Sur La Protection Des Données (RGPD)’ (2018) 81 Légifrance - Publications officielles - Journal officiel.

lists the requirement for a DPIA to be triggered whenever there is a high risk to the 'rights and freedoms of natural persons.'

The specific requirements for a DPIA are laid out in Article 35(7), in which reference is made to an assessment of risks to 'the rights and freedoms' of data subjects. At a minimum the evaluation should include:

- A detailed account of the processing activities and their objectives, detailing the controller's legitimate interests if applicable.
- An examination of how necessary and proportionate the processing activities are in achieving these objectives.
- A review of the potential impacts on the rights and freedoms of the individuals whose data is being processed.
- Proposed strategies to mitigate identified risks, encompassing protective measures, security protocols, and mechanisms that uphold personal data protection, considering the rights and justified interests of the individuals whose data is processed and other affected parties.

This assessment thus entails the weighing of legal rights as well as broader interests. As such, a full DPIA must consider risks of a legal, social, and ethical nature. As the complex obligations of risk assessment are primarily incumbent upon controllers, properly assigning roles is vital for ensuring that risks are accounted for and redressed.

7. Regulators and Supervision

7.1 National Regulators

As had previously been established under the 1995 Directive,⁴⁰³ the GDPR requires all EU member states to have a Supervisory Authority ('SA') dedicated to monitoring data protection compliance. The independence of Supervisory Authorities from 'external influence, whether direct or indirect' is mandated in Article 52 of the GDPR. Any individual may file a complaint with a Supervisory Authority if they believe their rights and freedoms have been harmed by the processing of personal data. The powers given to these Supervisory Authorities are broad and include advisory, investigative, and corrective controls.

In order to carry out their monitoring function SAs are given a range of investigative powers under Article 58(1) of the GDPR including the power to compel controllers and processors to provide all information required for the SA to perform their tasks.⁴⁰⁴ As well as the power to carry out data protection audits of organisations and companies including access to premises.

In order to ensure to protect fundamental rights and freedoms, SA's Authorities are also given significant remedial powers. At the lowest levels a SA can issue warnings if it is of the view that an intended processing operation is 'likely' to violate the GDPR or a reprimand if it believes a violation is already in place.⁴⁰⁵ Supervisory Authorities are also given coercive powers to compel controllers and processors to:

⁴⁰³ Article 28

⁴⁰⁴ A complementary obligation under Article 30 (4) of the GDPR requires controllers and processors to provide their records of processing activities (ROPAs) to the Supervisory authority upon request.

⁴⁰⁵ GDPR, Article 58(2)(a) and 58(2)(b)

- Bring processing operations into compliance with GDPR.⁴⁰⁶
- Comply with Data Subject Requests.⁴⁰⁷
- Communicate personal data breaches to impacted data subjects.⁴⁰⁸
- Rectify or erase personal data or restrict its processing pursuant to Articles 16, 17 and 18.⁴⁰⁹

Under Article 58(2)(f) Supervisory Authorities can also order a restriction or ban on data processing or order the suspension of data flows to a recipient in a third country or to an international organisation.⁴¹⁰

Finally, Supervisory Authorities are given significant powers to impose administrative fines.⁴¹¹ The conditions for fines are outlined in Article 83. For lesser violations these are set at up to EUR 10 million, or, if superior, up to 2% of the total worldwide annual turnover for the preceding financial year. While the most significant violations carry a penalty of up to EUR 20 million or, if superior, up to 4 % of the undertaking's total worldwide annual turnover. The amounts imposed are determined taking into account the type of violation as well as other factors listed in Article 83(2) GDPR, including the gravity, and duration of the infringement.

High profile examples of SA administrative fines include the imposition of a EUR 1.2 Billion fine to Meta by the Irish Data Protection Commission ('DPC Ireland') on 22 May 2023 for failure to ensure the security of data transfers to the US despite

⁴⁰⁶ *ibid.* Article 58(2)(d)

⁴⁰⁷ *ibid.* Article 58(2)(c).

⁴⁰⁸ *ibid.* Article 58(2)(e).

⁴⁰⁹ *ibid.* Article 58(2)(g).

⁴¹⁰ *ibid.* Article 58(2)(j).

⁴¹¹ *ibid.* Article 58(2)(i).

two high profile CJEU rulings.⁴¹² As well as, the imposition of a EUR 225 million fine on WhatsApp by the DPC Ireland on 2 September 2021 for significant transparency violations.⁴¹³ The former is significant as the largest fine ever levied for a violation of the GDPR. While the latter is the first fine issued as a result of a binding decision of the European Data Protection Board under its article 65 mandate to resolve disputes between different Data Protection Authorities within EU member states.⁴¹⁴

7.2 The EDPB and Cross Border Cooperation

The 1995 Directive had created the Article 29 Working Party composed of the representatives of the national DPAs. With the onset of the GDPR the Article 29 Working Party has been replaced by the European Data Protection Board ('EDPB').⁴¹⁵ The EDPB continues to be composed of a representative from each DPA. However, under the 1995 Directive, the EDPB board has its own legal personality and its own secretariat. The mandate of the EDPB as laid out in Article 70 is to 'ensure consistent application' of the GDPR. This is to be achieved *inter alia* by:

⁴¹² Data Protection Commission (Ireland), 'Data Protection Commission Announces Conclusion of Inquiry into Meta Ireland' (*Data Protection Commission*, 2023) <<https://www.dataprotection.ie/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland>> accessed 2 August 2023.

⁴¹³ Data Protection Commission (Ireland), 'The Data Protection Commission (DPC) Has Today Announced a Conclusion to a GDPR Investigation It Conducted into WhatsApp Ireland Ltd.' (*Data Protection Commission*, 2 September 2021) <<https://www.dataprotection.ie/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry>> accessed 4 November 2022.

⁴¹⁴ Data Protection Commission, Ireland, 'Binding Decision 1/2021 on the Dispute Arisen on the Draft Decision of the Irish Supervisory Authority Regarding WhatsApp Ireland under Article 65(1)(a) GDPR' (2021).

⁴¹⁵ Established under Article 68 of the GDPR.

- Advising the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of the GDPR.
- Examining any question covering the application of the GDPR and issuing guidelines, recommendations, and best practices in order to encourage consistent application of the GDPR.
- Encouraging the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks.
- Issuing binding decisions to national SAs pursuant to the dispute resolution provision of Article 65.

In July 2023, the European Commission unveiled a proposed regulation⁴¹⁶ aimed at enhancing the coordination among DPAs when implementing the GDPR across borders. This proposal introduces precise procedural guidelines for DPAs managing GDPR applications in cases impacting residents across multiple Member States. For instance, it mandates the lead DPA to share a 'summary of key issues' with involved counterparts, detailing investigative aspects and preliminary opinions. This change is to facilitate early input and promote consensus from the outset. The perceived benefit for individuals is a clearer complaint process, while businesses will gain clarity on their procedural rights during inquiries into GDPR compliance.⁴¹⁷

⁴¹⁶ Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679COM/2023/348 (2023) final.

⁴¹⁷ European Commission, 'Stronger Enforcement of the GDPR in Cross-Border Cases' (*European Commission - European Commission*)
<https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3610> accessed 28 March 2024.

8. Liability under the GDPR

The GDPR has altered the way in which responsibility and liability is determined in Data Protection Law. While primary responsibility for compliance lies with the controller, a number of obligations now fall upon the processor who is directly liable for not complying with these duties.⁴¹⁸

Liability under the GDPR takes two forms. The first is recourse to the power of SAs explored above.⁴¹⁹ Additionally, any person who has suffered damages, whether material or non-material, as a result of an infringement of the GDPR has the right to receive compensation.⁴²⁰ The rationale for this recourse stems from the legal principle *ubi jus, ibi remedium*, 'where there is a right, there is a remedy.'⁴²¹

The starting position is that 'any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation.'⁴²² The GDPR applies a 'strict' liability regime, by which the controller is held liable for infringements of the Regulation even in the absence of fault. As van Alsenoy explains:

The controller shall therefore remain liable for unlawful processing activities undertaken by the processor on its behalf, even if the controller

⁴¹⁸ GDPR, Article 82(2)

⁴¹⁹ See [Chapter Four, Section 10. Supervisory Authorities](#).

⁴²⁰ GDPR, Article 82. See Radoslaw Strugala, 'Art. 82 GDPR: Strict Liability Or Liability Based on Fault?' (2020) 2020 European Journal of Privacy Law & Technologies (EJPLT) 71.

⁴²¹ Gabriela Zanfira-Fortuna, 'Article 82: Right to Compensation and Liability', in Christopher Kuner, Lee Bygrave, Christopher Docksey and Laura Drechsler (eds.), *The EU General Data Protection Regulation: A Commentary*. (Oxford University Press 2020) 1162.

⁴²² *ibid.* Article 82(2).

were to demonstrate an absence of fault in either his choice or supervision of the processor.⁴²³

Thus the lack of personal fault is insufficient to exempt a controller. However, a controller is exempted from liability 'if it proves that it is not in any way responsible for the event giving rise to the damage.'⁴²⁴ This exemption occurs only where there is a fault rate of zero percent.⁴²⁵ This can occur only if it can be proved that there is no causal link between the infringement of the GDPR and the damage suffered or where the violation is based upon an entirely unavoidable event.⁴²⁶

In terms of processors, liability for damage shall only apply in two situations. (i) If the processor has 'not complied with obligations' of GDPR 'specifically directed to processors' or (ii) where the processor 'has acted outside or contrary to lawful instructions of the controller.'⁴²⁷

Article 82(4) goes on to outline a system of joint and several liability whereby multiple controllers and processors who are responsible for damage shall each 'be held liable for the entire damage.' The rationale behind this is 'to ensure effective compensation of the data subject.'⁴²⁸ The full arrangement of liability is explained by the Council of the EU:

⁴²³ Van Alsenoy (n 373) 104.

⁴²⁴ *ibid.* Article 82(3).

⁴²⁵ Council of EU, 'Note from Presidency to JHA Counsellors on the Proposed General Data Protection Regulation – Chapter VIII, 9083/15, 27 May 2015', 3.

⁴²⁶ Paul Nemitz, 'Article 82 GDPR, Margin Number 7', *Ehmann, Selmayr, Data Protection Regulation*, (2nd edn, CH Beck 2018).

⁴²⁷ GDPR, Article 82(2).

⁴²⁸ Emilio Tosi, 'Unlawful Data Processing Prevention and Strict Liability Regime under EU GDPR' (2021) 7 *Italian Law Journal* 873, 880.

Each non-compliant controller and/or processor involved in the processing are held liable for the entire amount of the damage. However, a controller or processor is exempted from this liability if it demonstrates that it is not responsible for the damage (0% responsibility). Thus, only controllers or processors that are at least partially responsible for non-compliance (however minor, e.g. 5%) with the Regulation, and/or in case of a processor, with the lawful instructions from the controller, can be held liable for the full amount of the damage.⁴²⁹

As such it is entirely at the discretion of the damaged party whether to claim compensation from a specific responsible party or all parties bearing responsibilities. Should only one controller or processor pay full compensation then that party is entitled to claim from the other responsible parties ‘that part of the compensation corresponding to their part of responsibility for the damage.’⁴³⁰ Here a principle of *pro rata* responsibility is introduced.

The use of *pro rata* liability is expanded upon in Recital 146. It is explained that where multiple responsible controllers or processors are ‘joined to the same judicial proceedings’ then ‘compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing.’ However, such an arrangement is only deemed acceptable if ‘full and effective compensation of the data subject who suffered the damage is ensured.’

As the damaged party has recourse against any of the responsible parties, the GDPR may be said to apply a ‘cumulative’ liability regime.⁴³¹ This regime follows the Principles of European Tort Law (‘PETL’) established in 2005 by the European

⁴²⁹ Council of EU (n 425) 3.

⁴³⁰ GDPR, Article 82(5).

⁴³¹ Tosi (n 428) 879. See also Van Alsenoy (n 373) 111.

Group on Tort Law.⁴³² Under Article 9:101 of the PETL ‘where the whole or a distinct part of the damage suffered by the victim is attributable to two or more persons’ the victim may claim full compensation from any one or more responsible parties.⁴³³

9. Conclusion

The core of the EU Data Protection regime is formed by the GDPR, which both encapsulates and expands upon the established definitions, principles, and regulatory regimes of the past. In our analysis we have focused upon the GDPR’s controller-based accountability model which constitutes the core concern of this thesis. To expound upon the implications of the roles assumed by controllers, and joint controllers, we have also analysed the most salient obligations set forth by the GDPR.

Like the 1995 Directive, the GDPR is a principle based legal instrument. Through its provisions the principles of Data Protection Law have been deepened and expanded. Furthermore, an amplified understanding of consent and control is a theme throughout. When consent is to be relied upon as a basis for processing personal data a set of higher standards must be met. Article 7 of GDPR outlines the conditions for consent. These have been clarified by the EDPB⁴³⁴ and include: (i) the right to withdraw consent at any time; (ii) the requirement for the controller to demonstrate that consent has been given; (iii) Consent requested in return for goods or services in a ‘take-it-or-leave-it’ manner may not be regarded as freely given.

⁴³² European Group on Tort Law, ‘Principles of European Tort Law (PETL)’ (2005).

⁴³³ Tosi (n 428) 879. See also Van Alsenoy (n 373) 111.

⁴³⁴ European Data Protection Board (EDPB), ‘Guidelines 05/2020 on Consent under Regulation 2016/679. Adopted on 4 May 2020’ (2020).

Other significant additions found in GDPR include the requirement for data protection to be considered in the development phases of new technologies. A concept defined as Data Protection by Design and by Default.⁴³⁵ The right to compensation to individuals for breaches of their data protection rights has been added. SAs have been given significant authority to levy fines and compel compliance with the GDPR.

The severity of fines has been significantly increased with fines being levied in the amount of Euro 20 million or 4 percent of total worldwide annual turnover of an entity.

The seven fundamental principles of data protection incumbent upon controllers have also been highlighted: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. These principles form the bedrock of the EU's approach to data protection and guide the interpretation and application of the regulation's more specific provisions.

Finally, the chapter explored the liability regime under the GDPR, which introduces a system of joint and several liability for controllers and processors. This regime aims to ensure effective compensation for data subjects in cases of infringement, while also allowing for the apportionment of responsibility among multiple responsible parties.

⁴³⁵ GDPR, Article 25.

Chapter Five: An Expanding Regime

1. Introduction

The EU data protection framework of the 2020s represents a significant advancement from its predecessors, characterised by both increased scope and depth. The GDPR and associated legislation substantially expand upon the requirements established by the 1995 Directive, reflecting a more comprehensive approach to data protection. This enhanced Data Protection Regime constitutes only a component of a broader regulatory ecosystem governing online services, digital markets, and data exchange within the EU.

Furthermore, the fundamental concepts, roles, and responsibilities initially introduced into EU law through the 1995 Data Protection Directive have undergone significant expansion through judicial interpretation. Consequently, the comprehensive EU domain of digital regulation can be understood as the product of both legislative initiatives and evolving jurisprudence, reflecting the EU's commitment to adapting its regulatory framework to the complexities of our digital age. Scholars argue that the expansive scope of contemporary data protection legislation is a response to the imperative of safeguarding fundamental rights in the face of significant socio-technical transformations.⁴³⁶

⁴³⁶ See Lynskey, 'Complete and Effective Data Protection' (n 32) 297; Merlin Gömann, 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) 54 Common Market Law Review 567; Colin J Bennett and Robin M Bayley, 'Privacy Protection in the Era of "Big Data": Regulatory Challenges and Social Assessments' in Bart van der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016).

In this chapter we highlight the expansion of the European Data Protection Regime both through legislation and case law.

2. Legislative Expansion

Since the GDPR's implementation in 2018, the EU has introduced and enacted a series of legal instruments as part of its overarching European Digital Strategy. The legislation of this regime may be conceived of in terms of concentric circles represented in *Figure 7 below*.

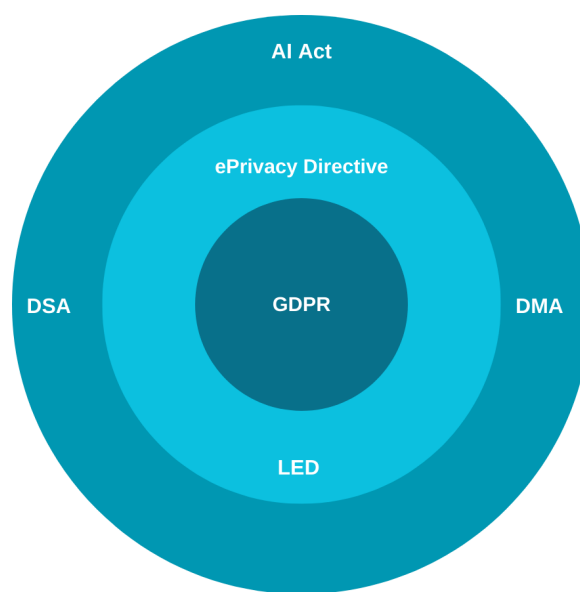


Figure 7. Concentric Circles of EU Digital Law

At the core is the GDPR itself, immediately beyond it are complementing legal instruments. These are the Law Enforcement Directive⁴³⁷ ratified along with the

⁴³⁷ Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and Repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 ('Law Enforcement Directive').

GDPR, the ePrivacy Directive first passed in 2002,⁴³⁸ and Regulation 2018/1725⁴³⁹ which governs personal data processed by EU institutions. In the widest circle we find new digital legislation including the Digital Services Act,⁴⁴⁰ the Digital Markets Act,⁴⁴¹ and the AI Act.⁴⁴²

In the following sections we outline this expanded regime. These laws provide added significance for this thesis through the varying accountability models which they employ. It is evident that the controller-based responsibility model is not the only option available to protect digital rights. What is more, overlapping obligations and supervision mechanisms will result from many of these laws.

⁴³⁸ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, as amended by Directive 2009/136/EC of 25 November 2009 [2002] OJ L201/37 ('ePrivacy Directive') .

⁴³⁹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC OJ L 295.

⁴⁴⁰ Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market For Digital Services [2022] OJ L277/1 ('Digital Services Act').

⁴⁴¹ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 reference OJ L 265/1 ('Digital Markets Act').

⁴⁴² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 OJ L, 2024/1689 ('Artificial Intelligence Act').

2.1 The Law Enforcement Directive ('LED')

The GDPR specifically excludes the processing of personal data for the prevention, investigation, detection, or prosecution of a criminal offence from its scope.⁴⁴³

Thus, the LED was passed as a complementing legal instrument.⁴⁴⁴

The LED utilises the same controller based responsibility model of the GDPR. Many of the same obligations apply in the LED as are found in the GDPR. Under the LED a controller must:

- Be able to demonstrate compliance with the LED.⁴⁴⁵
- Implement the principles of Data Protection by Design and Default.⁴⁴⁶
- Ensure appropriate technical and organisational safeguards for processed personal data.⁴⁴⁷
- Ensure sufficient guarantees from processors used.⁴⁴⁸
- Maintain a record of processing activities.⁴⁴⁹
- Carry out Data Protection Impact Assessments when envisioned processing is likely to result in a 'high risk to the rights and freedoms of natural persons'.⁴⁵⁰
- Notify the supervisory authority of personal data breaches without 'undue delay', and within 72 hours after having become aware of the incident.⁴⁵¹

⁴⁴³ GDPR, Article 2(2)(d).

⁴⁴⁴ See LED, Article 3. It must be noted that as the LED is a directive and not a regulation it requires the transposition into domestic law by EU Member States.

⁴⁴⁵ LED, Article 19.

⁴⁴⁶ *ibid.* Article 20.

⁴⁴⁷ *ibid.* Article 19.

⁴⁴⁸ *ibid.* Article 22.

⁴⁴⁹ *ibid.* Article 24.

⁴⁵⁰ *ibid.* Article 27.

⁴⁵¹ *ibid.* Article 30.

Beyond these, the LED lays out unique controller obligations without corresponding provisions in the GDPR. These include the obligation to:

- Make a 'clear distinction' between 'personal data of different categories of data subjects' including: (i) those suspected of committing a criminal offence, (ii) those convicted of a criminal offence, and (iii) victims of a criminal offence.⁴⁵²
- Distinguish between personal data based on facts and personal data based on personal assessments.⁴⁵³
- Verify the quality of personal data processed.⁴⁵⁴

More restrictive grounds for processing of personal data are also given. Under LED data processing is only considered lawful if it is necessary for the performance of a task carried out by a competent authority and based on Union law or Member State law.⁴⁵⁵ While, special category data can only be processed where it is 'strictly necessary' to do so.⁴⁵⁶

Given the specific scope of the LED, a more restrictive regime of data subject rights is outlined within it. Indeed, some rights such as the right to data portability are simply not relevant while others are subject to greater limitations.⁴⁵⁷ Thus, only three data subject rights remain. (i) The right for information to be made available

⁴⁵² *ibid.* Article 6.

⁴⁵³ *ibid.* Article 7.

⁴⁵⁴ *ibid.*

⁴⁵⁵ *ibid.* Article 8.

⁴⁵⁶ *ibid.* Article 10.

⁴⁵⁷ Commission nationale de l'informatique et des libertés (CNIL), 'Law Enforcement Directive: What Are We Talking About? | CNIL' <<https://www.cnil.fr/en/law-enforcement-directive-what-are-we-talking-about>> accessed 13 March 2024.

to the data subject, subject to possible limitations under Article 13. Furthermore, (ii) the right of access to information about data processing as established under Article 14, while Article 15 limits this right in order not to obstruct investigations or prejudice criminal prevention mechanisms. Finally, (ii) a right to rectification or erasure of incorrect personal data is established under Article 16.

2.2 The ePrivacy Directive

In 2002 the European Union passed ePrivacy Directive in order to widen telecommunications laws to cover all forms of electronic communications.⁴⁵⁸ The ePrivacy Directive was amended in November 2009⁴⁵⁹ as part of wider reforms to the EU telecommunications sector. The goal of these reforms was to ensure greater consumer choice and protection with an emphasis on consumer privacy.⁴⁶⁰ Importantly, the ePrivacy Directive lays out laws for the use of browser cookies and similar technologies. A browser cookie is a small piece of data sent from a website and stored on a user's device. Importantly, cookies are not isolated mechanisms but are often associated with identifiable personal details which users provide to use a platform or service. This link allows the entity responsible for setting the cookie to retain a consumer's information. This may allow a website to 'remember' user actions or preferences over a period of time by linking information to the user even if they delete the cookie.⁴⁶¹

⁴⁵⁸ Katie McMullan, 'Legislative Framework' in Eduardo Ustaran (ed), *European Data Protection* (2nd edn, IAPP Publications 2019). At 3.6.1.

⁴⁵⁹ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

⁴⁶⁰ McMullan (n 458).

⁴⁶¹ Róisín Á Costello, 'Impacts of AdTech on Privacy Rights and the Rule of Law' [2020] *Technology and Regulation* 11, 11.

Key provisions within the ePrivacy Directive include:

- The obligation for providers of publicly available electronic communications services to ensure appropriate technical and organisational measures to safeguard their services.⁴⁶²
- The requirement for opt-in consent for digital marketing, including emails, SMS and MMS messaging and faxes, but not person-to-person telephone marketing.⁴⁶³
- The restriction on the use of location data which may be processed only if it is made anonymous or if processed with the consent of users and for the duration necessary for the provision of a value-added service.⁴⁶⁴
- The obligation to inform subscribers when they are added to a directory.⁴⁶⁵
- The requirement for user consent to be gained for non-essential cookies placed on a user's device.⁴⁶⁶ This consent must occur with the user having been provided with clear and comprehensive information.⁴⁶⁷

The ePrivacy Directive does not utilise a controller-based responsibility model. Rather than applying a different framework, the instrument is silent on actors and accountability. Instead, member states are simply called upon to ensure respect for its provisions.

⁴⁶² ePrivacy Directive, Article 4.

⁴⁶³ *ibid.* Article 13.

⁴⁶⁴ *ibid.* Article 9.

⁴⁶⁵ *ibid.* Article 12.

⁴⁶⁶ *ibid.* Article 5 (3).

⁴⁶⁷ Data Protection Commission (Ireland), 'Guidance Note on Cookies and Other Tracking Technologies' <<https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf>> accessed 13 March 2024.

2.3 The Data Governance Act and The Data Act

In February 2020 the European Commission outlined its ‘European Strategy for Data’⁴⁶⁸ with the ambition of ‘creating a single market to ensure Europe’s global competitiveness and data sovereignty.’ Two regulations give life to this goal the Data Governance Act (‘DGA’) and the Data Act.⁴⁶⁹

The DGA introduces measures to improve trust and confidence in data sharing.⁴⁷⁰ It also aims to reduce barriers to transferring personal and non-personal data and improve reuse.⁴⁷¹ The DGA employs four ‘sets of measures’ in order to develop ‘trustworthy’ data-sharing. (I) Mechanisms to enable the reuse of public sector data which cannot be shared as open data. The DGA provides for rules and safeguards to facilitate re-use of protected data without compromising its status whenever it is possible under other legislation.⁴⁷² (II) Measures to ensure that data intermediaries will function as trustworthy organisers of data pooling within the common European data spaces. These mechanisms seek to respond to data sharing reticence on the part of companies which wish to preserve their

⁴⁶⁸ 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, 19.2.2020 COM (2020) 66’ <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>> accessed 18 November 2022.

⁴⁶⁹ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (‘Data Governance Act’) 2022.

⁴⁷⁰ European Commission, ‘European Data Governance Act | Shaping Europe’s Digital Future’ <<https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>> accessed 18 November 2022.

⁴⁷¹ Julie Baloup, ‘The Data Governance Act: New Rules for International Transfers of Non-Personal Data Held by the Public Sector’ (*European Law Blog*, 10 June 2021) <<https://europeanlawblog.eu/2021/06/10/the-data-governance-act-new-rules-for-international-transfers-of-non-personal-data-held-by-the-public-sector/>> accessed 16 November 2022.

⁴⁷² European Commission, ‘European Data Governance Act | Shaping Europe’s Digital Future’ (n 470).

competitive advantages.⁴⁷³ (III) Tools to foster ‘data altruism’ by making it easier for individuals and organisations to share data which can be used for the benefit of society. (IV) Structures and processes to facilitate data sharing across sectors and borders, and to enable the right data to be found for the right purpose.⁴⁷⁴

While the DGA establishes the mechanisms for sharing data, the Data Act clarifies ‘who can create value from data and under which conditions.’⁴⁷⁵ Specific provisions within the Data Act include measures aimed at (i) users of connected devices, (ii) small and medium enterprises (SMEs), (iii) Public sector bodies, and (iv) customers utilising cloud-based data processing services.⁴⁷⁶ The Data Act intends to rebalance the extractive nature of user generated data which is often ‘exclusively harvested by manufacturers.’⁴⁷⁷

The system of actors employed under the DGA and the Data Act mirrors that of the GDPR. Under Article 2 of both the DGA and Data Act the terms ‘data holders’, ‘data users’, ‘data’, and ‘data sharing’ are introduced. These correspond to the categories of ‘data subjects’, ‘controllers’, ‘personal data’ and ‘processing’ under Article 4 of the GDPR. Papakonstantinou and De Hert note that the DGA’s ‘mirroring’ of the GDPR system is ‘unmissable’ and as such refer to its provisions as holding ‘definitional GDPR mimesis’.⁴⁷⁸

⁴⁷³ *ibid.*

⁴⁷⁴ *ibid.*

⁴⁷⁵ ‘Data Act | Shaping Europe’s Digital Future’ <<https://digital-strategy.ec.europa.eu/en/policies/data-act>> accessed 28 November 2022.

⁴⁷⁶ ‘Data Act: Measures for a Fair and Innovative Data Economy’ (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113> accessed 25 November 2022.

⁴⁷⁷ *ibid.*

⁴⁷⁸ Papakonstantinou and De Hert (n 4).

2.4 The Digital Services Act

The DSA amends the twenty-two-year-old e-Commerce Directive⁴⁷⁹ creating new obligations and liabilities for digital intermediaries.⁴⁸⁰ The objectives of the DSA are to contribute to the ‘proper functioning of the internal market for intermediary services’ which both ‘facilitates innovation’ while ensuring respect for ‘fundamental rights enshrined in the Charter’ especially ‘the principle of consumer protection.’ Both goals are to be met through the provision of ‘harmonised rules for a safe, predictable and trusted online environment.’⁴⁸¹

Like the GDPR, the DSA has extraterritorial application covering provider services offered to recipients within the EU regardless of where the provider is based.⁴⁸² The actors regulated by the DSA are intermediary service providers, hosting services, online platforms, and very large online platforms.

(1) Intermediary Service Providers (ISPs) are defined by the DSA as online services which provide ‘mere conduit’ services, ‘caching’ services; or ‘hosting’ services.⁴⁸³ Examples include online search engines, wireless local area networks, cloud infrastructure services, or content delivery networks.⁴⁸⁴

⁴⁷⁹ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market [2000] OJ L178/1 (‘eCommerce Directive’).

⁴⁸⁰ Joao Pedro Quintais and Sebastian Felix Schwemer, ‘The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?’ (2022) 13 European Journal of Risk Regulation (EJRR) 191.

⁴⁸¹ DSA, Article 1.

⁴⁸² DSA, Article 2(1)

⁴⁸³ *ibid.* Article 3(g).

⁴⁸⁴ European Commission, ‘The Digital Services Act: Ensuring a Safe and Accountable Online Environment’ (*European Commission - European Commission*) <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en> accessed 23 March 2024.

(2) Hosting Services are intermediary service providers which store information at the request of the service user. Examples include cloud services and services enabling sharing information and content online, including file storage and sharing.⁴⁸⁵

(3) Online Platforms are hosting services which at a user's request 'store and disseminate' information to the public.⁴⁸⁶ Examples include online marketplaces, app stores, collaborative economy platforms and social media platforms.⁴⁸⁷

(4) Very large online platforms (VLOPs) and very large online search engines (VLOSE) are defined by their size. Entities require 45 million active monthly users in the EU to fall within this category.⁴⁸⁸

The DSA applies a tiered approach to its provisions. The most basic obligations apply to all online intermediary service providers with more strenuous obligations placed upon online platforms and the most rigorous apply to the largest actors.⁴⁸⁹ This tiered approach is represented in *Figure 8* below.

⁴⁸⁵ *ibid.*

⁴⁸⁶ DSA, Article 3(i).

⁴⁸⁷ European Commission, 'The Digital Services Act' (n 484).

⁴⁸⁸ DSA, Article 33 of the DSA.

⁴⁸⁹ European Commission, 'The Digital Services Act' (n 484).

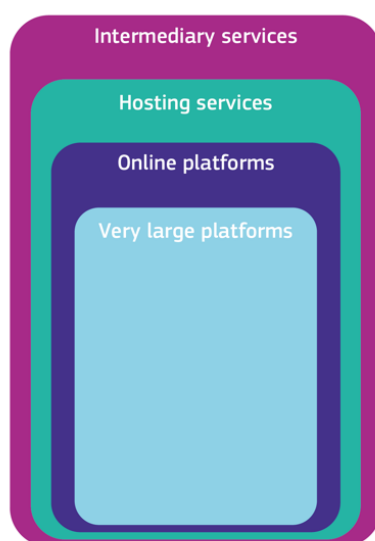


Figure 8. Tiered Approach under DSA⁴⁹⁰

The specific obligations which apply to each of the entities within the DSA is represented in *Table 5* below.

Table 5. Obligations under the DSA⁴⁹¹

DSA Obligations				
	Intermediary services	Hosting services	Online platforms	Very large Online platforms
Transparency reporting	•	•	•	•
Requirements on terms of service – due account of fundamental rights	•	•	•	•
Cooperation with national authorities	•	•	•	•

⁴⁹⁰ *ibid.*

⁴⁹¹ *ibid.*

Points of contact and, where necessary, legal representative	•	•	•	•
Notice and action and obligation to provide information to users		•	•	•
Reporting criminal offences		•	•	•
Complaint and redress mechanism and out of court dispute settlement			•	•
Trusted flaggers			•	•
Measures against abusive notices and counter-notices			•	•
Special obligations for marketplaces, e.g. vetting credentials of third-party suppliers ("KYBC"), compliance by design, random checks			•	•
Bans on targeted adverts to children and those based on special characteristics of users			•	•
Transparency of recommender systems			•	•
User-facing transparency of online advertising			•	•
Risk management obligations and crisis response				•

External & independent auditing, internal compliance function and public accountability				•
User choice not to have recommendations based on profiling				•
Data sharing with authorities and researchers				•
Codes of conduct				•
Crisis response cooperation				•

On 25 April 2023, the first designation decisions for VLOPs and VLOSEs were made by the European Commission.⁴⁹² The full list as of 18 January 2024 is laid out in *Table 6* below.⁴⁹³

⁴⁹² European Commission, 'Press Release. Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines. 25 April 2023, Brussels.' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413> accessed 26 January 2024.

⁴⁹³ European Commission, 'Supervision of the Designated Very Large Online Platforms and Search Engines under DSA' <<https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>> accessed 26 January 2024.

Table 6. VLOPs and VLOSEs Designated by The European Commission⁴⁹⁴

Very Large Online Platforms			
Main Establishment of the Provider in the EU	Designated Service	Average Monthly Users in Millions	Digital Services Coordinator
Alibaba (Netherlands) B.V.	AliExpress	104,3 (Self-Reported)	Netherlands
Amazon Services Europe S.à.r.l.	Amazon Store	181,3 (Self-Reported)	Luxembourg
Apple Distribution International Limited	App Store	123 (Self-Reported)	Ireland
Aylo Freesites Ltd.	Pornhub	Above 45 (Determined by European Commission)	Cyprus
Booking.com B.V.	Booking.com	Above 45 (Determined by European Commission)	Netherlands
Google Ireland Ltd.	Google Play	284,6 (Self-Reported)	Ireland
	Google Maps	275,6 (Self-Reported)	
	Google Shopping	70,8 (Self-Reported)	
	YouTube	416,6 (Self-Reported)	

⁴⁹⁴ *ibid.*

LinkedIn Ireland Unlimited Company	LinkedIn	Logged-in active users: 45.2 (Self-Reported) Logged-out site visits: 132.5 (Self-Reported)	Ireland
Meta Platforms Ireland Limited (MPIL)	Facebook	259 (Self-Reported)	Ireland
	Instagram	259 (Self-Reported)	
Pinterest Europe Ltd.	Pinterest	124 (Self-Reported)	Ireland
Snap B.V.	Snapchat	102 (Self-Reported)	Netherlands
Technius Ltd.	Stripchat	Above 45 (Determined by European Commission)	Cyprus
TikTok Technology Limited	TikTok	135,9 (Self-Reported)	Ireland
Twitter International Unlimited Company (TIUC)	X	115,1 (Self-Reported)	Ireland
WebGroup Czech Republic	XVideos	160 (Self-Reported)	Czech Republic
Wikimedia Foundation Inc 3	Wikipedia	151,1 (Self-Reported)	Any Member State
Zalando SE	Zalando	Monthly average in retail: 74.5 (Self-Reported)	Germany

		Monthly average for third-party content: 26.8 (Self-Reported)	
<u>Very Large Online Search Engines</u>			
Main Establishment of the Provider in the EU	Designated Service	Average Monthly Users in Millions	Digital Services Coordinator
Google Ireland Ltd.	Google Search	364 (Self-Reported)	Ireland
Microsoft Ireland Operations Limited	Bing	119 (Self-Reported)	Ireland

In December 2023, the European Commission opened its first proceedings into a VLOP to determine whether X (formerly Twitter) had violated the DSA. The alleged breaches occurred in multiple areas including risk management, content moderation, use of dark patterns, clarity in advertising, and provision of data to researchers.⁴⁹⁵

This decision followed a preliminary review which considered X's transparency report issued on 3 November 2023,⁴⁹⁶ and responses to a formal request for

⁴⁹⁵ European Commission, 'Press Release. Commission Opens Formal Proceedings against X under the DSA. 18 December 2023. Brussels' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709> accessed 26 January 2024.

⁴⁹⁶ X, Twitter International Unlimited Company (TIUC), 'DSA Transparency Report. X, Twitter International Unlimited Company (TIUC). 3 November 2023.' <<https://transparency.twitter.com/dsa-transparency-report.html>> accessed 26 January 2024.

information,⁴⁹⁷ which covered the spread of unlawful content during the terrorist attacks by Hamas against Israel on 7 October 2023 and subsequent Israeli invasion of Gaza.⁴⁹⁸

2.5 The Digital Markets Act

The Digital Markets Act targets large scale online platforms identified as ‘gatekeepers.’ Articles 101 and 102 of the TFEU⁴⁹⁹ allow for anticompetitive actions to be regulated in an *ex-post* manner. Through the DMA, certain anticompetitive behaviours would be prohibited *ex ante*.⁵⁰⁰

The criteria for gatekeepers are established under Article 3 (1) of the DMA.

1. An undertaking shall be designated as a gatekeeper if:
 - (a) it has a significant impact on the internal market;
 - (b) it provides a core platform service which is an important gateway for business users to reach end users; and
 - (c) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.

⁴⁹⁷ European Commission, ‘Press Release. The Commission Sends Request for Information to X under DSA. 12 October 2023, Brussels.’ (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953> accessed 26 January 2024.

⁴⁹⁸ European Commission, ‘Press Release. Commission Opens Formal Proceedings against X under the DSA. 18 December 2023. Brussels’ (n 495).

⁴⁹⁹ Treaty on the Functioning of the European Union (TFEU). OJ C 326/47. 1957.

⁵⁰⁰ Pieter Van Cleynenbreuge, ‘Digital Markets Act: Beware of Procedural Fairness and Judicial Review Booby-Traps!’ (*European Law Blog*, 24 June 2021) <<https://europeanlawblog.eu/2021/06/24/digital-markets-act-beware-of-procedural-fairness-and-judicial-review-booby-traps/>> accessed 23 March 2024. See also Axel Gutermuth, Alexander Italianer and Laurent Thiry, ‘Europe’s Digital Markets Act: New Regulation of Gatekeepers in the Digital Platform Economy.’ (2022) 34 *Intellectual Property & Technology Law Journal* 15.

The threshold of holding a ‘significant impact on the internal market’ under Article 3(1)(a) is to be met where an undertaking either ‘achieves an annual Union turnover equal to or above EUR 7.5 billion in each of the last three financial years’ or ‘where its average market capitalisation or its equivalent fair market value amounted to at least EUR 75 billion in the last financial year.’⁵⁰¹

An extensive list of ‘core platform services’ is given under Article 2(2) of the DMA including: online intermediation services, online search engines, online social networking services, video-sharing platform services, operating systems, web browsers, virtual assistants, cloud computing services, and online advertising services.

Core platform services are to be understood as important gateways are those with 45 million monthly active end users and at least 10 000 yearly active business users established or located in the Union.⁵⁰²

Finally, for an undertaking to enjoy an ‘entrenched and durable position’ as required by Article 3(1)(b) it must have met the thresholds of (I) 45 million monthly active end users and (II) at least 10 000 yearly active business users in each of the past three years or it be foreseeable that it will meet these thresholds.⁵⁰³

Obligations for gatekeepers under the DMA include the responsibility to:

- Allow users to simply uninstall software applications and change default settings on operating systems.⁵⁰⁴

⁵⁰¹ DMA, Article 3(2)(a).

⁵⁰² DMA, Article 3(2)(b).

⁵⁰³ DMA, Article 3(2)(c).

⁵⁰⁴ Article 6(3).

- Allow third parties to inter-operate with the gatekeeper's own services.⁵⁰⁵
- Provide advertising performance measuring tools and data to business users.⁵⁰⁶
- Allow end users to move their data to a different platform.⁵⁰⁷
- Allow business users access to the data that they have generated in their use of the gatekeeper's platform.⁵⁰⁸

Gatekeepers are further prohibited from *inter alia*:

- Reusing personal data of end users gained from business users for the gatekeeper's own purposes including advertising.⁵⁰⁹
- Using business user data to compete with business users.⁵¹⁰
- Ranking their own services or products above those of business users.⁵¹¹
- Preventing consumers from linking to businesses outside of the gatekeeper platform.⁵¹²

2.6 The AI Act

2.6.1 Overview

In its 2020 Resolution on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies, the European Parliament suggested that the Commission introduce a Regulation 'on ethical principles for the development,

⁵⁰⁵ Article 6(4).

⁵⁰⁶ Article 6(8).

⁵⁰⁷ Article 6(9). This corresponds to the Right to Data Portability under Article 20 of the GDPR.

⁵⁰⁸ Article 6(10).

⁵⁰⁹ Article 5(2).

⁵¹⁰ Article 6(2).

⁵¹¹ Article 6(5).

⁵¹² Article 5(4).

deployment and use of artificial intelligence, robotics and related technologies.’ This led to the European Commission releasing its proposal for a comprehensive Regulation to govern the use of Artificial Intelligence and Machine learning tools on 21 April 2021.⁵¹³ Following several months of ‘trilogue’ negotiations between the European Parliament, the EU Council of Ministers (representing the governments of EU Member States), and the European Commission an agreement on the AI Act was reached on 9 December 2023.⁵¹⁴ The final text was published in the Official Journal of the European Union on July 12, 2024.⁵¹⁵

Basic regulation of AI is already found in the GDPR. Through Article 22 individuals are granted a right not to be subject to decisions based solely on automated decision making if the results carry significant impacts. Moreover, the use of new technological methods of data processing resulting in ‘a high risk to the rights and freedoms of natural persons’ carries the obligation to conduct an impact assessment under Article 35. The AI Act represents a significant expansion of these clauses.

The AI Act governs the use of AI systems defined in Article 3(1):

‘AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after

⁵¹³ European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 Final, (Apr. 21, 2021)’ (n 5).

⁵¹⁴ European Commission, ‘Statement by President von Der Leyen on the AI Act 9 December 2023’ (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/statement_23_6474> accessed 20 January 2024.

⁵¹⁵ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 OJ L, 2024/1689 (‘Artificial Intelligence Act’).

deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

The European Commission describes the AI Act as a risk based legal instrument wherein systems are divided into four levels.⁵¹⁶ (I) At the uppermost level are ‘unacceptable risks’ which are prohibited. (II) Below this level are AI uses involving high risks, these are permitted only when certain compliance obligations have been met. (III) Thereafter, certain AI uses with mandatory transparency obligations are outlined. Importantly level two and three are not exclusive as certain activities may fall within the remit of both levels’ obligations. Finally, (IV) at level four are AI activities with minimal to no risk, which are permitted with no restrictions.⁵¹⁷ These tiers are illustrated in *Figure 9* below.

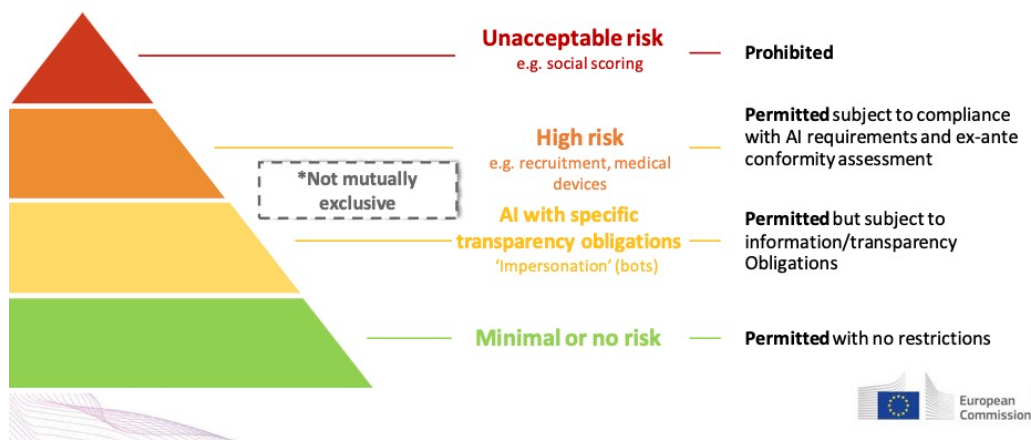


*Figure 9. Risk-Based Approach of the AI Act*⁵¹⁸

⁵¹⁶ European Commission, ‘Artificial Intelligence – Questions and Answers’ (European Commission - European Commission, 12 December 2023) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683> accessed 20 January 2024.

⁵¹⁷ *ibid.*

⁵¹⁸ Lucilla Sioli, ‘A European Strategy for Artificial Intelligence’ (CEPS webinar -European approach to the regulation of artificial intelligence, 23 April 2021).

Furthermore, the AI Act takes into account the potential systemic risks associated with general-purpose AI models. These versatile models are increasingly forming the foundation of systems employed throughout the Union. Powerful AI models have the potential to trigger severe mishaps or to be exploited for extensive cyberattacks. Should a model disseminate detrimental biases across a broad array of applications, the repercussions could impact a vast number of individuals.⁵¹⁹ Providers of such high-risk models are thus obligated to evaluate and mitigate risks, document serious incidents, perform tests and model assessments, guarantee cybersecurity, and disclose information regarding their models' energy consumption. They must collaborate with the European AI Office to formulate Codes of Conduct, clarifying the regulations in association with other experts. A scientific panel will have a pivotal role in monitoring general-purpose AI models.⁵²⁰

Presently, models trained with computing power exceeding 10^{25} Floating Point Operations ('FLOPs') are considered potentially hazardous, as increased computational resources typically yield more potent AI models. FLOPS signifies the total operations a computing system is capable of executing within one second. The figure 10^{25} denotes the strength of the supercomputing resources on which an AI model has been developed, as well as the duration of its training. This metric is a reflection of the sheer magnitude of computational energy invested in the training phase. The 10^{25} FLOPs threshold is deemed suitable for GPAI models with systemic risks as it encompasses the most sophisticated current models, such as OpenAI's GPT-4 and possibly Google DeepMind's Gemini. The understanding of these models is still emerging, and their potential systemic risks justify the

⁵¹⁹ European Commission, 'Artificial Intelligence – Questions and Answers' (n 516).

⁵²⁰ *ibid.*

imposition of additional obligations on their providers.⁵²¹ The AI Office within the Commission retains the authority to revise this benchmark based on technological progression and may also designate other models as systemically risky based on additional factors such as user count or autonomy level.

2.6.2 Accountability Regime

An AI Service is likely to be governed by both the GDPR and the AI Act. The anticipated result is one which we may define as the imposition of ‘contrasting and competing’ obligations as will be discussed in Chapter Nine.⁵²²

The AI Act does not employ a controller and processor-based system like that of the GDPR. Instead, specific obligations are placed upon different actors. These parties, their responsibilities, and their potential liabilities are laid out in the following subsections.

AI Providers

Article 3(3) of the AI Act gives the definition of AI providers:

‘provider’ means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge;

⁵²¹ *ibid.*

⁵²² See Chapter Nine, Section 9. Complementing and Competing Obligations.

The most onerous of the AI Act's obligations fall onto AI providers.⁵²³ In the case of High-Risk AI Systems these obligations are laid out in Article 16 and include:

- Establishing and implementing a quality management structure including a risk management framework.
- Logging obligations to enable AI deployers to monitor the operation of the high-risk AI System.
- Ensuring the quality of datasets used for training AI.
- Registering the AI System in accordance with Article 49 of the AI Act.
- Ensuring their system undergoes conformity assessment and potentially re-assessment in the case of significant modification.
- Affixing the EU conformity assessment 'CE' marking onto the signing declaration of conformity.
- Conducting ongoing monitoring at the post-market stage.
- Ensuring the accuracy, robustness, and cybersecurity of systems themselves.
- Designing the AI System to allow for human oversight.

Beyond these obligations Article 50 provides a general transparency obligation upon AI providers to ensure that all systems⁵²⁴ which are intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI System.

AI deployers

The definition of an AI deployer is given in Article 3(4) as 'a natural or legal person, public authority, agency or other body using an AI system under its

⁵²³ Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 4 Computer Law Review International 97, 102.

⁵²⁴ Not only High-Risk AI Systems.

authority.’ As in the case of the GDPR an exception to this scope is laid out ‘where the AI system is used in the course of a personal non-professional activity’.

Specific obligations for deployers of High-Risk AI Systems are laid out in Article 26 of the AI Act and include:

- Operating the AI System in accordance with its instructions of use.
- Ensuring human oversight when using the AI System.
- Vigilantly monitoring AI systems and halting operations should any grave concerns arise.
- Preserving and managing logs automatically generated by the system as required by law.
- Ensuring that input data is relevant in view of the intended purpose of the high-risk AI System.
- Monitoring operations of the AI System for possible risks.
- Informing the AI provider or distributor about any serious incident or any malfunctioning of the system.

Additionally, the AI Act also introduces the obligation for a Fundamental Rights Impact Assessment (‘FRIA’) to be undertaken by deployers in certain circumstances.⁵²⁵ When utilising high-risk AI systems, which have the potential to significantly influence fundamental rights, it is mandatory for public entities and private operators in public service, as well as those offering certain high-risk systems, to conduct a FRIA. This assessment must be reported to the relevant national authority.

⁵²⁵ AI Act, Article 27.

The assessment should comprehensively detail the operational processes that will incorporate the high-risk AI system, including usage duration and frequency. It should identify the individual and collective profiles likely to be influenced by the system's deployment, pinpoint specific risks of harm to these groups, and describe measures for human oversight and responses to risk realisation. In cases where a DPIA has already been performed by the provider, this should be integrated with the FRIA to ensure a cohesive evaluation of impacts on fundamental rights.⁵²⁶

Furthermore, general transparency requirements are placed upon AI System users in certain situations. Specifically, Article 50(3) mandates that users of emotion recognition or biometric categorisation systems must inform those who will be subject to them. While Article 50(2) mandates transparency obligations for so called 'deep-fake' content. This provision applies to users of systems which generate or manipulate image, audio or video content of existing persons, objects, places or other entities or events to create a false appearance of truth or authenticity. All such content must be accompanied by a disclosure of its artificial nature.

Importantly all other legal obligations including those under the GDPR apply to AI deployers.

AI System Importers and Distributors

The AI Act further extends obligations to the importer and distributor of an AI System. The definition of an importer is given under Article 3(6)

'[I]mporter' means a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country;

⁵²⁶ European Commission, 'Artificial Intelligence – Questions and Answers' (n 516).

Specific obligations are placed upon AI importers under Article 23 of the AI Act. Prior to placing a high risk-AI System on the market importers must ensure that:

- The appropriate conformity assessment procedure has been carried out by the provider of that AI System.
- The provider has drawn up the required technical documentation.
- The system bears the required conformity marking and is accompanied by the required documentation and instructions of use.

Importers are further prohibited from placing an AI System on the market if they have reason to consider that it is not in conformity with the AI Act.⁵²⁷ Importers also must ensure transparency and availability by providing their name, registered trade name, and the address at which they can be contacted on the system or its accompanying packaging and documentation.⁵²⁸ Importers must ensure safe storage and transit of the system⁵²⁹ and must be able to provide national authorities with all necessary information and documentation to demonstrate the conformity of the system with the AI Act.⁵³⁰

Additional obligations fall upon the distributor of an AI System. This party is defined in Article 3(7):

‘[D]istributor’ means a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market;

The obligations which fall upon a distributor of an AI System are substantially similar to those of an Importer. Prior to placing a product on the market,

⁵²⁷ AI Act, Article 23(2).

⁵²⁸ *ibid.* Article 23(3).

⁵²⁹ *ibid.* Article 23(4).

⁵³⁰ *ibid.* Article 23(6).

distributors must ensure that the system (i) bears the required CE conformity marking, (ii) is accompanied by the required documentation and instructions of use, and that (iii) the provider and the importer have complied with their AI Act obligations.⁵³¹ As is the case for importers, distributors are prohibited from placing an AI System on the market if they have reason to consider that it is not in conformity with the AI Act.⁵³² Moreover, distributors must ensure safe storage and transit of the system⁵³³ and must be able to provide national authorities with all necessary information and documentation to demonstrate the conformity of the system with the AI Act.⁵³⁴

2.7 Conclusion

Many of these laws create what we may term overlapping obligations and mechanisms of enforcement. A notable case is the usage of cookies and similar tracking technologies. These are governed by the ePrivacy Directive but will also fall within the remit of the GDPR as the CJEU has confirmed in *Breyer*⁵³⁵ that online identifiers constitute personal data. As such both regimes are relevant to cookie use. The result is that although the GDPR allows for any of the six lawful bases to process personal information, only consent will be valid for cookies per the ePrivacy Directive. Similarly, when personal data is processed within an AI Service this operation will be governed by both the GDPR and the AI Act. The anticipated result is one in which an individual will now hold 'complementing and competing' obligations under both laws.

⁵³¹ Ibid. Article 24(1).

⁵³² Ibid. Article 24(2).

⁵³³ Ibid. Article 24(4).

⁵³⁴ Ibid. Article 24(5).

⁵³⁵ *Case C-582/14 Breyer v. Bundesrepublik Deutschland* [2016] EU:C:2016:779 (n 324).

Complementary enforcement has also emerged, with an important precedent in the European Commission's investigation into Meta's change of terms and conditions in 2023. Successful challenges were raised to its lawful basis for processing personal data to provide personalised advertising. In November 2023 Meta, the parent company of Facebook and Instagram, introduced a novel subscription-based model known as 'pay or okay' in response to successful challenges to its use of personal data to provide personalised advertising.⁵³⁶ This new approach offers users in the European Economic Area a choice between continuing to use Meta's services free of charge while consenting to personalised advertising, or opting for a subscription model that precludes the use of their personal data for ad targeting. In response to these changes the privacy advocacy group NOYB (None of Your Business) has filed a complaint against Meta under the GDPR.⁵³⁷ At the same time the European Commission has used its enforcement powers under the Digital Markets Act to investigate this new model.⁵³⁸ Here, we have a situation in which regulation of this model is likely to result from a combination of both Data Protection Law and complementing digital legislation.

Moreover, the diverse accountability models employed by these laws offer critical insights for this thesis, underscoring that the controller-based model is not the sole approach to safeguarding digital rights. Rather, this model emerged as a

⁵³⁶ *Case C-252/21 Meta Platforms and Others (General terms of use of a social network) [2023] EU:C:2023:537*; 'Data Protection Commission Announces Conclusion of Two Inquiries into Meta Ireland' (*Data Protection Commission*) <<https://www.dataprotection.ie/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland>> accessed 14 August 2024. And

⁵³⁷ 'Noyb Files GDPR Complaint against Meta over "Pay or Okay"' <<https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay>> accessed 14 August 2024.

⁵³⁸ European Commission, 'Commission Sends Preliminary Findings to Meta over Its "Pay or Consent" Model for Breach of the Digital Markets Act.' (*European Commission - European Commission*, 1 July 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582> accessed 14 August 2024.

contingent response to specific circumstances and concerns as is discussed in the next chapter.⁵³⁹ The existence of alternative frameworks demonstrates the evolving nature of data protection strategies and highlights the importance of contextual factors in shaping regulatory approaches. This diversity in accountability models invites a more nuanced examination of the efficacy and appropriateness of the GDPR paradigm, challenging the notion of a one-size-fits-all solution and emphasising the need for adaptable, context-sensitive regulatory frameworks in our digital era.

3. Judicial Expansion

Since the EU first adopted data protection laws in 1995, the EU's data protection framework has been distinguished by its comprehensive scope of application. The framework's key concepts, which determine its material scope, are broadly defined, while exceptions are narrowly construed. Therefore, given that an increasing proportion of societal activity now incorporates a digital component, data protection has evolved into an almost ubiquitous legal framework.

This expansive reach of data protection law is not solely attributable to socio-technical developments; rather, it is equally the product of legal evolution. The broad applicability of data protection regulations reflects both the increasing digitalization of society and the deliberate expansion of the legal framework through legislative and judicial processes. This dual influence underscores the dynamic nature of data protection law, as it adapts to encompass the growing digital footprint of modern society while simultaneously expanding its legal purview.⁵⁴⁰

⁵³⁹ See [Chapter Six, Section 2. Controller Based Accountability: Historical Origins.](#)

⁵⁴⁰ Lynskey, 'Complete and Effective Data Protection' (n 32) 302.

Numerous instances of this expansion may be noted; two are highlighted in the following section: (1) the definition of personal data itself, and (2) the requirements for international data transfers. These two examples contextualise the expansion of the role of the controller by the CJEU. We are to understand that this is not an isolated act, but a component of an overall judicial philosophy.

3.1 The Expanded Scope of Personal Data

Data protection has evolved into an almost inescapable legal framework, extending its reach across a vast spectrum of endeavours. This phenomenon has led to the characterisation of data protection as a universally applicable legal construct. Thus, in phrasing introduced by Purtova,⁵⁴¹ data protection has become known as ‘the law of everything.’

As already discussed in this thesis,⁵⁴² the definition of personal data is expansive, encompassing ‘any information relating to an identified or identifiable natural person’. The application of data protection law is binary: it applies to the processing of ‘personal’ data but not to non-personal data.⁵⁴³ Consequently, the classification of data as ‘personal’ is crucial. While anonymous data falls outside the scope of personal data, pseudonymized data, which can be attributed to a specific individual when combined with additional separately held information, is considered personal data.

Taken together the constitutive elements of this definition are so extensive as to render it challenging to conceive of any digital activity that would not fall within

⁵⁴¹ Purtova (n 31).

⁵⁴² See [Chapter Four, Section 2.1 Personal Data](#).

⁵⁴³ Lynskey, ‘Complete and Effective Data Protection’ (n 32) 302.

the law's remit. The threshold for the law's application is easily met in many everyday scenarios. For instance, sharing a photograph or video on social media constitutes processing of personal data. The content is linked to individuals through its subject matter, and its processing may impact them, even if they are not immediately identifiable. Importantly, identifiability extends beyond immediate recognition to potential identification by third parties using reasonably likely means, such as combining the shared data with other available information.

544

Beyond the issue of identifiability, the element of 'information' within the definition of personal data is expansive, encompassing even inaccurate or artificially generated content. Lynskey provides the example of an academic submission by an author who has relied entirely upon an AI tool like ChatGPT. This article, despite containing inaccuracies or citing non-existent sources, would still qualify as 'information' under this broad interpretation. Initially, one might assume that an academic article, being primarily the product of intellectual effort rather than personal information, would not constitute personal data. However, the CJEU has adopted an expansive interpretation of personal data. In its ruling in *Nowak*,⁵⁴⁵ the Court ruled that information will be considered to relate to an individual if it is linked to them by virtue of its 'content, purpose, or effect'. Applying this principle to an academic context, the CJEU determined in *Nowak* that an examination script in an open-book examination 'related to' the candidate. The Court reasoned that the content of the answers reflected the candidate's knowledge and competence, the purpose of processing was to evaluate their professional abilities and suitability, and the use of this information could potentially impact their rights and interests. Furthermore, the Court held that the

⁵⁴⁴ Case C-582/14 *Breyer v Bundesrepublik Deutschland* [2016] EU:C:2016:779 at [43].

⁵⁴⁵ Case C-434/16 *Nowak v Data Protection Commission* [2017] EU:C:2017:994 at [35].

examiner's comments also related to the candidate, as they served to record an evaluation of the candidate's performance and could affect the candidate's interests. This reasoning can be extended by analogy to the academic peer review process. An article submitted for peer review, along with the reviewer's comments, would likely be considered personal data under this expansive interpretation. The article reflects the author's knowledge and abilities, while the review process aims to evaluate the author's work and can significantly impact their academic standing and career prospects.⁵⁴⁶

Additionally, academic literature shows that this definition can be extended to even more marginal connections to individuals. Purtova argues that even environmental data, such as weather information or wastewater composition, could potentially be classified as personal data if used to evaluate or influence individual behaviour. In support she provides the example of a smart city project in Eindhoven, Netherlands, where a public-private collective initiated efforts to anticipate, prevent, or de-escalate anti-social behaviour on *Stratumseind*, a street renowned for its vibrant social scene. The project collects data from various sources, including weather information such as hourly rainfall, wind direction, and speed. Purtova posits that this weather information, once digitised and integrated into the project's analytical framework, takes on new significance in relation to individuals. Her argument rests on three key points, first, the weather data, once digitised, becomes a form of 'information' that can be systematically analysed. Second, this information 'relates to' individuals insofar as it is utilised to assess and potentially influence behaviour deemed problematic. Finally, when combined with other sensor-collected data, this information could potentially lead to the 'identification' of specific individuals - a core objective of the project.⁵⁴⁷

⁵⁴⁶ Lynskey, 'Complete and Effective Data Protection' (n 32) 304–305.

⁵⁴⁷ Purtova (n 31) 57–60.

In a similar vein van der Sloot argues that wastewater can fall within the gamut of personal data and thus its analysis should be subject to Data Protection Law's provisions.⁵⁴⁸

The impact of the expanded definition of personal data results in an increase in the circumstances in which controllers must be able to apply the principles and mechanisms of the GDPR. Moreover, as the scope of personal data is increased so too are the instances in which unknowing and unintended personal data processing will take place. In such circumstances data subjects are forced to seek to exercise their rights, and thus gain *control of their data*, against *controllers* who are unlikely to be aware that such processing is even taking place. At the same time per Article 8(3) of the Charter, Supervisory Authorities are to exercise their mandated *control* over compliance of Data Protection Law against ever more controllers in ever increasing instances of data processing.

3.2 The Requirements for International Transfers of Data

As has been noted, the GDPR is characterised by a duality of objectives.⁵⁴⁹ On one hand, legislators have prioritised the safeguarding of fundamental rights and freedoms. Concurrently, there is a pronounced emphasis on facilitating economic growth and supporting market dynamics. This dual focus reflects the complex interplay between individual privacy concerns and the economic imperatives of data-driven commerce in the EU regulatory framework. A key illustration of the tension between these goals occurs in the case of transfers of personal data outside of the European Economic Area.

⁵⁴⁸ Bart van der Sloot, 'Truth from the Sewage: Are We Flushing Privacy down the Drain?' (2021a) 12 European Journal of Law and Technology.

⁵⁴⁹ See [Chapter Three, Section 3. The Ambitions of the EU Data Protection Regime.](#)

Under both the GDPR and the 1995 Directive, the simplest mechanism for such transfers is for the European Commission to designate a third country as providing an 'adequate level of protection' for data subjects.⁵⁵⁰ This designation facilitates the unhindered exchange of information between the EU and that country, yielding considerable economic advantages. In circumstances where an adequacy decision is not in place, the transfer of personal data may proceed under the condition that the data exporter has implemented and guaranteed the application of appropriate safeguards for the transferred data.⁵⁵¹

Given the stringent criteria for non-EU nations, alternative methods are available for data transfer from the EU, provided there are sufficient safeguards and that individuals' rights, and legal remedies are enforceable. Among these, 'standard contractual clauses' ('SCCs') and 'binding corporate rules' ('BCRs') stand out. BCRs, approved by the relevant EU authority as per Article 63 of the GDPR, enable intra-organisational data movement, while SCCs, based on Commission-approved templates, are widely used for transferring data to external entities in third countries. To use SCCs, data senders must embed these clauses in agreements with data receivers, thus binding both parties legally.⁵⁵²

For transfers to the United States, the US Department of Commerce, and the European Commission, jointly developed a self-regulatory framework in the form of the Safe Harbor mechanism. Following extensive negotiations, the Commission issued a decision on July 26, 2000, declaring that the Safe Harbor Privacy

⁵⁵⁰ GDPR, Article 45(1).

⁵⁵¹ *ibid.* Article 46.

⁵⁵² Maria H Murphy, 'Assessing the Implications of Schrems II for EU-US Data Flow' (2022) 71 *International and Comparative Law Quarterly* 245, 249.

Principles provided adequate protection for personal data.⁵⁵³ However this designation was undermined in 2013 with Edward Snowden's revelations of extensive data collection and surveillance by US intelligence agencies.⁵⁵⁴ In response, Maximillian Schrems challenged Facebook Ireland's transfer of his personal data to US based servers. Schrems filed a complaint with the Irish Data Protection Commission ('DPC') under the Data Protection Directive, seeking to prohibit such transfers. His argument centred on the inadequacy of US law in protecting personal data from surveillance practices conducted under national security measures. The Irish DPC initially rejected Schrems' complaint, citing the European Commission's Safe Harbour Decision that deemed US data protection adequate. Schrems sought judicial review, leading to the Irish High Court referring questions to the Court of Justice. In its ruling on those questions in *Schrems I*,⁵⁵⁵ the CJEU invalidated the Safe Harbour Decision, finding it failed to ensure adequate protection for data transferred to the US.

Subsequently, the Privacy Shield Decision replaced Safe Harbour, introducing improvements such as an ombudsman system for independent oversight. However, the underlying state surveillance practices that had prompted the original challenge remained largely unchanged, raising questions about the effectiveness of the new framework in addressing the fundamental privacy concerns highlighted in *Schrems I*.⁵⁵⁶ These events led to a second judgment in

⁵⁵³ European Commission, 'Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce.'

⁵⁵⁴ Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily (The Guardian, 6 June 2013)' <<https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>> accessed 1 September 2024.

⁵⁵⁵ *Case C-362/14 Schrems v Data Protection Commissioner ("Schrems I")* [2015] EU:C:2015:650 (n 214).

⁵⁵⁶ Costello, Róisín Áine, 'Schrems II: Everything Is Illuminated' (2020) 5 *European Papers* 1045, 1046–1047.

Schrems II,⁵⁵⁷ once more invalidating the adequacy decision of the European Commission.

A crucial aspect of the judgment was the CJEU's interpretation of the meaning of 'adequate level of protection' for data transfers as one 'essentially equivalent' to EU standards. As the Court found in *Schrems I*:

[T]he term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union.⁵⁵⁸

In both cases the court ruled that this high bar must be measured against the EU's Charter of Fundamental Rights rather than member state law⁵⁵⁹.

In its rulings the CJEU did establish guidelines for interpreting 'essential equivalence'. These criteria emphasise maintaining a high level of fundamental rights protection,⁵⁶⁰ ensuring effective practical implementation,⁵⁶¹ considering domestic laws and international commitments,⁵⁶² and implementing reliable self-certification systems.⁵⁶³ The CJEU stressed the importance of detailed explanations in adequacy decisions,⁵⁶⁴ prohibiting primacy of third-country law over EU law in

⁵⁵⁷ Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ('*Schrems II*') [2020] EU:C:2020:559 (n 214).

⁵⁵⁸ *Schrems I* at [73] (emphasis added).

⁵⁵⁹ *ibid.* [73]-[74] and [78]; *Schrems II* [99]-[100].

⁵⁶⁰ *Schrems I* [38]-[39] and [73].

⁵⁶¹ *ibid.* [75]-[77].

⁵⁶² *ibid.* at [71].

⁵⁶³ *ibid.* at [81].

⁵⁶⁴ *ibid.* at [83].

certain areas.⁵⁶⁵ It also mandated limitations on public authorities' power to interfere with fundamental rights, particularly regarding data access for national security purposes.⁵⁶⁶ The Court emphasised the need for clear, precise rules to prevent data abuse and specified that data storage and use by third countries must be strictly limited, differentiated, and justified based on specific, restricted objectives⁵⁶⁷.

The *Schrems* judgments expose inherent contradictions in EU data transfer regulation. They highlight the gap between the EU's aspirations for global data protection and the practical limitations of its regulatory approach. Kuner argues that this situation has created a dichotomy between reality and illusion in EU data protection law. While the law maintains the illusion of providing seamless, effective protection for data transferred globally, in reality, it struggles to provide practical, enforceable protections, especially against actions by foreign intelligence agencies.⁵⁶⁸

To address these challenges, Kuner advocates a shift from bureaucratic, paper-based compliance to mechanisms that provide actual protection in practice. This includes increased enforcement and transparency, particularly regarding intelligence-gathering practices. Kuner also emphasises the need to move beyond formalistic measures and to seek accommodation between different legal systems for privacy and data protection.⁵⁶⁹

⁵⁶⁵ *ibid.* [85]-[87].

⁵⁶⁶ *ibid.* at [88].

⁵⁶⁷ *ibid.* at [93].

⁵⁶⁸ Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post *Schrems*' (2017) 18 *German Law Journal* 881.

⁵⁶⁹ *ibid.*

However, the issue of evaluating regimes is not limited to the European Commission and Supervisory Authorities. Indeed, following *Schrems II* the European Commission issued a new set of Standard Contractual Clauses in June 2021.⁵⁷⁰ These require controllers to recognise and address any breaches of the ‘essence’ of EU fundamental rights.⁵⁷¹ As such controllers must now carry out even more analysis with a greater degree of sophistication. These expanded obligations place even more importance on identifying and understanding the accountability roles of the EU Data Protection Regime.

4. Conclusion

We have noted a marked evolution in Data Protection Law both through legislative initiatives and judicial interpretation. The EU's data protection framework of the 2020s represents a marked departure from its predecessors, characterised by increased scope and depth that goes well beyond the requirements established by the 1995 Data Protection Directive.

We began our analysis by illustrating the concentric circles of EU data protection legislation, with the GDPR at its core. Surrounding the GDPR are complementary legal instruments such as the Law Enforcement Directive, and the ePrivacy Directive. The outer circle encompasses newer digital legislation, including the

⁵⁷⁰ Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council [2021] OJ L 199/31. See in particular Par. 19 and Clause 14(a). The latter of which requires the parties to warrant that the ‘laws and practices’ of a country outside of the EEA where personal data is transferred ‘respect the **essence** of the fundamental rights and freedoms.’ (emphasis added)

⁵⁷¹ González Fuster (n 46) 5–6. See also Laura Drechsler and Irene Kamara, ‘Essential Equivalence as a Benchmark for International Data Transfers After Schrems II’, in Eleni Kosta, Ronald Leenes, and Irene Kamara (eds.), *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022) 17–18.

Digital Services Act, the Digital Markets Act, and the AI Act. This layered approach demonstrates the EU's comprehensive strategy to regulate the digital sphere, addressing various aspects of data processing, online services, and emerging technologies.

A key theme emerging from this analysis is the creation of 'complementing and competing' obligations and enforcement mechanisms across these various legislative instruments. We have provided examples of how these laws interact, such as the overlapping obligations for cookie usage under both the ePrivacy Directive and the GDPR. Similarly, the processing of personal data within AI services will be subject to both the GDPR and the AI Act, creating a complex regulatory landscape for businesses to navigate.

More significantly we have seen the divergence of accountability models employed by these laws. This diversity challenges the notion that the controller-based model of the GDPR is the only approach to safeguarding digital rights. Instead, it suggests that different regulatory frameworks may be appropriate for addressing various aspects of data protection and digital regulation.

Our second significant focus was upon the judicial expansion of the data protection regime. The CJEU has played a crucial role in broadening the scope of data protection law through its interpretations of key concepts. The expansive definition of 'personal data' has been particularly influential, with the court adopting a broad interpretation that encompasses a wide range of information relating to individuals. This judicial expansion has led to data protection becoming an almost ubiquitous legal framework, applicable to an ever-increasing range of

activities in our digitalized society. Per Purtova, data protection may be seen as the 'law of everything'.⁵⁷²

What is more, this judicial expansion translates to an increased standard for international data transfers, particularly in light of the *Schrems I* and *Schrems II* judgments. These cases expose inherent contradictions in EU data transfer regulation and highlight the gap between the EU's aspirations for global data protection and the practical limitations of its regulatory approach. The CJEU's interpretation of 'essential equivalence' as the standard for adequate protection in third countries has set a high bar for international data transfers, creating significant challenges for businesses operating globally.

What is more, the responsibility for assessing data protection regimes extends beyond the purview of the European Commission and Supervisory Authorities, encompassing a broader range of stakeholders. In the aftermath of *Schrems II*, the European Commission issued revised SCCs in June 2021, expanding the scope of evaluation beyond the Commission and Supervisory Authorities. These new SCCs mandate that controllers identify and address any infringements on the 'essence' of EU fundamental rights in third-country data transfers. This new obligation upon controllers demands an unprecedented level of expertise. As such the delineation of the role of controller has become even more important and more burdensome. This development underscores the increasing importance of understanding and delineating accountability roles within the EU Data Protection Regime. In Part II of this thesis we will review the challenges posed in applying this fundamental model.

⁵⁷² Purtova (n 31).

PART II: THE PROBLEM OF CONTROL

Chapter Six: The Problem of Control - History and Case Law

1. Introduction

As has been established in Chapter Three,⁵⁷³ the Individual Control Model underpins the contemporary EU Data Protection Regime.⁵⁷⁴ The GDPR intricately links the concept of ‘protection’ with that of ‘control’.⁵⁷⁵ However, the Regulation's approach incorporates diverse regulatory mechanisms to legitimise data processing. This multifaceted strategy results in a legal framework that balances individual control with elements of societal and regulatory protection.⁵⁷⁶ In order to achieve this goal, the GDPR relies upon a robust accountability system. Data subjects exercise control over their personal data by invoking rights against controllers, a relationship that forms the cornerstone of the European Data Protection Regime. However, the efficacy of this system hinges on a clear delineation of the controller's role.

Similarly, independent Supervisory Authorities, responsible for overseeing data protection law application and enforcement, exercise their powers based on the level of responsibility assigned to actors, particularly controllers. Their ability to function effectively depends on a precise understanding of controllership in various data processing scenarios. It thus follows that ambiguity in defining the controller's role has significant implications for both individual autonomy and

⁵⁷³ See [Chapter Three, Section 3.3 Defining the GDPR](#).

⁵⁷⁴ See [Chapter Three, Section 3.1 The Individual Control Model](#).

⁵⁷⁵ See Chapter Two, [Section 4.1 Privacy's Conceptual Disarray](#) and [Section 4.2 Data Protection and Informational Self-Determination](#).

⁵⁷⁶ See [Chapter Three, Section 3.2 The Societal Protection Model](#).

regulatory oversight effectiveness. When controllership boundaries are unclear, data subjects face uncertainty in directing their requests and complaints, impeding their ability to exercise rights and maintain control over personal information. This lack of clarity creates a substantial barrier to individual empowerment and regulatory oversight.

Moreover, In Chapter Five we illustrated the expansion of the EU Data Protection Regime through both legislative action and judicial interpretation. The latter has radically impacted the meaning and function of Data Protection Law's accountability model. As such, mapping these relationships and the parties within them has become an increasingly important task. However, the increasing intricacy of data flows involving multiple actors has obscured the distinction between controllers and processors, complicating individuals' efforts to exercise autonomy over their personal information. Parties throughout the data processing chain are impacted by the intricacy of these processes. In the first instance, data subjects lose autonomy as they are caught within a complex web of processing operations. At the same time, unanticipated burdens are placed upon users of technology who may unknowingly hold the role of controller under the GDPR. As a result, legal certainty is undermined as parties within a data processing relationship cannot be easily identified.

In this chapter, we will examine how this challenge has emerged. The first section summarises the historic model upon which Data Protection Law is based. The next outlines the challenges to this model which have emerged from the mid-1990s onwards. These challenges have been further complicated by recent rulings of the CJEU. We will explore the uncertain nature of control in data processing relationships with a specific focus upon the CJEU rulings in *Wirtschaftsakademie*, *Jehovan todistajat*, *Fashion ID*, *NVSC*, *Belgian State*, and most recently *IAB Europe*. Thereafter, we will analyse the impacts of the CJEU's stance on the controller-

based responsibility model. These consequences will be further explored in the chapters which follow.

2. Controller Based Accountability: Historical Origins

Early data protection laws were developed to address the apprehensions which accompanied the rise of automated data processing. As such regulators tailored their responses to the actors within these systems. At this stage the common use of databanks involved a government department instructing a database administrator on the collection and use of personal data, as is represented in *Figure 10* below. It is noteworthy that even the term databank feels anachronistic having fallen out of use.



Figure 10. Classic Model of Data Processing in 1970s

Early legislation was modelled on this arrangement. For instance, the world's first data protection law, the Hessian Data Protection Act of 1970 mandates that those charged with the 'handling' of 'personal data' are only permitted to disclose it when this is clearly allowed by the law or is authorised by 'those entitled to exercise control' (*'derjenigen die verfügbungsberechtigt sind'*).⁵⁷⁷ The category of handlers of personal data corresponds to the 'database administrator' of *Figure 10*, while 'those entitled to exercise control' refers to the 'government actor'. Similarly,

⁵⁷⁷ Hessian Data Protection Act, Section 3(1).

in the first national data protection law, the Swedish Data Act of 1973, it is the ‘responsible keeper of a register’ (*‘registeransvarig’*) who holds decision making power.

Similarly, the French Law on Informatics, Files and Liberties (*‘LIFL’*) of 1978 utilises a variety of terms to refer to these two different actors.⁵⁷⁸

- Parties ‘on whose behalf’ (*‘pour le compte de’*) personal data processing is carried out.⁵⁷⁹
- The party ‘who has the power to decide whether personal data shall be processed’ (*‘celle qui a pouvoir de décider la création du traitement’*).⁵⁸⁰
- The ‘holders’ or ‘users’ (*‘les détenteurs ou utilisateurs’*) of the personal data.⁵⁸¹
- ‘Entities charged with performing the processing’ (*‘organismes chargées de mettre en œuvre le traitement’*).⁵⁸²
- The party ‘responsible for the file’ (*le responsable du fichier*).⁵⁸³
- The party ‘holding the file’ (*l’organisme qui le tient*).⁵⁸⁴

It is within the OECD Guidelines of 1980 that the key roles of data subject and controller are first established. The simple application of the OECD Guidelines to the classic model of data processing from the 1970s and 1980s is shown in *Figure 11* below.

⁵⁷⁸ All terms identified by van Alsenoy (n 127).

⁵⁷⁹ LIFL, Articles 15–16.

⁵⁸⁰ *ibid.* Article 19.

⁵⁸¹ *ibid.* Article 21.

⁵⁸² *ibid.* Article 34.

⁵⁸³ *ibid.* Article 35.

⁵⁸⁴ *ibid.* Article 37.



Figure 11. Classic Model of Data Processing and Roles

The term ‘data controller’ is defined in Paragraph 1(a) of the OECD Guidelines as:

[A] party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.⁵⁸⁵

The Explanatory Memorandum to the OECD Guidelines clarifies that the role of data controller ‘is of vital importance’ as it is this party which should ‘carry ultimate responsibility for activities concerned with the processing of personal data.’ This definition supplies several key elements essential to the role of ‘data controller’.⁵⁸⁶

Party – The Explanatory Memorandum specifies that a data controller can be ‘a legal or natural person, public authority, agency or any other body.’⁵⁸⁷ A definition which matches that of the GDPR.⁵⁸⁸

⁵⁸⁵ Emphasis added.

⁵⁸⁶ Paragraph 40.

⁵⁸⁷ Paragraph 40.

⁵⁸⁸ See Article 4(7) of the GDPR as is explored in [Chapter Four, Section 3. Actors and Accountability](#).

Decision Making Power – A defining element for a data controller is that this entity is ‘competent to decide’ the ‘contents and use’ of the data processing in question. This amounts to decision making power. The Explanatory Memorandum places the decision-making power of the data controller in the context of ‘data and data processing activities.’⁵⁸⁹ Elsewhere it is explained that it is the data controller that decides ‘what activities should be carried out and for what purposes’ and ‘what data should be stored, who should be able to use them.’⁵⁹⁰ This is equivalent to the definition of controller under the GDPR as the party which ‘determines the purposes and means of the processing of personal data.’⁵⁹¹

Benefit – Beyond decision making power over the ‘contents and use’ of personal data, the data controller of the OECD Guidelines is the party for whose ‘benefit’ the processing of data is carried out.⁵⁹²

The rationale for the data controller holding primary responsibility is elucidated in the Explanatory Memorandum:

The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly, it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because

⁵⁸⁹ Paragraph 62.

⁵⁹⁰ Paragraph 40.

⁵⁹¹ GDPR, Article 4(7).

⁵⁹² Explanatory Memorandum Paragraph 62.

the processing of data is carried out on his behalf by another party, such as a service bureau.⁵⁹³

A natural equation of power and benefit leading to obligation is laid out in this explanation. As it is the data controller who both 'decides' and 'benefits' from data processing, it stands to reason that this party must also carry the onus for ensuring that the processing is carried out within the confines of the law.⁵⁹⁴

The constitutive elements of (i) decision making authority over (ii) the contents and use of data and (iii) benefit from the data processing were changed in Convention 108. The primary accountable actor under Convention 108 is the 'controller of the file'.⁵⁹⁵ This actor bears close resemblance to the data controller in the OECD Guidelines. As in the case of the data controller, the controller of the file can be any 'natural or legal person, public authority, agency or any other body.' As in the case of the OECD Guidelines, a defining element for the controller of the file is that this entity is 'competent to decide' the components of the automated data processing.⁵⁹⁶

The decision-making power that is to be exercised consists of three elements (i) 'the purpose of the automated data file', (ii) 'the categories of personal data' to be stored, and (iii) the nature of the operations applied to this data. A significant

⁵⁹³ Paragraph 62.

⁵⁹⁴ Joseph Alhadeff, Brendan Van Alsenoy and Jos Dumortier, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions', in: *D. Guagnin, L. Hempel, C. Ilten a.o. (eds.), Managing Privacy through Accountability* (Palgrave Macmillan 2012).

⁵⁹⁵ *ibid.* Article 2(d).

⁵⁹⁶ As the OECD Guidelines also refer to manual processing of personal information, the two actors differ in that the OECD's category of data controller is applicable regardless of whether the processing of personal information takes place through automated or non-automated means. In contrast the controller of a file under Convention 108 is only applicable in the case of automated data processing.

contrast to the OECD's data controller is that Convention 108's controller of the file is not required to benefit from the data processing.

The GDPR's predecessor, the 1995 Directive follows on from the OECD Guidelines and Convention 108 by placing the onus of responsibility on the data controller:

'[C]ontroller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.⁵⁹⁷

Elements well established in both the OECD Guidelines and Convention 108 are clear at this stage. The description of the controller as a 'natural or legal person, public authority, agency or any other body' is identical to the language found in the earlier instruments. Moreover, the controller is defined by their decision-making power in determining 'the purposes and means' of processing personal data. It is noteworthy that the Directive breaks with the OECD Guidelines, and instead follows Convention 108, by removing the criteria of benefit from the elements required for a data controller. This stance has been maintained under the GDPR.

A key innovation within this definition is the possibility of multiple actors being able to share the role of data controller. In its Opinion on the final draft of the 1995 Directive, the European Commission explains that the phrasing in this definition allows for the scenario in which 'a number of parties may jointly determine the purpose and means of the processing' in a single data processing operation. In

⁵⁹⁷ *ibid.* Article 2(d). Emphasis added.

such a case it follows that each of the ‘co-controllers must be considered as being constrained by the obligations imposed by the directive.’⁵⁹⁸

The Explanatory Memorandum accompanying the 1995 Directive provides the reasoning behind this change.

In practice it may occur, however, that several different persons decide to process personal data for a particular purpose or in the context of permanent relationship (e.g., within a collaboration framework or a professional association) and provide themselves with the necessary technical means to do so. In such a case, each of these persons, as soon as they do not operate as part of the same legal entity, shall be considered a joint controller. This situation may occur more and more in the future, for example in case of an exchange of data between governments or between companies in the context of telematics networks.⁵⁹⁹

The concept of joint controller was ultimately given a clear articulation in Article 26 of the GDPR as was explored in Chapter Four.⁶⁰⁰

3. Advancing Models and Challenges to Controllership

Already in the mid-1990s, Helen Nissenbaum identified the growing difficulty of assigning accountability in computing technologies. Her primary concern

⁵⁹⁸ Commission of the European Communities, ‘Opinion of the Commission Pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament’s Amendments to the Council’s Common Position Regarding the Proposal for a European Parliament and Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM (95) 375 Final- COD287, 18 July 1995.’ 3.

⁵⁹⁹ Commission of the European Communities, ‘Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM (92) 422 Final – SYN 287, 15 October 1992, OJ 27 November 1992, C 311/30-61’ (m).

⁶⁰⁰ See [Chapter Four, Section 3. Actors and Accountability.](#)

stemmed from the 'many hands problem,' a concept describing the diffusion of moral and operational responsibility in complex multi-agent systems. This phenomenon significantly complicates the assignment of accountability for collective outcomes. The 'many hands problem' presents a formidable challenge to governance structures, as it blurs the lines of responsibility and frequently hinders the effective resolution of systemic issues.⁶⁰¹

The field of computing is highly susceptible to the 'many hands problem'. Even in the 1990s computer systems were typically non-monolithic and constructed from various modules or segments, each potentially created by a different team of individuals. Many of these systems incorporate code from earlier versions or different networks, sometimes from entirely different creators. Furthermore, as networks expand and become increasingly complex, it is possible that no single individual comprehends the entire system or can account for all contributors to its various components.⁶⁰²

The reality has only become more complicated since Nissenbaum penned her critique in the mid-1990s. Contemporary computing systems are progressively characterised by (i) modularity, (ii) a reliance upon cloud-based architecture, and (iii) deepening interconnectivity. What is more, the emergence of 'agile' methodologies in recent decades has instigated a series of critical transformations within the realms of software creation, distribution, and infrastructural management. These methodologies have significant additional implications on the structuring of business organisations and the distribution of computational resources.⁶⁰³ The agile development process is now characterised by short iterative

⁶⁰¹ Helen Nissenbaum, 'Accountability in a Computerized Society' (1996) 2 *Science and Engineering Ethics* 25.

⁶⁰² *ibid.* 26-28

⁶⁰³ Jennifer Cobbe, Chris Norval and Jatinder Singh, 'What Lies beneath: Transparency in Online Service Supply Chains' (2020) 5 *Journal of Cyber Policy* 65.

cycles. These cycles are marked by continuous testing and revisions, accompanied by the commitment to iterative improvements post-deployment. Software is typically modularised and dispensed as a service. Resources have been made more adaptable with software progressively migrating towards cloud-based solutions.⁶⁰⁴ The process of contemporary software development often involves the incorporation of pre-existing modular components. These components are typically provided as services and are managed by external entities. The final product, therefore, is not simply a single system, instead it is an intricate amalgamation of multiple systems functioning collaboratively.⁶⁰⁵

Consequently, digital technologies are now centred on increasingly complex data supply chains. Within these supply chains, data is transmitted among numerous stakeholders, connecting systems that are designed, established, managed, and governed by various individuals and organisations, and these systems are often presented in the form of a single end service. Each of these entities maintains control solely over the specific subsystems they furnish as services to other parties. As such, applying the classic model of data processing roles becomes increasingly difficult. It is thus necessary to understand the threshold for control envisioned by this model.

4. Complete and Effective Protection

As has been discussed in Chapter Four, the GDPR outlines the core legal principles which must be adhered to for all processing of personal data.⁶⁰⁶ The last of these principles, Accountability, has been bolstered in comparison to the corresponding

⁶⁰⁴ Jennifer Cobbe, Michael Veale and Jatinder Singh, 'Understanding Accountability in Algorithmic Supply Chains' (SocArXiv 2023) <<https://osf.io/p4sey>> accessed 10 March 2024.

⁶⁰⁵ *ibid.*

⁶⁰⁶ GDPR, Article 5. See [Chapter Four, Section 7. Data Protection Principles](#).

provision of the 1995 Directive.⁶⁰⁷ The 1995 Directive had placed the onus on the controller to 'to ensure' compliance with the data protection principles. Under the GDPR a new requirement to 'demonstrate compliance' with the obligations of the Regulation is now placed upon the controller. While the processor also holds obligations, these are far less onerous.⁶⁰⁸ Additionally, even where these duties are imposed upon the processor, they are complemented by corresponding responsibilities levied on the controller at the same time.⁶⁰⁹ Thus, in order to facilitate stronger protection of individuals the CJEU has expanded its reading of the role of controller.

The CJEU's ruling in *Google Spain* can be seen as establishing the basis for this new comprehensive approach to data protection. While primarily known for establishing a 'right to be forgotten' in EU law, the decision's classification of Google's search engine as a data controller was equally significant.⁶¹⁰ This ruling diverged from the earlier opinion of the Article 29 Working Party, which had suggested that search engines acting purely as intermediaries should not be considered principal controllers of content, based on the principle of proportionality.⁶¹¹

⁶⁰⁷ Data Protection Directive, Article 6(2).

⁶⁰⁸ See Macmillan (n 323). See also Mike Hintze, 'Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR' (2018) 22 *Journal of Internet Law* 17. See also, Louisa Specht-Riemenschneider and Ruben Schneider, 'Stuck Half Way: The Limitation of Joint Control after Fashion ID (C-40/17) : Case Note – Fashion ID (C-40/17)' (*GRUR international*, 2020).

⁶⁰⁹ Wong (n 11) 376.

⁶¹⁰ Lynskey, 'Complete and Effective Data Protection' (n 32) 309.

⁶¹¹ Article 29 Working Party, 'Opinion 1/2008 on Data Protection Issues Related to Search Engines. Adopted 4 April 2008' (2008) 14 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf> accessed 13 March 2024.

The Court implicitly rejected comparisons with legal domains where intermediaries like Google Search enjoy relative immunity from liability for hosting illegal content until they become aware of it. Despite Google's argument that it did not distinguish between links containing personal data and those that did not, the Court applied a broad interpretation of the controllership test.⁶¹² It determined that in the context of linking activities, search engine operators define the purposes and means of personal data processing.⁶¹³ What is more, the Court asserted that excluding search engine operators from the definition of data controller would contradict both the literal wording and the intended objective of the law. It emphasised that search engines play a role that is distinct from that of primary publishers and can have a more significant impact on fundamental rights to privacy and data protection. Crucially, the Court viewed the broad definition of data controller as essential for ensuring 'effective and complete protection of data subjects.'⁶¹⁴

This emphasis upon 'effective and complete' protection has led to a transformation in the CJEU's approach to controllership. In a series of judgments in *Wirtschaftsakademie*, *Jehovan todistajat*, *Fashion ID*, *NVSC*, *Belgian State*, and *IAB Europe*, the court has established that only a low level of decision-making power is needed to designate an entity as a controller or joint controller.⁶¹⁵ Each of these cases is examined in the following sections.

⁶¹² *Google Spain* at [22].

⁶¹³ *ibid.* at [33].

⁶¹⁴ *ibid.* at [34].

⁶¹⁵ While the first three of these judgments were made under the 1995 Data Protection Directive, they remain valid. European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339) 18.

5. CJEU Decision in *Wirtschaftsakademie*

The principle that only a low level of decision-making power is needed to designate an entity as a controller was established by the CJEU in its ruling in *Wirtschaftsakademie*.

In this case, the educational *Wirtschaftsakademie* facility operated a ‘fan page’⁶¹⁶ hosted on Facebook. A component of Facebook’s non-negotiable conditions for such pages at the time allowed the administrator of the page to obtain statistical information on its visitors through the ‘Facebook Insights’ service. In order to do so personal data was collected through cookies placed on users’ devices by Facebook.⁶¹⁷ As has been explained above,⁶¹⁸ a browser cookie is a small piece of data sent from a website and stored on a user’s computer. Importantly, cookies are not isolated mechanisms but are often associated with identifiable personal details which users provide to use a platform or service. This linkage allows the entity responsible for setting the cookie to retain a consumer’s information. This may allow a website to ‘remember’ user actions or preferences over a period of time by linking individuals to devices even if the user deletes the cookie.⁶¹⁹ In the case of Facebook, aggregation of these browsing activities over time enables trackers to

⁶¹⁶ More commonly referred to as a Facebook ‘page’, a ‘fan page’ is a business account representing a company or organisation.

⁶¹⁷ Charlotte Ducuing, Jessica Schroers and Els Kindt, ‘The *Wirtschaftsakademie* Fan Page Decision: A Landmark on Joint Controllership - A Challenge for Supervisory Authorities Competences Case Notes’ (2018) 4 *European Data Protection Law Review* (EDPL) 547, 547. See also Orla Lynskey, ‘Another Turn of the Screw? The “Facebook Fanpages” Judgment’ (*European Law Blog*, 25 June 2018) <<https://europeanlawblog.eu/2018/06/25/another-turn-of-the-screw-the-facebook-fanpages-judgment/>> accessed 23 March 2024. See also Lorna Woods, ‘EU Law Analysis: Facebook Fan Pages and EU Data Protection Law: The Implications of *Unabhängiges Landeszentrum Für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*’ (*EU Law Analysis*, 3 July 2018) <<https://eulawanalysis.blogspot.com/2018/07/facebook-fan-pages-and-eu-data.html>> accessed 23 March 2024.

⁶¹⁸ See [Chapter Five, Section 2.7 Legislative Expansion: Conclusion](#).

⁶¹⁹ Costello, ‘Impacts of AdTech on Privacy Rights and the Rule of Law’ (n 461) 11.

construct detailed profiles which are leveraged for online behavioural advertising.⁶²⁰

However, neither *Wirtschaftsakademie* nor Facebook had informed visitors of this data collection. As such, the Supervisory Authority for Schleswig-Holstein, ('ULD') ordered *Wirtschaftsakademie* to deactivate these pages. *Wirtschaftsakademie* challenged this finding arguing that it was not responsible for the data processing conducted by Facebook. The dispute ultimately arrived at the German Federal Administrative Court which referred the question of whether *Wirtschaftsakademie* could be held responsible together with Facebook for this breach of Data Protection Law to the CJEU.⁶²¹

The CJEU concluded that operators of a Facebook fan page were indeed joint controllers together with Facebook. This position stemmed from the fact that fan page administrators 'exerted influence' over Facebook's collection of data from visitors of the fan page. As the Court observed:

The administrator [of a page] may, with the help of filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook. Consequently, the administrator of a fan page hosted on Facebook contributes to the processing of the personal data of visitors to its page.⁶²²

Thus, the Court concluded that the administrator of Facebook pages 'must be regarded as taking part...in the determination of the purposes and means of

⁶²⁰ Shradha Jain and HC Purohit, 'Consumer Acceptance of Online Behavioural Advertising: Role of Persuasion Knowledge and Protection Motivation.' (2022) 18 48.

⁶²¹ *Wirtschaftsakademie* at [24].

⁶²² *ibid* at [36].

processing the personal data of the visitors to its fan page'⁶²³ and as such must be considered a joint controller.

The Court additionally drew attention to the fact that fan pages hosted on Facebook could also be visited by individuals who are not Facebook users. Accessing a fan page, even without a user account, results in the processing of personal data by Facebook. In these cases, the Court viewed the fan page administrator as holding even greater responsibility as 'the mere consultation of the home page by visitors automatically starts the processing of their personal data.'⁶²⁴

What is more, the Court ruled that joint controllership does not require the parties involved to each have access to the data concerned.⁶²⁵ Finally, the Court drew a distinction between joint *controllership* and joint *responsibility*:

The existence of joint responsibility does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case (or Member State law).⁶²⁶

These conclusions have been reinforced by the CJEU in its rulings since *Wirtschaftsakademie*.

⁶²³ *ibid.* at [39].

⁶²⁴ *ibid.* at [41].

⁶²⁵ *ibid.* at [38].

⁶²⁶ *ibid.* at [43].

6. CJEU Decision in *Jehovan todistajat*

The low threshold for joint controllership was reaffirmed by the CJEU in *Jehovan todistajat*. Here, the Court examined whether the Jehovah's Witnesses community in Finland was itself a joint controller together with individual members conducting door-to-door preaching. These members would take physical notes of their interactions with households, including names, addresses, religious beliefs, and family circumstances. The data subjects about whom this information was collected, had neither been informed nor consented to this processing.⁶²⁷ Importantly, the Jehovah's Witness Community did not have access to these notes themselves.⁶²⁸

Among the issues in dispute was whether the notes taken by door-to-door preachers fell within the scope of the GDPR. As has been discussed in Chapter Four,⁶²⁹ the GDPR applies to both automated processing as well as manual processing if the data 'form part of a filing system or are intended to form part of a filing system.' On this matter, the Court ruled that the concept of a filing system 'covers a set of personal data collected in the course of door-to-door preaching' as long as the data is kept in a manner which 'in practice, enable them to be easily retrieved for subsequent use'. The Court found that it is not necessary for the 'filing system' to 'include data sheets, specific lists, or other search methods.'⁶³⁰

On the question of whether the Jehovah's Witnesses community itself was a joint controller in this data processing, the Court found that it was sufficient that the

⁶²⁷ *Jehovan todistajat* at [15].

⁶²⁸ *ibid* at [23].

⁶²⁹ See [Chapter Four, Section 4.1 Material Scope](#).

⁶³⁰ *Jehovan todistajat* at [58].

preaching activity had taken place to achieve the aims of the community.⁶³¹ The CJEU noted that the preaching had been ‘organised, coordinated and encouraged’ by the Jehovah’s Witness Community.⁶³² As such, the Court maintained that the Community’s status as a joint controller was correct even though it did not have ‘access’ to the data being processed.⁶³³

Notably, the Court understood that the criteria of ‘determining the means and purposes of processing’ used to define the role of controller should not be conflated with written instruction. Rather any ‘natural or legal person’ will be a controller whenever it ‘exerts influence’ over the means and purposes for which personal data is processed.⁶³⁴

In its judgment, the Court also reiterated the principle established in *Wirtschaftsakademie* that joint controllership does not equate to equal responsibility and liability. The language employed is identical to that found in the *Wirtschaftsakademie* ruling.⁶³⁵

In *Jehovan todistajat* we may distinguish between two components of processing. The first (i) is the overarching purpose of data processing—in this instance, to recruit new community members—which was determined by the religious community. The second (ii) is the more specific elements of processing, such as

⁶³¹ Susanna Lindroos-Hovinneimo, ‘Who Controls Our Data? The Legal Reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojavaltuutettu v Jehovan Todistajat*’ 28 *Information & Communications Technology Law* 225.

⁶³² *Jehovan todistajat* at [76].

⁶³³ *ibid.* at [75]

⁶³⁴ *ibid.* at [67]-[68].

⁶³⁵ *Ibid.* at [66].

data selection and access permissions, which were decided by individual preaching members.

The Court deemed the community's orchestrating role sufficient to establish responsibility under data protection law, despite the community lacking direct access to the data or failing to produce written guidelines for data processing. This decision appears logical, given that the preaching activities were conducted in pursuit of the community's fundamental objective of propagating its faith. The community, in essence, acted as the 'intellectual lead' in the data processing activities.⁶³⁶

Thus, in *Jehovan todistajat* we find an 'orchestrating' interpretation of controllership where overall direction and purpose-setting can create legal responsibility, even in the absence of direct data handling or explicit procedural guidelines. Such an approach prioritises the conceptual and strategic aspects of data processing over its tactical implementation when determining legal accountability. This orchestrating approach is apparent in the subsequent cases of *NVSC* and *IAB Europe*. However, the Court's rulings in *Wirtschaftsakademie*, *Fashion ID*, and *Belgian State* show a completely different thrust to joint controllership.

7. CJEU Decision in *Fashion ID*

In *Fashion ID*, the Court expanded upon the principles established in its decision in *Wirtschaftsakademie*. The German online clothing retailer, Fashion ID, had embedded a Facebook 'Like' button on their website to support social media engagement and marketing of their business. This standard social media plug-in placed cookies on the devices of website visitors, transferring information,

⁶³⁶ Lynskey, 'Complete and Effective Data Protection' (n 32) 313.

including IP addresses, to Facebook. This was the case even when the visitor did not have a Facebook account and did not even click on the embedded 'Like' button.⁶³⁷

As in the case of *Wirtschaftsakademie*, no information was relayed to the website user about this use of personal data. In response, Verbraucherzentrale NRW, a German consumer protection group, sought an injunction against Fashion ID in the District Court of Germany. In its defence, Fashion ID claimed to have had no knowledge of the data processing being carried out by Facebook. Additionally, Fashion ID highlighted the fact that it did not have access to the data which Facebook was processing.

The District Court found in favour of Verbraucherzentrale NRW, and imposed a EUR 250 000 fine on Fashion ID. This decision was appealed to the Higher Regional Court which referred the issue to the CJEU.

In its decision the CJEU reiterated its position in *Google Spain* and *Wirtschaftsakademie*, that the purpose of interpreting the concept of controller broadly is to ensure 'effective and complete protection of data subjects.'⁶³⁸ In addressing Fashion ID's claim that it did not have access to the personal data processed by Facebook, the Court restated the principle found in *Wirtschaftsakademie* and *Jehovan todistajat* that 'the joint responsibility of several

⁶³⁷ See Jure Globocnik, 'On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID: Directive 95/46/EC, Arts. 2(d) and (h), 7(a) and (f), 10.' (2019) 50 IIC - International Review of Intellectual Property & Competition Law 1033. And Monika Zalnieriute and Genna Churches, 'When a "Like" Is Not a "Like": A New Fragmented Approach to Data Controllership' (2020) 83 Modern Law Review 861, 861.

⁶³⁸ *Fashion ID* at [66], *Google Spain* at [34], and *Wirtschaftsakademie* at [28].

actors' for processing 'does not require each of them to have access to the personal data concerned.'⁶³⁹

A key innovation of this ruling is that the Court provided a 'fragmented'⁶⁴⁰ or 'phase oriented'⁶⁴¹ approach to data processing.⁶⁴² At first repeating the understanding of *Wirtschaftsakademie* and *Jehovan todistajat* that 'joint liability does not necessarily imply equal responsibility'⁶⁴³ of all controllers. Instead, the Court explains:

On the contrary, those operators may be involved at *different stages* of that processing of personal data and to different degrees, with the result that the *level of liability* of each of them must be assessed with regard to all the relevant circumstances of the particular case.⁶⁴⁴

While this phrasing originates in *Wirtschaftsakademie* and *Jehovan todistajat*,⁶⁴⁵ the court now elaborated on the distinction between stages of processing. Going back to the definition of 'processing' under Data Protection Law⁶⁴⁶ as 'any operation or set of operations which is performed upon personal data' the court chose to emphasise that one act of processing may involve numerous operations which can

⁶³⁹ *ibid.* at [69]. Emphasis added.

⁶⁴⁰ See *Zalnieriute and Churches* (n 637) 867.

⁶⁴¹ See René Mahieu and Joris van Hoboken, 'Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?' (*European Law Blog*, 30 September 2019) <<https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/>> accessed 23 March 2024.

⁶⁴² See Wong (n 6) who prefers the term 'operation-specific' approach for the CJEU's decision in *Fashion ID*. The preference for the terms 'phase-orientated' and 'fragmented' approaches stems from the confusion that may arise from Wong's term. In reality the whole act of data transfer and absorption from Fashion ID to Facebook may be understood as a single 'operation' which has now been divided into different fragments or phases.

⁶⁴³ *Wirtschaftsakademie* at [43] and *Jehovan todistajat* at [66]. Emphasis added.

⁶⁴⁴ *Fashion ID* at [70]. Emphasis added.

⁶⁴⁵ *Wirtschaftsakademie* at [43] and *Jehovan todistajat* at [66].

⁶⁴⁶ 1995 Directive, Article 2(b); GDPR, Article 4(2).

be divided among controllers.⁶⁴⁷ As such the Court concludes that natural or legal persons ‘cannot be considered to be a controller...in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means.’⁶⁴⁸ This fragmented approach results in the breaking up of data processing into a chain of activities. In this way an entity cannot be considered a joint controller for activities which occur before or after the joint/collective event for which the parties together define the means and purpose of processing. As Zalnieriute and Churches explain:

[T]he CJEU has limited the boundaries of joint controllership by regarding two actors as joint controllers only for the stages of processing where they determine common purposes and means of processing. Therefore, joint controllership might exist for activities, such as data collection, but not for further processing, where one party might be solely responsible.⁶⁴⁹

Thus, the Court ruled that Fashion ID could be considered a joint controller for the initial data processing in the ‘collection and disclosure by transmission’ of the personal data of its website visitors to Facebook. However, Fashion ID could not be held responsible for Facebook’s own processing of the data once it had been transferred. Indeed, the CJEU deemed it ‘impossible’ to say that ‘Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook after their transmission to the latter.’⁶⁵⁰ Thus, Fashion ID was required to provide information to their website visitors relating to the transfer of personal data to Facebook, such as the identity of Facebook and the purposes for processing. It was also incumbent upon Fashion ID to justify this processing on a legal ground under Article 6 of the GDPR.

⁶⁴⁷ *Fashion ID* at [71-74].

⁶⁴⁸ *ibid.* at [74].

⁶⁴⁹ Zalnieriute and Churches (n 637) 872.

⁶⁵⁰ *Fashion ID* at [76].

A summary of the findings in *Fashion ID* may be explained and represented in these terms: Controller A captures data from data subjects for their purposes through a website. This website has a plugin which was provided by Controller B which allows for the transfer of personal data between Controller A and Controller B for the purposes of Controller B. The overlap in processing activities and accountability is illustrated in *Figures 12 and 13* below.

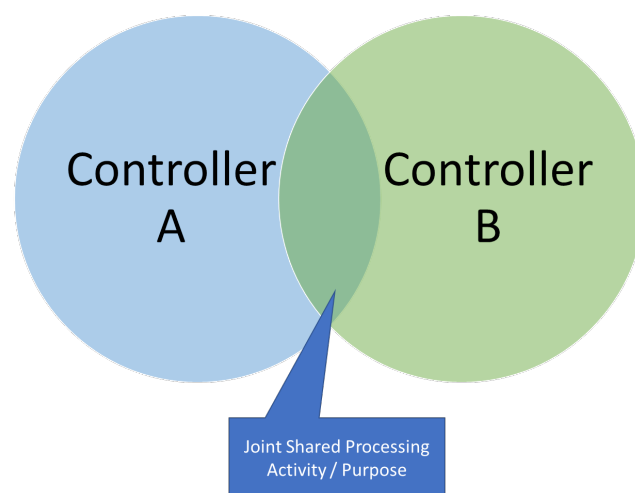


Figure 12. *Controller Relationships per Fashion ID Part 1*

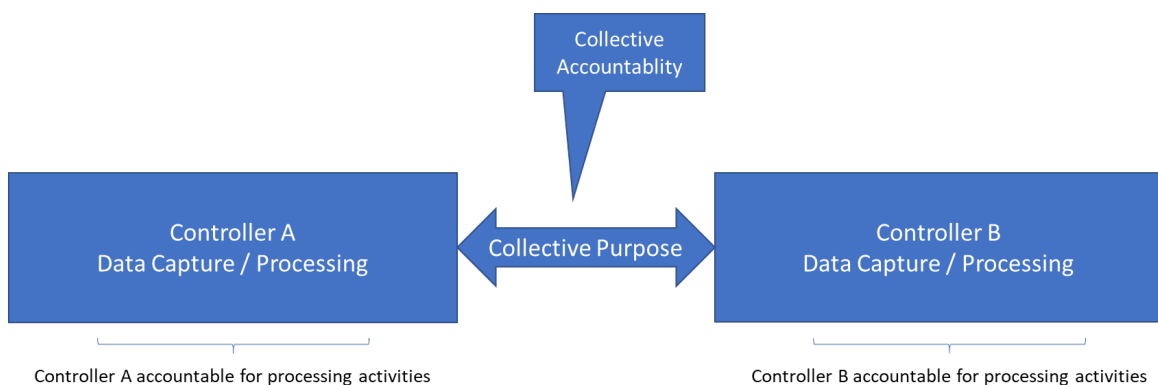


Figure 13. *Controller Relationships per Fashion ID Part 2*

The decision in *Fashion ID* is notable for its innovation in creating the idea of fragmented processing. Yet, it also seems to move against the direction of *Jehovan todistajat* where control was tied specifically to an orchestrating function. It was

this orchestrating role which was seen to be the rationale for applying the role of controller to the Jehovah's Witnesses community itself even when it did not have access to the data being processed. Yet, in *Fashion ID*, the role of the website operator is diminished to the point that it cannot be said to hold any orchestrating power. Indeed, Fashion ID seems to hold less decisive power and potentially less knowledge than the administrator of a Facebook page as in *Wirtschaftsakademie*. Rather, we see in both *Fashion ID* and *Wirtschaftsakademie* an approach of including all actors who facilitate the processing. Such a contribution surely amounts to far less than the orchestration approach of *Jehovan todistajat*.

8. CJEU Decision in NVSC

The principles established in *Wirtschaftsakademie Schleswig-Holstein*, *Jehovan todistajat*, and *Fashion ID* were once more reinforced by the CJEU in its December 2023 ruling in *NVSC*.

This case stemmed from a dispute between Lithuania's National Public Health Centre ('NVSC') and the Lithuanian Data Protection Supervisory Authority, the State Data Protection Inspectorate ('VDAI'). Amid the COVID-19 pandemic, the Lithuanian Health Minister directed the NVSC to expedite the development of an IT system to register and track data for epidemiological purposes. During this time, an individual representing the NVSC, engaged an IT company ITSS to create a relevant mobile application. This collaboration led to various exchanges on the application's design and content. As the application took shape, ITSS and the NVSC were identified as controllers within the app's privacy notice. The app was released on popular app stores and remained active for a period, during which over 3 800 individuals provided personal information while using it. Despite these developments, no formal public contract was finalised between the NVSC and ITSS for the app's official procurement. Subsequently, the NVSC distanced itself

from the app, requesting ITSS to remove any references to the NVSC within it and ultimately halted the procurement process due to funding issues.⁶⁵¹

An investigation by the VDAI revealed that personal data collection was indeed facilitated by the app. It was also discovered that a Lithuanian company managing an infectious disease IT system was set to receive this data, and that testing of the app had involved actual employee phone numbers. The VDAI subsequently fined both the NVSC and ITSS for GDPR violations, considering them joint controllers. Disagreeing with this assessment, the NVSC appealed this decision to the Regional Administrative Court of Vilnius arguing that ITSS alone should be considered the controller, while ITSS claimed it acted merely as a processor under the NVSC's direction. The Regional Administrative Court of Vilnius stayed proceedings referring a number of questions to the CJEU relating to controllership.⁶⁵²

In its ruling the CJEU clarified that an entity which has commissioned the creation of a mobile app and has influenced the decision-making regarding the processing purposes and methods used within that application must be considered a controller. This holds true even if the entity has not directly conducted any data processing activities, has not explicitly consented to certain processing activities or the public release of the app, and has not taken possession of the application itself. Furthermore, this influence can be implicit, and the entity can be deemed a controller even if it has not explicitly consented to the dissemination of the app or the resulting data processing. This interpretation stands unless the entity has

⁶⁵¹ NVSC at [12-19].

⁶⁵² *ibid.* at [20-24].

clearly opposed the release of the application and the subsequent data processing activities before the app was made publicly available.⁶⁵³

Moreover, the Court stated that the mere mention of an entity as a controller in a privacy notice or the inclusion of links in an application does not necessarily make it a controller.⁶⁵⁴ Rather the NVSC's designation as a controller was due to its participation in shaping the purposes and means of data processing through the development of a mobile app for COVID-19 data management.⁶⁵⁵

Furthermore, the Court reiterated that joint control of data does not require a formal arrangement between entities on the purposes and means of data processing. Instead, it arises from each entity independently meeting the definition of a 'controller' and their participation in the determination of the purposes and means of processing. The existence of such an arrangement is an obligation under Article 26(1) of the GDPR once the entities have been classified as joint controllers. However, not having fulfilled this obligation does not impact the classification of controllers.⁶⁵⁶

Once again, the court repeated the now well-established principle from *Wirtschaftsakademie*⁶⁵⁷ that 'the existence of joint responsibility does not necessarily imply equal responsibility'.⁶⁵⁸ To this assessment the court added the phase-oriented analysis established in *Fashion ID*⁶⁵⁹ noting that actors may be involved

⁶⁵³ *ibid.* at [38].

⁶⁵⁴ *ibid.* at [34].

⁶⁵⁵ *ibid.* at [32-33].

⁶⁵⁶ *ibid.* at [45].

⁶⁵⁷ *Wirtschaftsakademie* at [43].

⁶⁵⁸ *NVSC* at [42].

⁶⁵⁹ *Fashion ID* at [70].

‘at different stages of that processing of personal data’ each of which carries different responsibilities.⁶⁶⁰

In this ruling, the court once more reiterated its position from *Jehovan todistajat*, that the criteria for controllership is that of ‘exerting influence’ over the processing in question.⁶⁶¹ This remains true regardless of whether an entity gives explicit written instructions or is formally designated as a controller. Thus, in *NVSC*, we see a return to the orchestrating role of controllers, rather than the facilitation approach of *Wirtschaftsakademie* and *Fashion ID*.

9. CJEU Decision in *Belgian State*

The meaning of controllership has been stretched further by the CJEU in its January 2024 judgment in *Belgian State*.

On 12 February 2019, an incident involving *Moniteur belge* – Belgium’s authoritative gazette of official and public documents – led to a breach of Data Protection Law. *Moniteur belge* published an extract from a company decision regarding a capital reduction which inadvertently included personal information of a shareholder. This inclusion resulted from an error by the notary associated with one of the company’s shareholders. The document, after preparation by the notary, was sent to the relevant court and then forwarded for publication in the official gazette.

Upon discovering his personal information in the extract, the affected individual exercised his right to erasure under Article 17 of the GDPR requesting its deletion.

⁶⁶⁰ *NVSC* at [74].

⁶⁶¹ *Jehovan todistajat* at [67-68].

However, this request was denied by the Federal Public Service Justice ('FPS Justice'), to which Moniteur belge is affiliated. Following this denial, the individual filed a complaint against FPS Justice with the Data Protection Authority of Belgium ('Belgian DPA'). On 23 March 2021, the Belgian DPA ruled in favour of the individual, ordering FPS Justice to proceed with the deletion promptly. In response, the Belgian State filed an appeal with the Brussels Court of Appeal, challenging the Belgian DPA's decision.

The Brussels Court of Appeal referred two questions to the CJEU. The first (I) was whether Moniteur belge should be considered a controller as per Article 4(7) of the GDPR. The second (II) was whether Moniteur belge it should bear sole responsibility for adhering to the data processing principles outlined in the GDPR or if responsibility should also extend to other entities involved earlier in the data processing chain, which had handled the data before its publication and had made the error which led to the breach.

In its ruling the CJEU clarified that the determination of a controller can be made either explicitly or implicitly through national law.⁶⁶² In the latter case even where the designation of controllership is not made clear, it may be understood from the legal provisions that define the roles, tasks, and powers of the entities involved. In this implicit scenario, it is essential that the purposes and means of data processing, as well as the designation of the controller, are inferred with 'sufficient certainty'.⁶⁶³ In this case Belgian law had met this threshold.⁶⁶⁴

⁶⁶² *Belgian State* at [30].

⁶⁶³ *ibid.*

⁶⁶⁴ *ibid.* at [34].

Belgian State may be seen as the clearest divergence from the orchestration approach to controllership. In its ruling, the Court asserted that neither a lack of legal personality nor the inability to review personal data before publication disqualifies the *Moniteur belge* from holding the role of controller. Its primary role, as delineated by national law, is to disseminate public documents and acts as they are received, which is inherently linked to the purpose and means of data processing as defined by the GDPR.

This conclusion appears somewhat paradoxical. *Moniteur belge*'s *raison d'être* is not to exercise powers of determination. It is a simple publisher without the ability to choose, challenge or correct its content before dissemination. This is the antithesis of the criterion of 'exerting influence' over processing established in *Jehovan todistajat*.⁶⁶⁵ However, this lack of decisive power was rendered a form of determination by the Court.

The Court also discussed the possibility of joint responsibility in data processing directly. The CJEU accepted that the GDPR allows for multiple actors to be jointly responsible for the same data processing chain if joint responsibility is explicitly stated in law or inferred from legal provisions concerning the roles and data processing activities of the entities involved.⁶⁶⁶ However, in this case, the CJEU held that *Moniteur belge* was solely responsible for GDPR compliance concerning the data it processes, as Belgian law had not indicated joint responsibility with other entities.⁶⁶⁷

⁶⁶⁵ *Jehovan todistajat* at [67-68].

⁶⁶⁶ *Belgian State* at [49]-[50].

⁶⁶⁷ *ibid.* at [52].

Regarding the responsibility for compliance with GDPR principles, the Court noted that the processing done by Moniteur belge is not only subsequent but also distinct from that performed by the notary and the court registry which had made the error leading to the breach. This process involves digitisation, publication, public dissemination, and storage of data, which are tasks delegated to it by national legislation. Consequently, Moniteur belge bears the responsibility for ensuring compliance with GDPR obligations related to these data processing activities.⁶⁶⁸ This approach is consistent with the phrase orientated approach of *Fashion ID*. Even though the flaw in the data itself was inherited from actors and processing higher up in the processing-chain, Moniteur belge is held responsible for its own processing action, which takes place in a separate phase of the processing.

10. CJEU Decision in *IAB Europe*

In March of 2024, a final case with relevance to the evolving notions of control and controllership was adjudicated by the CJEU. In September 2023, the court heard arguments in *IAB Europe* with its judgment rendered on 7 March 2024.⁶⁶⁹

IAB Europe is a sectoral association for digital advertisers.⁶⁷⁰ It refers to itself as ‘the European-level association for the digital marketing and advertising ecosystem.’⁶⁷¹ The essence of the case centres on IAB’s role and responsibilities regarding data protection compliance within its Transparency and Consent Framework (‘TCF’), a system integral to the real-time bidding process in digital

⁶⁶⁸ *ibid.* at [42].

⁶⁶⁹ *Case C-604/22 IAB Europe v Gegevensbeschermingsautoriteit* [2024] EU:C:2024:214 (n 25).

⁶⁷⁰ For a larger treatment of the role of IAB Europe see Costello, ‘Impacts of AdTech on Privacy Rights and the Rule of Law’ (n 461).

⁶⁷¹ ‘IAB Europe’ (<https://iabeurope.eu/>) <<https://iabeurope.eu/>> accessed 8 March 2024.

advertising. TCF operates by encoding user preferences for advertising into a Transparency and Consent String ('TC String'), essentially a digital code. Complaints lodged with the Belgian DPA argued that the way this TC String processes user preferences fails to meet the standards set by the GDPR.

The Belgian DPA found merit in these concerns and imposed a fine of EUR 250 000 on IAB Europe. It determined that the TC String's function of recording unique expressions of consent, objections, and preferences tied to identifiable individuals, constitutes processing of personal data. This operation was deemed non-compliant with GDPR requirements, particularly as it lacked an identified lawful basis for data processing. Furthermore, the Belgian DPA designated IAB Europe as a joint controller due to its oversight and development of the TCF standard, despite the actual application of the system being carried out by its member organisations.

This led to two legal questions being referred to the CJEU for clarification. The first concerns the nature of the TC String itself—whether it should indeed be classified as personal data under GDPR. The second, directly relevant for this thesis, seeks to establish whether IAB Europe, as a standard-setting entity in the digital advertising sector, holds the position of a controller with respect to the TCF, given that its members are the ones who practically implement and use the TCF system. In rendering its judgment the Court once more reiterated that the 'objective' of 'the broad definition of the concept of controller is to ensure 'effective and complete protection of data subjects.'⁶⁷²

⁶⁷² *ibid.* at [55] and [64].

Regarding the first question, the CJEU found that a sequence of letters and symbols, like the TC String, which records a user's data processing preferences qualifies as personal data. This classification applies if it is reasonably possible to link this sequence to a specific identifier, such as the IP address of a user, thereby making the individual identifiable.⁶⁷³ This finding is consistent with *Breyer*⁶⁷⁴ where the Court had ruled that dynamic IP devices can constitute personal data. Moreover, the court held that the fact that IAB Europe could not itself combine the TC String with other identifying data like a user's IP address was irrelevant.⁶⁷⁵ This is consistent with the findings of the Court in *Jehovan todistajat*.⁶⁷⁶

Addressing the second question, the CJEU held that the purpose of creating the TCF and the TC String was 'in essence, to promote and enable the sale and purchase' of behavioural advertising.⁶⁷⁷ What is more IAB was found to determine the rule by which 'the various parties involved in the TCF may consult the preferences, objections and consents of users contained in the TC Strings.'⁶⁷⁸ As such the court ruled that IAB had met the threshold established in *Jehovan todistajat* of controllership being determined by the criterion of 'exerting influence' over processing.⁶⁷⁹

Furthermore the ruling affirmed that '[p]articipation in the determination of the purposes and means of processing can take different forms, since such

⁶⁷³ *IAB Europe* at [45]-[51].

⁶⁷⁴ *Case C-582/14 Breyer v. Bundesrepublik Deutschland* [2016] EU:C:2016:779 (n 324). See [Chapter Four, Section 2.1 Personal Data and the Data Subject](#).

⁶⁷⁵ *IAB Europe* at [46].

⁶⁷⁶ *Jehovan todistajat* at [76].

⁶⁷⁷ *IAB Europe* at [61].

⁶⁷⁸ *ibid.* at [67]

⁶⁷⁹ *ibid.* at [57] and [68].

participation can result from a common decision taken by two or more entities or from converging decisions of those entities.’⁶⁸⁰

The stage-based approach to data processing established in *Fashion ID* was once more upheld by the court. As such, IAB Europe could not be considered a joint-controller for the further processing of personal data outside of the remit of the TCF.⁶⁸¹

11. Conclusion

The cumulative impact of the cases considered in this chapter is of controllership as a nebulous legal concept. Through *Wirtschaftsakademie Schleswig-Holstein*, *Jehovan todistajat*, *Fashion ID*, *NVSC*, and *IAB Europe* the boundaries of controllership have been morphed in unprecedented ways. In three of the cases, *Jehovan todistajat*, *NVSC*, and *IAB Europe*, we see appeal to a conceptual ideal of controllership as defined through an orchestrating role in the processing of data. However, such reasoning is not possible in *Wirtschaftsakademie* and *Fashion ID*, where the actors which have been added as joint controllers render little influence over the processing in question. Going further, through *Belgian State*, controllership has been disconnected from any notion of determination or *control*.

Following *Fashion ID*, the EDPB concluded that joint controllership may arise either in the form of ‘common decision’ taken by multiple entities to process personal data, or it may result from ‘converging decisions’ by multiple parties. In the case of converging decisions, the EDPB explains:

⁶⁸⁰ *ibid.* at [59].

⁶⁸¹ *ibid.* at [73]-[77].

Decisions can be considered as converging...if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing.⁶⁸²

Advocate General Bobek noted in his advisory opinion in *Fashion ID* 'it seems that the crucial criterion after *Wirtschaftsakademie* and *Jehovan todistajat* is that the person in question 'made it possible' for personal data to be collected and transferred. As Edwards *et al* explain this means that anyone in a 'personal data chain' who makes data processing 'possible' becomes a joint controller.'⁶⁸³ Moreover, AG Bobek explains, a controller can be so classified without even having access to any 'fruits of joint labour.'⁶⁸⁴ That is to say that even if a party does not have access to any of the data processed, they may nevertheless be considered a joint controller.⁶⁸⁵

Yet in *Belgian state*, we are confronted with a controller which not only does not enjoy access to the data in question, but by virtue of its own legal mandate cannot exercise any influence over it. The hollowing out of this role would thus appear to be complete as the term controller is now devoid of functional meaning. Moreover, the controller has been severed from its legal definition as the entity which

⁶⁸² European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (2021) 18.

⁶⁸³ Lilian Edwards and others, 'Data Subjects as Data Controllers: A Fashion(Able) Concept?' (*Internet Policy Review*) <<https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400>> accessed 23 March 2024.

⁶⁸⁴ *Case C-40/17 Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* [2018] EU:C:2018:1039 *Opinion of AG Bobek. At 71.*

⁶⁸⁵ See Tobias Rothkegel and Laurenz Strassmeyer, 'Joint Control in European Data Protection Law – How to Make Sense of the CJEU's Holy Trinity - A Case Study on the Recent CJEU Rulings (Facebook Fanpages; Jehovah's Witnesses; Fashion ID).' (2019) 20 *Computer Law Review International* 161. See also Louisa Specht-Riemenschneider and Ruben Schneider (n 608).

‘determines the purposes and means of the processing of personal data’.⁶⁸⁶ This is in sharp contrast to the criterion of ‘exerting influence’ over processing as established in *Jehovan todistajat*. In its most recent ruling on controllership, in *IAB Europe* the CJEU reaffirmed the orchestration conception of controllership after having almost completely negated it in its previous decision just two months earlier in *Belgian State*. We are thus forced to grapple with the role of orchestration as a decisive threshold for accountability.

In the next chapter we will review the consequences of the Court’s expanded reading of the role of controllership. Additionally we will examine whether these consequences are compatible with the Court’s ambitions of ensuring ‘effective and complete’ protection for individuals.

⁶⁸⁶ The GDPR, Article 4(7). Emphasis added.

Chapter Seven: The Consequences of the Problem of Control

1. Introduction

The CJEU's approach of extending the definition of controllership has been the subject of much debate. In *Wirtschaftsakademie*, the referring court proposed a potential expansion of the existing framework for attributing responsibility in data processing. This court suggested a 'third way' that would extend beyond the established categories of controllership and joint controllership. The referring court posited that while a fan page operator might not be classified as a controller in the traditional sense, the act of selecting which operators to engage with could potentially entail some degree of responsibility.⁶⁸⁷ This suggestion implied a more nuanced approach to data processing responsibility, acknowledging the complexities of modern digital ecosystems.

However, the CJEU did not adopt this proposed 'third way'. Instead, it adhered to the existing legal framework, classifying the fan page operator as a joint controller. This decision underscores the Court's preference for applying established legal categories, even in the face of evolving digital relationships and responsibilities.

Furthermore, Advocates General of the CJEU have also pushed against the expansive reading of controllership. In *Google Spain*, Advocate General Jääskinen proposed incorporating a knowledge component into the definition of a data controller. This proposition suggested that a data controller should possess awareness, in a 'semantically relevant way,' of the nature of personal data being

⁶⁸⁷ *Wirtschaftsakademie* at [24].

processed and the rationale behind such processing.⁶⁸⁸ Furthermore, the controller should process this data with a specific intention related to its status as personal data.

Additionally, in his advisory opinion in *Fashion ID*, Advocate General Bobek raised the concern that by extending the chain of responsibility, data subjects are in fact less protected. He argued that the ‘effective protection of something tends to dramatically decrease if everyone is made responsible for it. Making everyone responsible means that no-one will in fact be responsible’.⁶⁸⁹ This critique highlights the potential practical challenges and unintended consequences of an overly inclusive definition of data controllership. In this chapter we outline the key challenges which emerge from the CJEU’s case law on controllership. Thereafter we will examine these challenges in light of the Court’s ambitions of ensuring ‘effective and complete’ protection for individuals.

2. Framing and Linguistic Problems

A first question that may be asked about the CJEU’s ‘fragmented’ or ‘phase orientated’ approach is whether it is compatible with the framework of the GDPR itself.

In *Fashion ID* the Court made appeal to an organic reading of the act of ‘processing’ as a series of independent actions.⁶⁹⁰ In reality, there is no reference to a separation of these phases of processing in either the GDPR or its predecessor the 1995

⁶⁸⁸ Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos, González* [2013] EU:C:2013:424, *Opinion of AG Jääskinen* at [83].

⁶⁸⁹ Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2018] EU:C:2018:1039 *Opinion of AG Bobek* (n 636) At [92].

⁶⁹⁰ *Fashion ID* at [71]-[74].

Directive. Instead, both define processing as '[a]ny operation or *set of operations* which is performed on personal data or on sets of personal data.'⁶⁹¹ The inclusion of the term 'set of operations' indicates an understanding of data processing as a variety of acts forming one chain. This is in contrast to a phased or fragmented conception, in which every stage of a processing activity would be considered an independent event. As Mahieu *et al* observe 'there is no existing framework for assigning specific responsibilities to specific "stages" as such 'the reach and limits of the shared responsibility are unknown.'⁶⁹² Thus, we must conclude that the division of data processing does not seem to have a simple framework onto which it can be applied.

Beyond the issue of framing, a linguistic problem exists as words have been stripped of their meaning. We may understand the Court's expansion of controllership to include orchestration as in the case of *Jehovan todistajat*. However, to say that a party 'determines' the means and purposes of processing in a situation like that described in *Fashion ID* is unintuitive at best. While in *Belgian State*, it is simply not possible to identify any meaningful form of determination as a requirement for controllership.

Moreover, the notion of control central to the aims of Data Protection Law is stripped of any ordinary meaning. The controller-processor model of EU Data Protection Law operates under the presumption that the *controller* has the ability to exercise *control* over the processing activities.⁶⁹³ The meaning of control however

⁶⁹¹ 1995 Directive, 2(b); the GDPR, Article 4(2).

⁶⁹² René Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and Its Application to Data Access Rights in Europe, 10 (2019) Para 1.' (2019) 10 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 85, 96.

⁶⁹³ Peter Blume, 'An Alternative Model for Data Protection Law: Changing the Roles of Controller and Processor' (2015) 5 International Data Privacy Law 292, 292.

has now been stretched to include allowing or facilitating data processing. We may question what *control* Fashion ID really held over the personal data being processed by Facebook. This is even more clearly the case in *Belgian State* where we are confronted with a controller which by virtue of its own legal mandate cannot exercise *control*.

3. Diminishing Legal Certainty

The identification of the actors in data processing relationships is fundamental to ensuring legal certainty under the GDPR. As the EDPB notes in its 2020 ‘Guidelines on the concepts of controller and processor in the GDPR’.

The concepts of controller, joint controller and processor play a crucial role in the application of the General Data Protection Regulation 2016/679 (GDPR), since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice.⁶⁹⁴

Similarly, Recital 79 of the GDPR highlights the vital need for legal certainty around the responsibilities and liabilities of actors in data processing in order to ensure legal certainty.

The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

⁶⁹⁴ European Data Protection Board, ‘Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021’ (n 339).

In the cases examined in the previous chapter, the CJEU extended the boundaries of responsibility, control, and accountability under EU Data Protection Law in ways which impact this legal certainty.

In the first three cases the Court clarified the earlier developed concepts of ‘joint responsibility’ and ‘joint liability’. However, while the CJEU has used these terms interchangeably, there is in fact a crucial distinction as Zalnieriute and Churches explain:

‘[L]iability’ in general refers to answerability for legal obligations (in this case to data subjects), whereas ‘responsibility’ refers to duties of the data controllers; to inform, obtain consents, and process data fairly.’⁶⁹⁵

While not all liability falls upon weaker parties, the issue remains that all data protection obligations do.⁶⁹⁶ Article 26(3) of the GDPR states that data subjects may exercise their rights ‘in respect of and against each of the [joint] controllers’ *regardless* of the way joint controllers have chosen to divide roles.⁶⁹⁷ As Ducuing *et al* note:

While ... the joint processing might only pertain to a small part of the overall processing ... all the obligations with regard to joint controllership relating to this specific processing will apply. This means that the joint-controllers need to make agreements determining their respective responsibilities for compliance, including and in particular with regard to their duties to provide information and with regard to the rights to the data subject (visitors with or without a Facebook account), including possibly a contact point.⁶⁹⁸

⁶⁹⁵ Zalnieriute and Churches (n 637).

⁶⁹⁶ For more on liability under GDPR see Van Alsenoy (n 373).

⁶⁹⁷ Wong (n 11) 379.

⁶⁹⁸ Ducuing, Schroers and Kindt (n 617) 551.

This may further undermine data protection rights through a misallocation of responsibility. As Wong argues, following *Fashion ID* EU Data Protection Law ‘may misallocate responsibility, by failing to allocate responsibility to the entity best placed to fulfil that responsibility.’⁶⁹⁹ This is especially problematic where a controller is practically unable to perform some of its data protection obligations.

The problem is further complicated by the principle established by CJEU that a party does not need to have access to the personal data concerned to be determined to be a joint controller. Without this access a controller would not be able to fulfil the obligations set out in the GDPR and instead be forced to compel their joint controller partner to do so on their behalf. This situation may be untenable when a significant imbalance in power and knowledge exists between these joint controllers.

This difficulty reaches its logical conclusion in the paradoxical holding in *Belgian State*. The essential role of *Moniteur belge* is to act *without* any discretionary authority—it merely publishes content as it is devoid of the capacity to select, question, or alter the material prior to its release. Yet, this very absence of decision-making authority is, in itself, construed by the Court to be a distinctive form of determination.

Compounding the lack of legal certainty is the issue of domain revision. Certain use cases have been mapped out in Data Protection Law’s accountability framework. Through case law, and guidance from the WP29, the EDPB, and national Supervisory Authorities these domains have been mapped out for data processing relationships. Yet, the constantly evolving use of technology means

⁶⁹⁹ Wong (n 11) 383.

that as new applications and use cases emerge, the established assumptions of these domains must be revisited. If the act of providing clarity may be likened to cartography we are now forced to admit that the world we sought to map has veered beyond our understanding. Thus, legal certainty decreases for actors in data processing chains, and data subjects find their control rights obscured.

A key example is that of cloud computing. Cloud computing has emerged as the foundation for a myriad of internet-based services. The term refers to the practice of accessing computing resources and capabilities, such as databases, software, and analytics, through a network. These resources and capabilities are typically offered as services that can be rented on demand and paid for based on usage. Cloud services support various applications, such as websites, mobile apps, and other software and services.⁷⁰⁰ There has been a marked increase in the adoption of cloud services among application developers, who are drawn to the potential for diminished barriers to market entry and reduced operational expenditures, benefits derived from the substantial economies of scale achieved by cloud service providers. The result is the model of ‘anything as a service’ – reflecting the reality that any software or technology infrastructure can be offered to a customer through licensing contracts.⁷⁰¹ Cloud Computing has been largely defined through the WP29’s Opinion 05/2012⁷⁰² and a certified Code of Conduct.⁷⁰³ The Cloud Code of Conduct was developed by the EU Cloud Code of Conduct General Assembly and approved by the Belgian Data Protection Authority (*‘Autorité de protection des*

⁷⁰⁰ W Kuan Hon, Christopher Millard and Jatinder Singh, ‘Cloud Technologies and Services’ in Christopher Millard (ed), *Cloud Computing Law* (Oxford University Press 2021) <<https://doi.org/10.1093/oso/9780198716662.003.0001>> accessed 22 March 2023.

⁷⁰¹ Yucong Duan and others, ‘Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends’, *2015 IEEE 8th International Conference on Cloud Computing* (2015).

⁷⁰² Article 29 Working Party, ‘Opinion 05/2012 on Cloud Computing 01037/12/EN WP 196’.

⁷⁰³ Under Article 40 of the GDPR, industry associations and representative bodies can create codes of conduct to specify the application of GDPR provisions in specific sectors.

données Gegevensbeschermingsautoriteit') in May 2021,⁷⁰⁴ following approval from the EDPB.⁷⁰⁵ As such the roles of actors within cloud platforms are largely defined.

In the simplest scenario, it is cloud service customers and end users who hold the role of controller. This is reflected both in EDPB guidance⁷⁰⁶ and within the contractual terms for large cloud service providers. AWS's terms of service make clear that in the vast majority of instances it is the Cloud customer who acts as the controller.⁷⁰⁷ This division of roles is common to a variety of major Cloud Service Providers including Microsoft⁷⁰⁸ and Google.⁷⁰⁹ In the majority of circumstances Cloud Service Providers of all varieties will hold the role of processor. In contrast, where the Cloud Service Provider utilises data for its own purposes it acts as a controller.⁷¹⁰ Yet when cloud computing serves to facilitate more innovative processing such as in the case of AI supply chains, the markers of certainty are moved.

⁷⁰⁴ Belgian Data Protection Authority ('Autorité de protection des données Gegevensbeschermingsautoriteit', 'General Secretariat Decision N° 05/2021 of 20 May 2021'.

⁷⁰⁵ European Data Protection Board, 'Opinion 16/2021 on the Draft Decision of the Belgian Supervisory Authority Regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" Submitted by Scope Europe Adopted 19 May 2021'.

⁷⁰⁶ European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339) 27.

⁷⁰⁷ 'GDPR - Amazon Web Services (AWS)' (*Amazon Web Services, Inc.*) <<https://aws.amazon.com/compliance/gdpr-center/>> accessed 29 March 2023.

⁷⁰⁸ Microsoft, 'Microsoft Products and Services Data Protection Addendum (DPA)' (2023) 7 <<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>> accessed 15 June 2023.

⁷⁰⁹ Google Cloud DPA Section 5 'Cloud Data Processing Addendum' (*Google Cloud*) <<https://cloud.google.com/terms/data-processing-addendum>> accessed 15 June 2023.

⁷¹⁰ European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the Potential of Cloud Computing in Europe"' <https://edps.europa.eu/sites/edp/files/publication/12-11-16_cloud_computing_en.pdf> accessed 19 July 2023.

Legal certainty is particularly damaged by inconsistencies of the CJEU's approach leading it to abandon clear readings of the GDPR itself. A notable example follows from the Court's ruling in *Google Spain*, where the CJEU designated Google Search as a data controller, despite concerns about the feasibility of compliance with data protection law for search engine operations. The subsequent case of *GC*,⁷¹¹ further illuminated the mismatch between search engine functionality and legal requirements. At issue in *GC* was the prohibition on processing 'special category' personal data, as outlined in Article 9(1) of the GDPR. This provision clearly prohibits the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic, biometric, and health data, unless one of the exceptions in Article 9(2) applies. None of these exceptions readily fit Google's search engine operations. A literal interpretation of the law would, therefore, put Google in direct conflict with the prohibition on processing sensitive data, rendering its operations illegal.

To reconcile this conflict, the Court invoked a 'responsibilities formula' first introduced in *Google Spain*, stating that a search engine operator must comply with the law within the framework of its responsibilities, powers and capabilities'.⁷¹² In *GC*, this formula was used to create a unique interpretation of the law's application to search engines. While affirming that the prohibition on processing sensitive data applies to all controllers, including search engines, the Court emphasised the 'specific features' of search engines that affect the extent of their responsibility under the law.⁷¹³ It held that the prohibition could only apply to search engine operators concerning the act of linking to existing publications, subject to

⁷¹¹ *Case C-136/17 GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* [2019] EU:C:2019:773.

⁷¹² *GC and Others* at [31].

⁷¹³ *ibid.* at [45]

verification by competent national authorities based on a data subject's request. The Court's approach in *GC* effectively transformed what was clearly worded as a prohibition in the GDPR into a right that could only be enforced upon request by a data subject. The outcome in *GC* was that the Court maintained the appearance of the law's full applicability to Google Search while interpreting the prohibition as a right, thereby accommodating Google's business model. In *Lynskey*'s wording 'This ad hoc rationalisation of the law to accommodate Google's business model not only goes against a literal interpretation of the provision but also contradicts the law's general scheme.'⁷¹⁴

This jurisprudential evolution reflects the broader challenges in applying data protection law to complex digital ecosystems. The Court's approach, while solving immediate practical issues, raises questions about legal certainty and the consistent application of data protection principles across different technological contexts.

We may thus agree with Van Alsenoy who argues that '[t]he aspirations of legal certainty motivating the distinction between controllers and processors have not been realised in practice.'⁷¹⁵ Thus we conclude that the goal of ensuring legal certainty has ultimately been undermined through (i) the increased complexity in data processing relationships; (ii) the radical expansion of controllership; (iii) the issue of domain revision whereby even mapped technologies have become uncertain again through new applications; and (iv) the ad hoc rationalisation of the law through inconsistent CJEU decisions.

⁷¹⁴ *Lynskey*, 'Complete and Effective Data Protection' (n 32) 332.

⁷¹⁵ *van Alsenoy* (n 127) 576.

4. Undermining Consent and Transparency

The GDPR outlines the core principles which must be adhered to for all processing of personal data. As mentioned above,⁷¹⁶ Article 5 (2) places the onus upon the controller to both comply with these principles and to demonstrate compliance with them. The first of these principles is that personal data should be processed ‘lawfully, fairly and in a transparent manner’.⁷¹⁷

One obligation under Article 13 of the GDPR, which stems from the principle of Transparency, is the requirement for the controller to provide information to the data subject ‘at the time when personal data are obtained.’ Included in information to be provided is the ‘the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.’⁷¹⁸

Under the fragmented approach to processing envisioned by the CJEU, the controller of a website like Fashion ID would only need to provide this information for the purposes of processing that it takes part in. That is to say, the purpose of placing cookies on a user’s computer through the Facebook plug-in on Fashion ID’s website. This collection and transfer of personal information to Facebook is only facilitated in order to promote Fashion ID’s brand. However, the chain of purposes quickly grows from this starting point to include the full gamut of uses to which Facebook employs information. These include tracking the user, combining the data with other inputs to profile an individual, and providing the data subject with targeted advertising. All of this begins at the moment when a

⁷¹⁶ See

⁷¹⁷ GDPR, Article 5 (1)(a).

⁷¹⁸ *ibid.* Article 13(c)

cookie is placed on the user's device as they access Fashion ID's webpage. As Mahieu and van Hoboken explain:

[T]he cookies related to the like button allow Facebook to track that an individual has visited the Fashion ID website, and through further processing of that information, enables Fashion ID to show advertisements on Facebook specifically targeted to those people who previously visited its website. Moreover, this information, combined with tracking that is happening on other websites, is used to create detailed profiles of individuals and to further optimize the targeting that takes place on Facebook.⁷¹⁹

Moreover, under the ePrivacy Directive which complements the GDPR, consent must be gained for non-essential cookies placed on a user's device.⁷²⁰ Consequently, consent must be the lawful basis of processing relied upon in cases involving social media plug-ins.

Zalnieriute and Churches make the convincing argument that consent which covers only a fragment of the overall processing is in fact 'uninformed and not specific.'⁷²¹ This seems clear considering the GDPR's own definition of consent:

'consent' of the data subject means any freely given, *specific, informed* and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.⁷²²

⁷¹⁹ Mahieu and van Hoboken (n 641).

⁷²⁰ See [Chapter Five, Section 2.2 The ePrivacy Directive](#).

⁷²¹ Zalnieriute and Churches (n 637) 874.

⁷²² The GDPR, Article 4(11) (emphasis added).

As the EDPB explains in its ‘2020 Guidance on Consent’ ‘[i]f the controller does not provide accessible information, *user control becomes illusory*, and consent will be an invalid basis for processing.’⁷²³

Consent holds significance only when individuals are thoroughly informed, presented with suitable options, and capable of making an informed assessment regarding their choices. The essence of consent is diminished if, despite the absence of coercion or manipulation, an individual does not possess a comprehensive grasp of the repercussions tied to their selection. As such, a webpage like that of Fashion ID would be required to provide all information on the purposes to which Facebook will utilise the personal data of website users. This is information which is simply beyond the knowledge of an entity like Fashion ID and thus cannot be provided by it directly. Arguing a similar point, Finck observes:

The problem is...that as that controller would have no access to the software [used by Facebook], it could not independently determine the important elements of the processing or ensure that consent is ‘informed’ where this is the chosen legal basis. As a consequence, such information could only take the following form (and thus be useless): ‘[w]e collect your IP address and Browser-ID and transfer this personal data to Facebook. We do not know what Facebook does with the data.’⁷²⁴

Furthermore, it is absurd to believe that all entities utilising social media plug-ins will be in a position to compel a multinational corporation, such as Facebook’s parent company Meta, to deliver the information required to the data subject.

⁷²³ European Data Protection Board, ‘Guidelines 05/2020 on Consent under Regulation 2016/679 Version 1.0 Adopted on 4 May 2020’ (2020) 14 at [62] (emphasis added).

⁷²⁴ Finck (n 338) 336.

Thus, weaker party joint controllers would simply lack the ability to comply with the GDPR.

Additionally, GDPR's Article 26 requirement for joint controllers to arrange their respective responsibilities either becomes a legal fiction when applied between large technology platforms and individuals, or is widely disregarded. Both outcomes undermine the law's credibility and legitimacy.⁷²⁵

The Court's expansive interpretation of responsibility in Data Protection Law thus leads to situations where compliance becomes practically impossible, aligning with one of Fuller's characteristics of problematic legislation.⁷²⁶

Ultimately, new foundational issues arise from the CJEU's fragmented approach to joint controller status. In data processing relationships where consent is relied upon as the lawful processing basis required under the GDPR the integrity of this consent may be challenged as being insufficiently specific and informed to constitute a legal basis for processing under EU Data Protection Law. Even where lawful grounds to process the individual's data may exist, the complexity of data processing relationships will undermine the principles of Fairness and Transparency found under Article 5 of the GDPR.

In his advisory opinion in *Fashion ID*, Advocate General Bobek had cautioned that this conceptual lack of clarity regarding responsibility allocation might lead to

⁷²⁵ Lynskey, 'Another Turn of the Screw?' (n 617) 322.

⁷²⁶ Lon L Fuller, *The Morality of Law* (Revised edn, Yale University Press 1969) 39.

impossibility of compliance for potential joint controllers.⁷²⁷ However, this warning did not significantly influence the Court's stance.

This situation highlights a fundamental tension in current Data Protection Law: the pursuit of comprehensive coverage may paradoxically undermine the law's practical effectiveness and enforceability. It suggests a need for recalibration to balance the aims of comprehensive protection with realistic compliance expectations, particularly in complex, networked digital ecosystems.

5. Weakening Individual Control and Obscuring Data Commodification

In the CJEU's judgments in *Fashion ID*, *NVSC*, *Belgian State*, and *IAB Europe* it restated that the purpose of interpreting the concept of controller broadly is to ensure 'effective and complete protection of data subjects.'⁷²⁸ However, the impact may be the opposite.

More specifically, Mahieu and van Hoboken reason 'the effects on and the risks for the rights and freedoms of individuals of such complex systems, are – as a whole – much bigger than the mere sum of the risks connected to the individual processing phases.'⁷²⁹

⁷²⁷ Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2018] EU:C:2018:1039 Opinion of AG Bobek (n 123) at [84].

⁷²⁸ *Fashion ID* at [66]; *NVSC* at [29]; *Belgian state* at [28]; *IAB Europe* at [55].

⁷²⁹ Mahieu and van Hoboken (n 641).

Similarly, Zalnieriute and Churches⁷³⁰ explain that despite the prevalent view that individuals voluntarily share their data with Facebook, the case of *Fashion ID* illustrates the falsity of this claim.

[I]ndividuals visiting Fashion ID's website actually lacked specific knowledge about the intended purposes of Facebook processing and could not be fully aware of the extensive scope of data surveillance. In fact, Fashion ID demonstrates that Facebook will have your data even if you did not press the 'Like' button, don't have an account, and did not visit Facebook's website. While the decision may cause Fashion ID to implement some form of consent before the collection occurs, that consent and information will not reveal the true and intended commercial extent of processing.

This confusion may be the unwitting result of a controller simply trying to carry out their own data processing. However, in other cases the nature of relationships is rendered purposefully opaque, thus undermining a key aim of Data Protection Law that of strengthening individual *control* and autonomy.

The example of a single entity with multiple subsidiaries comes to mind. An individual may be comfortable giving over specific information to a health provider, different information to a GPS guidance service, another set of information to a financial advisor, and a final set to a video streaming platform which may reveal political and religious interests. The expectations and understanding of this individual are that each of these entities acts independently. They have been given some claim to the self, but certain limitations have been upheld. Moreover, these limitations are the basis of the relationship, facilitating both control and autonomy by the individual as well as trust in the relationship. However, should it turn out that each of these entities were in fact controlled by a

⁷³⁰ Zalnieriute and Churches (n 637) 875.

single organisation and controller, then the relationship has been inextricably altered. The same level of autonomy is no longer in place.

Such a case may be relevant for Alphabet's numerous holdings including Google, Fitbit, Android, Nest, Google Maps, and YouTube. Each of these platforms holds access to important, but perhaps limited data about the individual. However, the central actor, Google's parent company Alphabet, has a far more holistic and perhaps disconcerting understanding of the individual than that individual had intended to allow. As such, the uncertainty in data processing relationships ultimately obscure the pervasiveness of data commodification, making it both harder to understand and respond to as a societal problem. Despite the growth of actors involved, certain pivotal entities within these supply chains have emerged as dominant forces. These are the tech giants which have become household names in the past two decades.⁷³¹

6. Impact on 'Complete and Effective Protection'

Ensuring robust data protection in Europe necessitates a balanced approach that integrates private enforcement, including actions by civil society, compliance by regulated data controllers, and oversight by public authorities. Indeed, a recurring justification in all the cases examined in Chapter Six is that the objective of maintaining 'a broad definition of the concept of "controller"' is to ensure 'effective and complete protection' of data subjects.⁷³²

⁷³¹ Jatinder Singh, Jennifer Cobbe and Chris Norval, 'Decision Provenance: Harnessing Data Flow for Accountable Systems' (2019) 7 IEEE Access 6562.

⁷³² *Google Spain* at [34]; a close variation of this phrasing appears in *Jehovan todistajat* at [66], *Wirtschaftsakademie* at [45], *Belgian State* at [28], and *IAB Europe* at [55]. It is interesting that in *NVSC* the CJEU only appeals to 'effective protection' but does not mention the ideal of complete protection, see *NVSC* at [29].

By extending accountability to a wider range of individuals and entities, the intention was to foster a more comprehensive and pervasive culture of compliance. This approach has, to some extent, been validated by subsequent developments, particularly in how it has empowered data protection regulators to address systemic concerns more effectively.⁷³³

A notable example of this strategy's impact can be observed in the actions of NOYB, a civil society organisation, which submitted 101 complaints to various European data protection authorities, asserting that website operators utilising Google Analytics and Facebook Business Tools were illegally transferring data from the EU to the United States.⁷³⁴ In response to these complaints, the EDPB issued an initial advisory assessment, emphasising the obligation of each website operator to 'carefully examine whether the respective tool can be used in compliance with data protection requirements.'⁷³⁵ This stance underscores the regulatory expectation that even smaller entities must actively engage in ensuring compliance, rather than simply relying on the practices of larger tech companies.

Moreover, this broad application of responsibility has potentially significant implications for the regulatory landscape, particularly in light of the challenges encountered with the GDPR's pan-European enforcement mechanism. By distributing responsibility more widely, this approach may effectively restore competence to national data protection authorities in cases where the data processing operations of joint controllers affect residents solely within their

⁷³³ Lynskey, 'Complete and Effective Data Protection' (n 32) 324.

⁷³⁴ NOYB, 'EU-US Transfers Complaint Overview' <<https://noyb.eu/en/eu-us-transfers-complaint-overview>> accessed 7 September 2024.

⁷³⁵ European Data Protection Board (EDPB), 'Report of the Work Undertaken by the Supervisory Authorities within the 101 Task Force. 28 March 2023' 5 <https://www.edpb.europa.eu/system/files/2023-04/edpb_20230328_report_101task_force_en.pdf> accessed 7 September 2024.

jurisdiction. This shift could lead to more localised and potentially more responsive regulatory oversight, addressing some of the limitations observed in the centralised enforcement model.

This policy direction reflects a nuanced understanding of the data protection ecosystem, recognizing that effective regulation requires engagement at multiple levels. By making a broader range of entities accountable, it creates a more comprehensive regulatory network that can potentially identify and address compliance issues more efficiently. However, this approach also raises questions about the proportionality of compliance burdens and the capacity of smaller entities to navigate complex regulatory requirements. As stated above, it is unrealistic to expect that all entities employing common technologies would possess the leverage necessary to compel multinational corporations, such as Alphabet or Meta, to furnish requisite information to data subjects. This power imbalance creates a situation where smaller or less influential joint controllers may find themselves inherently incapable of complying with the GDPR requirements. Moreover, Article 26, which mandates that joint controllers delineate their respective responsibilities, further complicates this landscape. When applied to relationships between large technology platforms and individuals or smaller entities, this requirement risks becoming either a legal fiction or a widely disregarded provision. Both outcomes have the potential to undermine the credibility and legitimacy of the data protection legal framework.

The interpretation of Data Protection Law has been characterised by an expansive approach, primarily driven by the aim of preventing human rights infringements. However, this expansive approach is increasingly subject to scrutiny. Advocate General Bobek posits that the current interpretation is 'gradually transforming the GDPR into one of the most de facto disregarded legislative frameworks under EU

law'.⁷³⁶ This sentiment is echoed in academic discourse. Indeed, Bygrave and Tosoni suggest that the law's extensive scope of application may exceed its capacity for effective compliance and enforcement.⁷³⁷ While, Nolan observes that the Court's approach seems to assume a positive correlation between the number of actors subject to data protection law and the quality of protective outcomes.⁷³⁸ Koops goes further, characterising data protection law as 'meaningless law on the books' as a result of its broad scope, among other factors.⁷³⁹

This critique highlights a potential paradox: while the Court justifies its expansive application of the law on human rights grounds, this quest for comprehensive coverage may inadvertently undermine the law's effectiveness and, consequently, the attainment of these very objectives. In Lynskey's rendering, 'we must query whether data protection law can be both complete *and* effective.'⁷⁴⁰

This tension between the expansive interpretation of data protection law and its practical efficacy underscores a critical challenge in the field. It suggests a need for a nuanced reconsideration of the balance between comprehensive coverage and practical enforceability in data protection legislation.

Beyond the concern of controllers, we must consider the impact of extended accountability on the ability to regulate data processing. While the responsibility for full implementation of the law does not rest solely with regulators, they continue to play a crucial role in the overall effectiveness of the EU's data

⁷³⁶ C-245/20 *X and Z v Autoriteit Persoonsgegevens* [2021] EU:C:2021:822, *Opinion of AG Bobek*.

⁷³⁷ Bygrave and Tosoni (n 319) 113.

⁷³⁸ Nolan (n 280) 142.

⁷³⁹ Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 250, 251.

⁷⁴⁰ Lynskey, 'Complete and Effective Data Protection' (n 32) 318. Emphasis in the original.

protection framework. Their actions significantly influence both the degree of private enforcement initiated and the extent to which regulated entities voluntarily comply with the law. Consequently, the broad scope of the law's application presents notable challenges for the regulators tasked with its interpretation and enforcement.

The introduction of the GDPR has led to a marked increase in the volume of cases handled by regulators, indicating a heightened awareness and mobilisation among individuals to address data misuse issues. For instance, the Irish DPC experienced a threefold increase in complaints received between May and December 2018 compared to 2013.⁷⁴¹ This surge in public engagement, while positive, has strained the capacity of regulatory bodies to manage the increased demand for their services. A survey conducted by the EDPB revealed that 82% of regulators explicitly stated they lack sufficient resources to fulfil their duties effectively.⁷⁴² This resource constraint, coupled with the law's broad scope, poses significant challenges for regulators in meeting their legal supervisory obligations.

While insufficient resources exacerbate the enforcement difficulties, the problem extends beyond budgetary concerns. It also involves setting clear regulatory boundaries in a context where data protection law applies to a broad and diverse range of entities. Lynskey compares data protection to regulatory fields such as

⁷⁴¹ 910 Complaints were received in 2013 while 2864 were received between May and December 2018. Data Protection Commission (Ireland), 'Annual Report 25 May - 31 December 2018' <<https://www.dataprotection.ie/sites/default/files/uploads/2019-03/DPC%20Annual%20Report%2025%20May%20-%2031%20December%202018.pdf>> accessed 7 September 2024.

⁷⁴² European Data Protection Board (EDPB), 'Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities' 10 <https://www.edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf>.

energy or competition law, where the regulated parties are more homogenous.⁷⁴³ In contrast, data protection involves a much more varied regulated community. These include individuals, charities, political parties, public authorities, and commercial organisations, each operating within different contexts.⁷⁴⁴ This diversity creates additional challenges for regulators, who benefit from the existence of a ‘cohesive interpretive community,’ where those enforcing and those subject to the rules share a common understanding of the law’s provisions.⁷⁴⁵ For data protection to be effective, regulators and controllers need to operate within a shared interpretive framework. Yet, given the heterogeneity of the regulated community, achieving this coherence is inherently difficult.

The varied nature of the regulated community also results in regulators addressing a wide array of regulatory issues. Recent examples include systemic concerns in data-centric industries, compliance assessments of public data processing initiatives (such as contact tracing applications during the COVID-19 pandemic), complaints against institutional data controllers, and interpersonal disputes involving technologies like smart doorbells and home security devices.⁷⁴⁶ This breadth of contexts and actors makes it challenging for regulators to provide comprehensive and authoritative guidance applicable to all situations.

Moreover, the ability to interpret these open-ended principles effectively can be disproportionately challenging for smaller entities and individuals, who often lack the expertise and resources required for proper compliance. Larger organisations

⁷⁴³ See Niamh Dunne, ‘Knowing When to See It: State Activities, Economic Activities, and the Concept of Undertaking’ 16 *Columbia Journal of European Law* 427.

⁷⁴⁴ Lynskey, ‘Complete and Effective Data Protection’ (n 32) 326.

⁷⁴⁵ Julia Black, *Rules and Regulators* (Clarendon Press; Oxford University Press 1997) 30.

⁷⁴⁶ Lynskey, ‘Complete and Effective Data Protection’ (n 32) 327. The issue of smart home devices is dealt with in greater detail in the next chapter.

may have dedicated legal teams to navigate the nuances of Data Protection Law, whereas smaller actors may struggle to understand and apply abstract principles like fairness. This disparity in capacity further complicates the regulatory landscape and underscores the need for additional support mechanisms to ensure that data protection laws are applied equitably across different sectors and scales of operation.

In summary, in aiming for complete protection for data subjects by expanding the boundaries of controllership, it is clear that the CJEU's stance creates two key challenges for effectiveness. First, in many instances, the law's requirements are practically impossible to comply with in full. Second, the law's broad reach has expanded the diversity of the regulated community, making it harder for all parties to develop a common understanding of the rules. This increased diversity also complicates the regulators' ability to effectively oversee the wide range of data processing activities that fall under their supervision.

7. Conclusion

7.1 Main Challenges

The CJEU's 'fragmented' or 'phases orientated' interpretation of data processing prompts the question of its compatibility with the GDPR's framework. Neither the GDPR nor its predecessor, the 1995 Directive, speak of phases of processing. Rather, the GDPR describes processing 'as any operation or set of operations conducted on personal data or sets of personal data.'⁷⁴⁷ This definition clearly suggests an understanding of data processing as a variety of acts leading to one chain. This is in contrast to a phased or fragmented conception of processing, in

⁷⁴⁷ Article 4(2) (emphasis added).

which every stage of a processing activity would be considered an independent event.

Furthermore, there is currently no structure for assigning responsibilities to particular stages, leaving the extent and boundaries of shared responsibility undefined. Consequently, the segmentation of data processing appears to lack a straightforward context for application.

What is more, a linguistic problem exists as words have been stripped of their meaning. The controller-processor model of EU Data Protection Law operates under the unspoken presumption that the *controller* can in fact *control* the processing activities.⁷⁴⁸ The meaning of *control* however has now been stretched to include facilitating data processing.

In the paradoxical holding of *Belgian State* a new boundary has been met. The fundamental function of the government journal *Moniteur belge* is not to exert control over its content; it is merely a conduit for publication, lacking any power to pick, dispute, or modify what it disseminates. Nevertheless, this very relinquishment of control has been interpreted by the Court as a form of determinative power in its own right.

The increasing complexity of data processing relationships directly impacts the individual who finds herself the data subject in a network of data control relationships. Furthermore, in cases involving actors without expert knowledge the impact may also fall upon a user of technology who now finds herself to be an actor with legal responsibilities under the GDPR.

⁷⁴⁸ Blume (n 693) 292.

Beyond the linguistic and framing challenge identified above, five key consequences of *the Problem of Control* have been identified. In the first instance, (I) legal certainty is undermined as actors, their responsibilities, and liabilities cannot be easily identified. Moreover, (II) consent is hollowed out and can no longer be considered a meaningful lawful basis for the processing of personal data. Furthermore, (III) Even where lawful grounds to process the individual's data do exist, the complexity of data processing chains will undermine the key principles of 'Fairness' and 'Transparency'. (IV) Uncertainty in data processing relationships ultimately obscures the pervasiveness of data commodification, making it both harder to understand and respond to as a societal problem. (V) The cumulative result is that the Individual Control Model which underpins contemporary Data Protection Law is undermined. Indeed, increasingly complex processing chains cannot be understood by individuals, much less commanded by them. In this way both *control* and *controllership* have been rendered void of meaning.

7.2 Complete and Effective Protection

In examining the question of whether these consequences undermine the CJEU's goal of complete and effective protection of data subjects. It is evident that the broad reading of controllership creates significant challenges for the Law's effectiveness in two principal ways. First, the comprehensive nature of Data Protection Law has, in certain circumstances, made compliance with its requirements practically unattainable. Secondly, the broad scope of Data Protection Law has led to a further diversification of the regulated community. This diversity presents substantial challenges for both controllers and regulators charged with exerting *control*. For controllers, it hampers the development of a shared understanding of the law's requirements across different sectors and

contexts. For regulators, it complicates the exercise of effective oversight over the vast array of data processing operations falling within their purview.

These tensions highlight the complex interplay between the ambition for comprehensive protection and the practical realities of implementation and enforcement. They underscore the need for a nuanced approach to data protection that balances the desire for comprehensive coverage with the pragmatic considerations of effective regulation.

7.3 The Limits of Control

While the decisions in *Fashion ID* and *IAB Europe* originate in the realm of online retail and advertising and *NVSC* is connected to the governance of IT procurement, the general principles in relation to controllership are broadly applicable to a great variety of contexts. The possible use cases in the online world are numerous. As Zalnieriute and Churches note the CJEU's findings 'imply that joint controllership could be far more prevalent than previously thought and understood.'⁷⁴⁹ This is a view echoed by Millard who maintains that the CJEU has extended the 'boundaries of the concept of joint control' to include 'any arrangement that involves collaboration in data collection.'⁷⁵⁰ The category of controller thus extends to any party allowing for personal data to be processed. This would include server hosting, peer-to-peer file sharing, and distributed ledger technologies like blockchain.⁷⁵¹

⁷⁴⁹ Zalnieriute and Churches (n 637) 870.

⁷⁵⁰ Christopher Millard, 'At This Rate, Everyone Will Be a [Joint] Controller of Personal Data!' (2019) 9 *International Data Privacy Law* 217.

⁷⁵¹ See Sam Wrigley, "'When People Just Click': Addressing the Difficulties of Controller/Processor Agreements Online' in Marcelo Corrales Compagnucci, Mark Fenwick and Helena Haapio (eds), *Legal Tech, Smart Contracts and Block Chain, Perspectives In Law, Business and Innovation* (Springer Nature 2019) 223–228.

Beyond the online world, the natural extension of the *Fashion ID* and *IAB Europe* decisions plays out when personal data is collected in the physical world through smart devices and is then shared with other parties. It logically follows that data collected through these devices facilitates the processing of the personal data of others. Thus, any user of a smart device could be placed in the role of joint controller. As such, Chapter Eight examines the erosion of the home as a physical and legal sanctuary due to the proliferation of smart home devices. This example is particularly significant as it challenges established legal principles. Despite the longstanding exemption of the home from interference and legal obligations in Privacy and Data Protection Law, *the Problem of Control* nonetheless permeates this domain, highlighting the far-reaching implications of modern technology on traditional legal constructs.

In contrast, Chapter Nine delves into the relatively uncharted territory of AI Service Chains for Data Protection Law. The intricate nature of AI supply chains, with creation, deployment, and utilisation distributed across numerous interconnected stakeholders, presents a formidable challenge to the accountability framework of Data Protection Law. This exploration allows for a critical analysis of whether the controller-based accountability model, originating in the 1980s, remains relevant in the face of these complex, modern technological ecosystems. By examining this domain, the chapter addresses the fundamental question posed at the outset of this thesis: whether the ambitions of Data Protection Law can still be effectively realised with the tools developed thus far.

Chapter Eight: The Disappearing Sanctuary of the Home

1. Introduction

As has been discussed in Chapter Two, the ideal of the home and the retreat it promises is central to both privacy and data protection.⁷⁵² We intuitively understand that some areas are more protected, more sacred, more discreet.⁷⁵³ It was the collapse of the boundaries between the public sphere, the *Polis*, and the domestic realm of the home, the *Oikos*,⁷⁵⁴ which led Warren and Brandeis to pen their argument for a legal right to privacy.

However, an important consequence of *the Problem of Control* is the erosion of this zone as a sanctuary. Over the past two decades the boundaries of the home have been challenged once more. An instructive example of this shift is the case of ‘smart’ home devices. These intelligent devices, from home assistants to smart refrigerators, offer convenience and quality of life. At the same time, they also penetrate the inviolable confines of the home. This benign infiltration opens a gateway for information collection and surveillance.

While these concerns are significant, the particular relevance of smart home devices to this study stems from the unexpected obligations which may accompany their use. Smart surveillance devices and systems are marketed as consumer electronics. As such, the assumption would be that the user is the data

⁷⁵² See [Chapter Two, Section 2. From Privacy to Data Protection.](#)

⁷⁵³ See Westin (n 163) pt One.

⁷⁵⁴ See [Chapter Two, Section 2.1 Early Formulations.](#)

subject and the holder of data protection rights in this regard. However, *the Problem of Control* changes this reality and in so doing may further undermine the divisions between public and private realms. This chapter explores the data protection implications of smart home devices with specific attention given to systems facilitating domestic surveillance.

We will begin with an account of the home in law and the ‘smart home reversal’. Thereafter, attention will be given to the specific case of smart home surveillance. This example provides an important illustration of how *the Problem of Control* may result in the disappearance of the home as a separate domain.

2. The Home in Law

The sacrosanct nature of the home is one found throughout jurisdictions. As the 18th Century English Jurist William Blackstone rendered in his treatise, *Commentaries on the Laws of England*, ‘[t]he law of England has so particular and tender a regard to the immunity of a man’s house, that it stiles it his castle, and will never suffer it to be violated with impunity.’⁷⁵⁵

The connection between the protection of the home and the right to privacy is reflected in the consistent interface between these two ideas. Article 12 of the UDHR tellingly frames the two as components of the same ideal.

No one shall be subjected to arbitrary interference with his *privacy*, family, *home* or correspondence, nor to attacks upon his honour and

⁷⁵⁵ Book 4; Chapter 16, The Avalon Project, ‘Blackstone’s Commentaries on the Laws of England Book the Fourth - Chapter the Sixteenth: Of Offences Against the Habitations of Individuals’ <https://avalon.law.yale.edu/18th_century/blackstone_bk4ch16.asp> accessed 15 February 2022.

reputation. Everyone has the right to the protection of the law against such interference or attacks.⁷⁵⁶

In tracing the drafting process which led to the acceptance of this version, Diggelmann and Cess note that the protection of the home was included in almost every proposal.⁷⁵⁷

In a similar vein, both the ECHR in Article 8 and the CFREU in Article 7 include specific references to the 'home'. The CJEU has yet to interpret the concept of 'home' in the context of Article 7 of the Charter. This contrasts with the case law of the ECtHR where 'home' is recognised as holding an independent meaning.⁷⁵⁸ As such it does not require 'classification under domestic law' in order to be protected.⁷⁵⁹

In *Stolyarova v Russia*, the ECtHR highlighted that the home is integral to an individual's identity, self-determination, and secure place in society.⁷⁶⁰ Thus, the current legal understanding aligns with the traditional notion of Blackstone's view of the home as one's sanctuary.

In Ireland the protection of the home as the 'Inviolability of the Dwelling' is established under Article 40.5 of the Irish Constitution

The dwelling of every citizen is inviolable and shall not be forcibly entered
save in accordance with law.

⁷⁵⁶ Emphasis added.

⁷⁵⁷ Diggelmann and Cleis (n 93).

⁷⁵⁸ Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (n 45) 90–91.

⁷⁵⁹ *Chiragov v Armenia* (n 84) at [206].

⁷⁶⁰ *Stolyarova v Russia Application no 15658/09 [2016] CE:ECHR:2016:0628DEC001565809* at [59].

This version remains fundamentally intact from the corresponding provision in Article 7 of the 1922 Constitution.⁷⁶¹ The same construction is found in Article 13(1) of the German Basic Law ('inviolability of the dwelling') ('*unverletzlichkeit der Wohnung*'). Hogan *et al* explain the basis of both the Irish and German versions to be the 1919 Constitution of the Weimar Republic.⁷⁶²

The relevance of this provision for privacy has been explored by Hogan J. in *Sullivan v Boylan*.⁷⁶³

Article 40.5 protects the rights of the residents of a dwelling to security, protection against all-comers and privacy ... [t]hese are rights which are enjoyed by all who reside in the dwelling and not simply those who have legal title to that property.

While in *the People v O'Brien*⁷⁶⁴ Hardiman J. observed:

This constitutional guarantee presupposes that in a free society the dwelling is set apart as a place of repose from the cares of the world. In so doing, Article 40.5 complements and reinforces other constitutional guarantees and values, such as assuring the dignity of the individual (as per the Preamble to the Constitution), the protection of the person (Article 40.3.2), the protection of family life (Article 41) and the education and protection of children (Article 42). Article 40.5 thereby assures the citizen that his or her privacy, person and security will be protected against all comers, save in the exceptional circumstances presupposed by the saver to this guarantee.

⁷⁶¹ Gerard Hogan and others, *Kelly: The Irish Constitution* (5th edn, Bloomsbury Professional 2018) <https://www.bloomsburyprofessionalonline.com/view/kelly_irish_constitution/TIC-section-00002991.xml> accessed 15 February 2022.

⁷⁶² *ibid.*

⁷⁶³ *Sullivan v Boylan* [2012] IEHC 389, [2012] 10 JIC 0407. At [27]

⁷⁶⁴ *DPP v O'Brien* [2012] IECCA 68, [2012] 7 JIC 0201. At 17

Moreover the appeal to the home was reinforced in the *Schrems*⁷⁶⁵ decision before the Irish High Court which led to the two decisions of the same name by the CJEU discussed in Chapter Five.⁷⁶⁶ Mr Schrems had brought a complaint to the Irish DPC against Facebook Ireland for exporting his personal data to its parent company in the United States. The complaint followed Edward Snowden's June 2013 revelations of a mass surveillance programme carried out by the US' National Security Agency.⁷⁶⁷ The DPC had rejected Mr Schrems' complaint as the transfer of data between the EU and the USA had been deemed adequate by the European Commission through the 'Safe Harbour' mechanism. Mr Schrems' sought a judicial review of the DPC's decision. Ultimately, Hogan J. elected to refer the issue over the continued validity of the Safe Harbour mechanism to the CJEU. The judgment itself examines the relevance of Article 40.5 as a basis guaranteeing privacy of communications generated within a dwelling. Hogan J explains:

One might add that the accessing by State authorities of private communications generated within the home - whether this involves the accessing of telephone calls, internet use or private mail - also directly engages the inviolability of the dwelling as guaranteed by Article 40.5 of the Constitution.⁷⁶⁸

⁷⁶⁵ *Schrems v Data Protection Commissioner* [2014] IEHC 310, [2014] 2 ILRM 401.at 50

⁷⁶⁶ See [Chapter Five, Section 3.2 The Requirements for International Transfers of Data.](#)

⁷⁶⁷ See 'Six Months of Revelations on NSA' (*Washington Post*)
<<http://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/>> accessed 15 February 2022; Greenwald (n 554).

⁷⁶⁸ *Schrems v Data Protection Commissioner* [2014] IEHC 310, [2014] 2 ILRM 401 (n 728) at [48].

As Hogan *et al.* note ‘The decision in *Schrems* in particular suggests that Article 40.5 could have far-reaching effect as a guarantee of privacy, albeit confined to activities conducted within the dwelling itself.’⁷⁶⁹

3. The Smart Home Reversal

Shoshana Zuboff begins her monumental work *The Age of Surveillance Capitalism*⁷⁷⁰ with a contrasting depiction of technology and the home. She outlines a project undertaken in 2000 by a group of computer scientists and engineers at Georgia Tech known as the ‘Aware Home.’⁷⁷¹ This undertaking was imagined as ‘a human-home symbiosis’ in which many animate and inanimate processes would be captured by an elaborate network of ‘context aware sensors’ embedded in the house and by wearable computers worn by the home’s occupants.⁷⁷²

Zuboff records the three initial assumptions which underlined the project. Firstly, (I) the researchers and developers recognised the emergence of a novel realm of knowledge stemming from these innovative data systems. Furthermore, (II) there was an underlying belief that the ownership of this newfound knowledge and the authority to utilise it for personal betterment would rest solely with the inhabitants of the home. Finally, (III) despite its technological advancements, the team envisioned the Aware Home as a contemporary representation of the timeless notion of the home as ‘the private sanctuary of those who dwell within its walls.’⁷⁷³

⁷⁶⁹ Hogan and others (n 761).

⁷⁷⁰ Zuboff (n 249).

⁷⁷¹ Cory D Kidd and others, ‘The Aware Home: A Living Laboratory for Ubiquitous Computing Research’, *Proceedings of the Second International Workshop on Cooperative Buildings, Integrating Information, Organisation, and Architecture* (Springer-Verlag 1999).

⁷⁷² Zuboff (n 249) 5.

⁷⁷³ *ibid.*

The image presented is one in which the autonomy of the individual and the sanctity of the home as a safe-protected domain are axiomatic. In fact, the design team of the Aware Home decided that as the technology employed would 'be constantly monitoring the occupants' whereabouts and activities . . . even tracing its inhabitants' medical conditions, there was a clear need to give the occupants knowledge and control of the distribution of this information.'⁷⁷⁴

In stark contrast to the ideals of the Aware Home, the Global 'Smart Home' economy was valued at US \$ 36 Billion at the time of Zuboff's writing. Within two years it had doubled in size to an estimated global value of US \$ 79 Billion.⁷⁷⁵ The fact that this market is growing rapidly is not in itself an issue. Rather, it is the inversion of the foundational values laid out by the Aware Home project that is truly of interest to us.

The example of Google's Nest thermostat is illustrative of this shift. As Zuboff explains:

The Nest thermostat does many things imagined in the Aware Home. It collects data about its uses and environment. It uses motion sensors and computation to 'learn' the behaviours of a home's inhabitants. Nest's apps can gather data from other connected products such as cars, ovens, fitness trackers, and beds.'⁷⁷⁶

⁷⁷⁴ Kidd and others (n 771). Quoted in Zuboff (n 249) 6.

⁷⁷⁵ 'Global Smart Home Market Research Report (2021 to 2026) - by Product, Technologies, Service, Deployment and Region - ResearchAndMarkets.Com' (7 December 2021) <<https://www.businesswire.com/news/home/20211207005627/en/Global-Smart-Home-Market-Research-Report-2021-to-2026---by-Product-Technologies-Service-Deployment-and-Region---ResearchAndMarkets.com>> accessed 31 January 2022.

⁷⁷⁶ Zuboff (n 249) 6.

An unending volume of personal data is generated from the Google Nest. Like Zuboff, we may pose the question of who is to benefit from the ‘immense new stores of knowledge and therefore new power’ created by these devices?⁷⁷⁷

In one version of the smart home industry, manufacturers and developers would simply vie for competitive advantages in selling their devices to the consumer. These devices would be more powerful, convenient, and impressive than the consumer technology that had been bought and enjoyed by users since the mid-20th century. These machines would bear little resemblance to the televisions, radios, gaming devices, and personal computers of previous decades, yet they would be part of a clear evolutionary line. Instead, the reality faced is one of a fundamental departure from the devices of the past, where data is simultaneously extracted from individual users, even as services are rendered to them.

We are reminded of the Cold-War joke-form known as the Russian Reversal.⁷⁷⁸ The through line of many of these jokes is the theme of surveillance with a notable variation was told by Academy Awards host Bob Hope in 1958: ‘in America you watch the TV, in the Soviet Union the TV watches you.’⁷⁷⁹ This is an anachronism, but only in the sense that there could be any locale where some form of surveillance is not tied into consumer technology.

⁷⁷⁷ *ibid.*

⁷⁷⁸ Debora Battaglia, ‘Coming in at an Unusual Angle: Exo-Surprise and the Fieldworking Cosmonaut’ (2012) 85 *Anthropological Quarterly* 1089, 1103. At Footnote 22. A well-known example is ‘in America you can always find a party, while in the Soviet Union the Party can always find you.’

⁷⁷⁹ As described by Time Magazine: ‘Bob Hope, back from his Russian junket, noted that there had been TV in all the rooms of his Moscow hotel—‘only it watches you’” Lily Rothman, ‘In Soviet Russia, the Oscars Host You’ (*Time*, 23 February 2015) <<https://time.com/3715747/bob-hope-russian-reversal/>> accessed 5 July 2023.

Marketed under the banner of consumer electronics, smart surveillance devices and systems are typically utilised with the assumption that the user is the data subject. Yet, the reality is more complex as the Irish DPC notes an unanticipated problem associated with smart surveillance technology when used by private individuals is that they 'may not appreciate their obligations in relation to the rights of others, including privacy and data protection rights.'⁷⁸⁰ Through the use of these devices not only is it possible to make oneself observable within the confines of one's own home. But one may also have turned this realm into an extension of surveillance for others.

4. The Impact of Smart Home Devices

Amazon's smart home products provide a valuable case study of this change in the status of the home. Amazon's acquisitions in recent years extend beyond the familiar territory of e-commerce, enabling the company to gain an intricate, potentially invasive perspective on the consumer's domestic environment and routines. The 2014 launch of Alexa, Amazon's virtual assistant technology, opened a significant mechanism for data access, including voice recordings and a multitude of personal consumer data. Built to facilitate tasks such as answering queries, playing music, and controlling other smart devices, Alexa provides a level of convenience and interactivity that appears to have materialised from science fiction. The virtual assistant constantly listens for its 'wake word' to initiate its functions. This persistent aural surveillance generates a considerable volume of

⁷⁸⁰ Data Protection Commission, Ireland, 'Guidance on the Use of Domestic CCTV.' (2021) <<https://www.dataprotection.ie/en/dpc-guidance/guidance-use-domestic-cctv>> accessed 13 March 2024.

personal data, which is subsequently stored and used for various purposes by Amazon and potentially third-party entities.⁷⁸¹

There is increasing apprehension about the commodification of personal data gathered by Alexa.⁷⁸² This data, ranging from mundane conversations to sensitive personal information, is transformed into a profitable asset in the vast digital marketplace. This commodification process is often shrouded, further exacerbating privacy concerns. Moreover, the implications for individual rights under the GDPR are significant. Alexa users are subjected to a complex web of data processing activities, the full extent of which can be difficult to discern or control. While Amazon contends that it has robust policies in place to ensure user privacy, the power asymmetry between the controller (Amazon) and the data subjects (Alexa users) presents a clear challenge to achieving the ideals of the GDPR.⁷⁸³

Furthermore, the 'always on' nature of devices like Alexa can blur the line between public and personal domains, altering the individual's perception and experience

⁷⁸¹ Anne Pfeifle, 'Alexa, What Should We Do about Privacy: Protecting Privacy for Users of Voice-Activated Devices Comments' (2018) 93 Wash. L. Rev. 421.

⁷⁸² See Eoghan Furey and Juanita Blue, 'Alexa, Emotions, Privacy and GDPR', *Proceedings of the 32nd International BCS Human Computer Interaction Conference* 32 (2018); Josephine Lau, Benjamin Zimmerman and Florian Schaub, 'Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers' (2018) 2 *Proceedings of the ACM on human-computer interaction* 1; Katherine Minorini, 'A Vendetta against Alexa: Privacy Concerns in the Age of the Smart Home' (2021) *Boston College Intellectual Property and Technology Forum* 1; Yupeng Mou and Xiangxue Meng, 'Alexa, It Is Creeping over Me - Exploring the Impact of Privacy Concerns on Consumer Resistance to Intelligent Voice Assistants' (2024) 36 *Asia Pacific Journal of Marketing and Logistics* 261.

⁷⁸³ See Furey and Blue (n 782); Lau, Zimmerman, and Schaub (n 782); Minorini (n 782); Mou and Meng (n 782).

of privacy within their own homes.⁷⁸⁴ This subtle, yet profound, shift has implications for the interpretation and enforcement of privacy and data protection rights.

By 2018, Amazon had also acquired Ring, a purveyor of smart home devices⁷⁸⁵ for a reported fee of US\$ 839 Million.⁷⁸⁶ Ring offers a wide variety of products including video cameras, and alarm systems with motion detection.⁷⁸⁷ The best known of these is Ring's video doorbell, which allows users to view, communicate and record people who come to their home entrances. In a further move in 2022, Amazon's attempted acquisition of iRobot, known for their robotic vacuum cleaners, would have allowed Amazon a novel glimpse into the interiors of individual's homes.⁷⁸⁸

This acquisition strategy underscores Amazon's deepening engagement with surveillance capitalism, a term coined by Zuboff to describe 'the unilateral claiming of private human experience as free raw material for translation into behavioural data.'⁷⁸⁹ Amazon possesses a holistic understanding of the consumer's

⁷⁸⁴ 'The Privacy Threat From Always-On Microphones Like the Amazon Echo | ACLU' (*American Civil Liberties Union*, 12 January 2017) <<https://www.aclu.org/news/privacy-technology/privacy-threat-always-microphones-amazon-echo>> accessed 28 February 2024.

⁷⁸⁵ Samuel Gibbs, 'Amazon Buys Video Doorbell Firm Ring for over \$1bn' *The Guardian* (28 February 2018) <<https://www.theguardian.com/technology/2018/feb/28/amazon-buys-video-doorbell-ring-smart-home-delivery>> accessed 5 July 2023.

⁷⁸⁶ Rani Molla, 'How Amazon's Ring Is Creating a Surveillance Network with Video Doorbells' (*Vox*, 5 September 2019) <<https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell-hacks>> accessed 10 March 2024.

⁷⁸⁷ Kristin A Kelly, 'The Ring Video Doorbell and the Entry of Amazon into the Smart Home: Implications for Consumer-Initiated Surveillance.' (2023) 46 *Journal of Consumer Policy* 95, 95.

⁷⁸⁸ iRobot, 'Amazon and iRobot Sign an Agreement for Amazon to Acquire iRobot' (*iRobot MediaKit*) <<https://media.irobot.com/2022-08-05-Amazon-and-iRobot-sign-an-agreement-for-Amazon-to-acquire-iRobot>> accessed 5 July 2023. This acquisition has subsequently been abandoned.

⁷⁸⁹ Zuboff (n 249) 8.

preferences, habits, emotions, routines, purchasing patterns, and property characteristics.

In an important development, the US Federal Trade Commission ('FTC') issued two decisive judgments against Amazon on May 31, 2023. In the first decision, Amazon was charged with violating the Children's Online Privacy Protection Act ('COPPA')⁷⁹⁰ by retaining and exploiting Alexa's voice recordings and geolocation data for an extended period.⁷⁹¹ The second ruling held Ring responsible for infringing customers' privacy by allowing illicit surveillance by its employees.⁷⁹² These judgments underscore the need for scrutiny of Amazon's data processing practices.

5. The Smart Home: Roles and Expectations

Amazon's Ring service provides an illustrative case study in showing the complexities of data processing relationships through smart home devices.

Upon purchasing a Ring product, users are able to access the basic features of real time footage and the ability to communicate with a person within the viewing area of the smart doorbell. For users on 'the Ring Protect Plan', who pay a subscription

⁷⁹⁰ Children's Online Privacy Protection Act [1998] 15 U.S.C. §§ 6501–6506 (Public Law) 112 Stat. 2681-728 (United States).

⁷⁹¹ 'FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests' (*Federal Trade Commission*, 31 May 2023) <<https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>> accessed 5 July 2023.

⁷⁹² 'FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras' (*Federal Trade Commission*, 31 May 2023) <<https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users>> accessed 5 July 2023.

fee, videos are also recorded in a cloud-based server.⁷⁹³ In addition, users have the option of creating links to share the videos recorded on Ring's cloud servers. In this case a separate copy of the video is created in Ring's cloud server for the explicit purpose of sharing. In the US, the option also exists for devices to integrate with Ring's social media app 'Neighbors', where users can post videos of suspicious activity and crimes outside their front doors, as well as view posts from other people within a limited radius of their homes.⁷⁹⁴ Neighbors is not available in the EU.

A user is automatically enrolled in the Neighbors social media upon installing a Ring device in the US. Individuals without Ring devices can also use the app, where they can anonymously read or post — using video or not — about crime, safety, suspicious activity, and lost pets within a five-mile radius of their home. The app also alerts users to real-time 911 emergency service call data as well as content from Ring's own news team.⁷⁹⁵

⁷⁹³ This is explained on Ring's EU Privacy Notice. 'If you do not have a Ring Protect Plan, Ring does not record or store your videos, but you can still view your device's live video stream (Live View). If you do have a Ring Protect Plan (including a free trial), Ring records and stores videos when motion is detected by your device (including devices linked to cameras such as an alarm system's motion detector), the video doorbell button is pressed, or you initiate Live View. Video recordings in your account are automatically deleted following the expiration of your account's applicable storage period under the Ring Protect Plan. Amazon, 'Privacy New' (Ring) <<https://eu.ring.com/pages/privacy>> accessed 21 January 2022.

⁷⁹⁴ Eric Kuhn Neighbors Head of, 'Ring Announces New Neighbors App Features, Sunsets Request for Assistance Post' (*The Ring Blog*, 24 January 2024) <<https://blog.ring.com/about-ring/ring-announces-new-neighbors-app-features-sunsets-request-for-assistance-post/>> accessed 28 February 2024.

⁷⁹⁵ Kelly (n 787) 99–100. Molla (n 786).

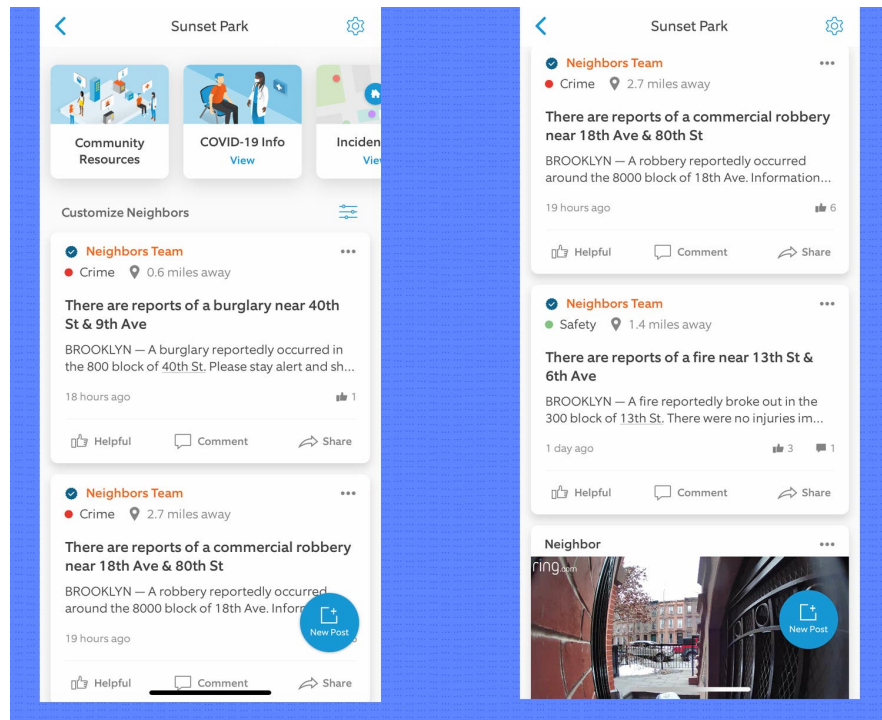


Figure 14. Ring's 'Neighbors' App⁷⁹⁶

One issue for smart doorbell systems such as Ring is the access given to users' data beyond that which is understood by the owner and their household. Even greater concern surrounds the unrealised obligations which the user may hold when utilising the service. It is fully possible for a Ring Product owner to be a controller without realising this fact.

In its EU terms of Service, Ring makes it clear that it views itself as the processor of information acting on behalf of the product user:

You are the data controller with respect to personal information you obtain when using our products and services (such as video or audio recordings, live video or audio streams, images, comments, and data our

⁷⁹⁶ Image taken from: 'Ring Neighbors Is the Best and Worst Neighborhood Watch App' (Wirecutter: Reviews for the Real World, 3 June 2021) <<https://www.nytimes.com/wirecutter/blog/ring-neighbors-app-review/>> accessed 19 January 2022.

products collect from their surrounding environment to perform their functions) and you are solely responsible for ensuring that you comply with applicable law when you use our products or services.⁷⁹⁷

Such a relationship places the full onus of obligations upon a Ring owner and user to protect others whose data is now processed by Ring. This is represented in *Figure 15* below.

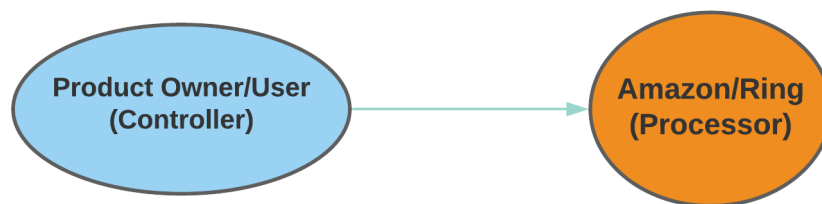


Figure 15. Ring Owner/User as Controller

6. The Disappearing Household Exemption

The starting point for discussion is whether smart surveillance domestic devices fall within the framework of data protection under the GDPR. The household exemption as discussed in Chapter Four should have obvious application within the context of an individual's own home.⁷⁹⁸

In the *Ryneš* case,⁷⁹⁹ the CJEU examined whether the household exemption would also apply to a security camera used for a home which also recorded the public footpath outside of the property. The Court found that such usage could not be construed as 'purely' personal and would be subject to Data Protection Law.⁸⁰⁰ As

⁷⁹⁷ 'Privacy Notice' (Ring) <<https://eu.ring.com/pages/privacy-notice>> accessed 10 September 2024.

⁷⁹⁸ See [Chapter Four, Section 4. Material Scope of the GDPR](#).

⁷⁹⁹ Case C-212/13 *Ryneš v Úřad pro ochranu osobních údajů* [2014] EU:C:2014:2428.

⁸⁰⁰ Costello, *Privacy Law in Ireland* (n 75) para 8.47.

such, the first issue with any form of domestic surveillance is its use beyond the home. In this vein the Irish DPC advises ‘all householders to operate their devices in a way that only captures images within the perimeter of their own property.’⁸⁰¹ The Irish DPC notes that most cases it has dealt with fall within the household exemption.⁸⁰²

However, the case of smart surveillance systems presents another issue for domestic use – that of data being shared beyond the household via an online setting. The limitations of the household exemption to sharing of personal information via online means have already been tested in the *Lindqvist* decision.⁸⁰³ In its ruling the CJEU clarified that the household exemption must ‘be interpreted as relating only to activities which are carried out in the course of private or family life of individuals,’ however this ‘is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.’⁸⁰⁴ Thus outside disclosure of personal information to an indefinite number of people would no longer fall under the household exemption.

Following the *Lindqvist* ruling, the European Data Protection Board explains that ‘any disclosure of personal data is a separate kind of processing of personal data for which the controller needs to have a legal basis in Article 6.’⁸⁰⁵ It would thus appear that in a case where the use of smart surveillance devices results in data

⁸⁰¹ Data Protection Commission, Ireland (n 780) 2.

⁸⁰² *ibid.*

⁸⁰³ *Case C-101/01 Lindqvist v Åklagarkammaren i Jönköping [2003] EU:C:2003:596.*

⁸⁰⁴ *ibid.* at [47].

⁸⁰⁵ European Data Protection Board, ‘Guidelines 3/2019 on Processing of Personal Data through Video Devices Version 2.0 Adopted on 29 January 2020’ (n 909) 15.

flows which simply cannot be limited to the home itself, then the household exemption will not apply.

This conclusion is supported by Chen *et al*:

Before the advent of smart home IoT technologies, ascertaining how data protection law should regulate users in a domestic setting was once straightforward; the burdens of domestic data controllers were alleviated by relieving them of the data protection responsibilities. This is not the case anymore.⁸⁰⁶

Finck similarly accepts that ‘the conclusion that smart homeowners can be controllers has become unavoidable. Importantly, smart homeowners collect various kinds of data, both related to others (visitors) and inhabitant(s).’⁸⁰⁷

It is also clear from the *Lindqvist* decision that should the user share the videos recorded on smart devices on a social network, then the user would act as a controller who is not exempt from the GDPR under the household exemption. However, two scenarios already occurring with Ring’s use of data indicate that more complex data sharing relationships exist.

The first is the case of Ring’s ‘Neighbors’ app, where users are encouraged to share videos on a social media account controlled by Ring. The second is where Ring makes use of the personal data of individuals captured on Ring devices for other

⁸⁰⁶ Jiahong Chen and others, ‘Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption’ (2020) 10 INTERNATIONAL DATA PRIVACY LAW 279.

⁸⁰⁷ Finck (n 338) 339.

uses. This has already occurred in the US where such data has been used for advertising purposes.⁸⁰⁸

In both these cases it would appear that the correct understanding of the data-sharing is a joint controller relationship. Following the rulings of the CJEU anyone in a ‘personal data chain’ who makes data processing ‘possible’ becomes a joint controller.⁸⁰⁹ In the case of Ring, it would appear that the owner of the product or user would fill the Fashion ID⁸¹⁰ role by facilitating the data processing of personal data collected from data subjects captured on Ring devices. Indeed, without the Ring user it is clear that Ring and Amazon would not be able to process this personal data. Importantly, this does not imply equal responsibility and liability as the CJEU has emphasised in all the decisions discussed in Chapter Six.

Moreover, SA conclusions in the case of cloud computing carry important significance for this assessment. In its 2012 ‘Recommendations’⁸¹¹ the French Supervisory Authority, the CNIL, maintained that in certain situations a cloud service provider will in fact act as a joint controller. The CNIL argued that in instances where customers cannot issue directives to a cloud provider or ascertain the efficiency of its data safety measures, the cloud provider should be designated as a joint controller as it ‘contributes to the definition of the purposes and means

⁸⁰⁸ Matthew Guariglia, ‘Amazon’s Ring Is a Perfect Storm of Privacy Threats’ (*Electronic Frontier Foundation*, 8 August 2019) <<https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats>> accessed 19 January 2022.

⁸⁰⁹ Edwards and others (n 683).

⁸¹⁰ See [Chapter Six, Section 7. CJEU Decision in Fashion ID](#).

⁸¹¹ Commission nationale de l’informatique et des libertés (CNIL), ‘Cloud Computing : CNIL’s Recommendations for Companies Using These New Services’ (2012) <<https://www.cnil.fr/en/cloud-computing-cnils-recommendations-companies-using-these-new-services>> accessed 19 July 2023.

for personal data processing.’⁸¹² More recently this finding has been supported by the Slovenian Supervisory Authority. In its 1 June 2022 ruling, the Information Commissioner (Slovenia) found that a particular cloud computing provider decided on the essential means of processing. As such it was to be considered a controller.⁸¹³

Given the determinations by the CNIL and Slovenia’s Information Commissioner regarding cloud computing entities, it would seem prudent to reconsider this classification. Through this lens we may view manufacturers of these devices as joint controllers. The likely relationship between parties is represented in *Figure 16* below.

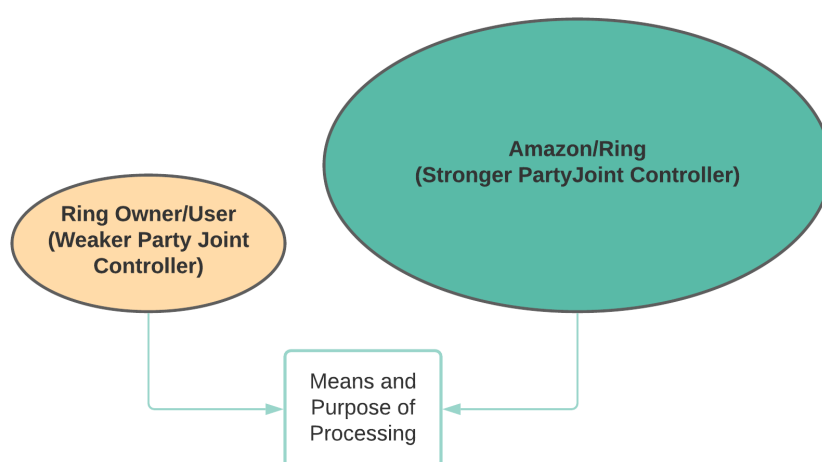


Figure 16. Ring Owner/User as Joint Controller

To be clear, the assertion of this thesis is not that individuals should never be placed in the role of data controller. This will often be appropriate and clear,

⁸¹² *ibid* 5.

⁸¹³ Information Commissioner (Slovenia), ‘Decision No. 0612-23/2019/19’ <https://gdprhub.eu/images/8/89/IP_%28Slovenia%29_-_0612-23-2019-19.pdf> accessed 19 July 2023.

further ensuring individual rights and obligations. However, this is not the case when an individual could not have understood that they were taking on this role. The Ring purchaser or user is not likely to have envisioned the potential data processing which others coming into their home would now be subject to as well. If they were aware of Data Protection Law's provisions, the assumption would be that they should be exempted via the household exemption. Thus the resultant obligations could not fairly have been foreseen by an individual buying or utilising a device for the protection of their own household. As such *the Problem of Control* is exacerbated in this context by further undermining the expectations of individuals entering into the informational and physical domain of the home.

7. Conclusion

The delineation of private and public spheres is an enduring theme of legal and philosophical analysis. The boundaries set by these two domains have been continuously remoulded. Yet, amidst this interplay between personal sanctuary and societal engagement, the home – the epitome of private domain – has always retained its sacred status. As an emblem of individual privacy, the sanctity of the home is a core focus of this chapter.

The proliferation of smart home devices has reshaped the once clearly demarcated realms of private and public. This benign infiltration opens a gateway for information collection and surveillance that could inadvertently jeopardise the very foundation of data protection.

Furthermore, it is worth noting how adeptly manufacturers of these surveillance solutions navigate the regulatory landscape. By portraying themselves as mere processors under the GDPR, they seek to sidestep the heavier responsibilities that come with their systems. However, given the determinations by the CNIL and Slovenia's Information Commissioner regarding cloud computing entities, it

would seem prudent to reconsider this classification. Through this lens we may view manufacturers of these devices as joint controllers.

Nevertheless, this problem will still impact ordinary households utilising these devices. They might unknowingly assume roles as data controllers or as joint controllers. The once-reliable shield of the household exemption now seems less certain, ushering in new responsibilities and potential liabilities for these unsuspecting users. It stands to reason that as technology continues to evolve and redefine our lived experiences, so must our regulatory and legal structures rise to address the emerging challenges.

The sanctity of the home is foundational to the right to privacy under Article 7 of the Charter and Article 8 of the ECHR. In *Stolyarova v Russia*, the ECtHR highlighted that the home is integral to an individual's identity, self-determination, and secure place in society.⁸¹⁴ Yet we once again return to the claim of Warren and Brandeis that 'what is whispered in the closet shall be proclaimed from the house-tops.'⁸¹⁵

Yet again, it is technology which has rendered the physical walls of the past porous. Yet again, the legal defences of the past are inadequate as *the Problem of Control* has confounded the expectations of individual users of technology. What is new, is that through an expanding market of smart devices we have now been co-opted into betraying the data protection expectations of ourselves and those who enter our dwellings.

⁸¹⁴ *Stolyarova v Russia Application no 15658/09 [2016] CE:ECHR:2016:0628DEC001565809* at [59].

⁸¹⁵ Warren and Brandeis (n 77) 195.

Chapter Nine: AI Services and the Limits of the Control Model

1. Introduction

The rise of commercial AI systems represents a paradigm shift in multiple sectors, from healthcare to financial services. These tools process vast volumes of data in order to initiate actions, make decisions, and in some instances, evolve their own operating parameters. While the potential societal benefits are numerous, so too are the intricate legal and ethical questions raised.

The introduction of ChatGPT⁸¹⁶ and DALL-E⁸¹⁷ by OpenAI has further changed perceptions of this market. Microsoft's expanded investment in OpenAI in January 2023⁸¹⁸ and its February 2023 announcement of the integration of AI solutions into its own search engine, Bing, highlight the potential growth of this domain.⁸¹⁹ Beyond Bing, Microsoft offers AI Services through its Azure products.⁸²⁰ Other systemically large actors within this space include Amazon,⁸²¹

⁸¹⁶ OpenAI, 'ChatGPT' <<https://openai.com/product/chatgpt>> accessed 31 May 2023.

⁸¹⁷ OpenAI, 'DALL·E 2' <<https://openai.com/product/dall-e-2>> accessed 31 May 2023.

⁸¹⁸ Microsoft, 'Microsoft and OpenAI Extend Partnership' (*The Official Microsoft Blog*, 23 January 2023) <<https://blogs.microsoft.com/blog/2023/01/23/microsoftandopenaiextendpartnership/>> accessed 31 May 2023.

⁸¹⁹ Yusuf Mehdi, 'Reinventing Search with a New AI-Powered Microsoft Bing and Edge, Your Copilot for the Web' (*The Official Microsoft Blog*, 7 February 2023) <<https://blogs.microsoft.com/blog/2023/02/07/reinventing-search-with-a-new-ai-powered-microsoft-bing-and-edge-your-copilot-for-the-web/>> accessed 31 May 2023.

⁸²⁰ Microsoft, 'Azure AI Platform—Artificial Intelligence | Microsoft Azure' <<https://azure.microsoft.com/en-us/solutions/ai/>> accessed 31 May 2023.

⁸²¹ AWS, 'Artificial Intelligence Services' (*Amazon Web Services, Inc.*) <<https://aws.amazon.com/machine-learning/ai-services/>> accessed 31 May 2023.

Alphabet (Google),⁸²² and IBM.⁸²³ All of these providers offer both bespoke and pre-built general-purpose services. Specific providers also offer tailored AI packages for unique purposes such as hiring, as is the case with HireVue⁸²⁴ and Pymetrics.⁸²⁵ ClearviewAI's⁸²⁶ facial recognition surveillance service provides a more controversial example of a specific-use AI product. The ever-growing use cases for AI Service processing chains are highlighted in expanding research.⁸²⁷

The intertwined nature of AI ecosystems, where multiple entities contribute to data processing compounds *the Problem of Control*. This chapter explores these challenges, dissecting the tension between the existing regulatory framework and novel situations such as those brought about by AI Systems. Through this exploration, we aim to provide an illustration of the limitations of the classic controller-based responsibility model of Data Protection Law.

⁸²² Google Cloud, 'AI & Machine Learning Products' (*Google Cloud*) <<https://cloud.google.com/products/ai>> accessed 31 May 2023.

⁸²³ IBM, 'IBM Watson Products and Solutions' <<https://www.ibm.com/watson>> accessed 31 May 2023.

⁸²⁴ HireVue, 'HireVue Hiring Platform: Video Interviews, Assessment, Scheduling, AI, Chatbot | HireVue' (*hirevue.com*) <<https://www.hirevue.com/>> accessed 1 June 2023.

⁸²⁵ Pymetrics, 'Pymetrics' Gamified Skills Assessments Leverage Behavioral Science and AI Technology to Help Companies Build Diverse and Innovative Teams.' <<https://www.pymetrics.ai/>> accessed 1 June 2023.

⁸²⁶ It must be noted that Clearview's offering is likely to fall within the prohibited use category of AI Services under the proposed AI Act. Clearview AI, 'Clearview AI Product Overview' <<https://app.hubspot.com/documents/6595819/view/454213073?accessId=c85a92>> accessed 31 May 2023.

⁸²⁷ Thomas Davenport and Ravi Kalakota, 'The Potential for Artificial Intelligence in Healthcare.' (2019) 6 *Future Healthcare journal* 94; Seyyed Ahmad Javadi and others, 'Monitoring Misuse for Accountable "Artificial Intelligence as a Service"', *Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society* (arXiv 2020) <<http://arxiv.org/abs/2001.09723>> accessed 1 June 2023; Morgan Klaus Scheuerman, Jacob M Paul and Jed R Brubaker, 'How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis Services' (2019) 3 *Proc. ACM Hum.-Comput. Interact.* <<https://doi.org/10.1145/3359246>>; Grand View Research, 'Artificial Intelligence as a Service: Market Research Report.' <<https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-as-a-service-market-report>>.

Moreover, AI Services deserve special consideration in this study for several key reasons. (I) First, they are inherently linked to achieving specific functionality in user facing applications. Unlike traditional cloud services that mainly support application deployment, AI Services play a direct role in providing functionality. An AI Service may provide the categorisation, evaluation and forecast that is essential for the customer's application to function as intended. This may amount to deciding the 'means' and 'purposes' of data processing which falls within the exclusive purview of the controller.

Additionally, (II) AI Systems may magnify biases, inaccuracies, and inequalities. Thus, facilitating the dissemination of advanced AI capabilities with minimal provider supervision, can easily lead to dangerous or potentially unlawful applications. (III) The demand for AI Services is expected to increase in the future. Developing Machine Learning ('ML') solutions is often beyond the capacity of organisations due to the expertise, computational capacity and large-scale data sets required. AI Services enable developers to access ML capabilities for their applications despite these constraints.⁸²⁸

Furthermore, (IV) The AI Service sector is likely to amplify the consolidation of power by leading tech firms. Despite the emergence of OpenAI,⁸²⁹ this is a sector already largely dominated by Amazon, Microsoft, and Google. These companies can leverage their significant resources to create AI Services with which upstarts cannot compete. This is likely to be complemented by the opportunities provided by the large market reach enjoyed by these firms. By adding AI capabilities to

⁸²⁸ Jennifer Cobbe and Jatinder Singh, 'Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges' (2021) 42 Computer Law & Security Review 105573, 5–6.

⁸²⁹ We must note that Microsoft's sizeable stake in OpenAI undercuts assumptions that it can be treated as an independent actor.

existing systems further dominance can be achieved. This may create a greater dependency on major players for other organisations that already use their cloud services. This consolidation of AI Services positions the key tech firms as central agents of the social changes that may result from the ubiquity of AI technologies.

Recital 15 of the GDPR states that the protection to be afforded by Data Protection Law ‘should be technologically neutral’. However, the unique challenges posed by AI systems brings this promise into question as will be demonstrated in this chapter. To this end, attention will first be given to the definition of AI and the scope of AI services. Thereafter we will focus upon the challenge of data harvesting which feeds these systems. While this issue is a significant challenge for the EU Data Protection Regime it does not exacerbate *the Problem of Control*. As such, only a brief treatment of the subject will be presented in this chapter.

Instead, the bulk of our analysis will be given to the complexity of assigning accountability in AI services. Focus will be placed upon applying the CJEU’s approach of phase-based processing to the numerous operations inherent within AI Services. Cobbe, and Singh⁸³⁰ provide a complex depiction of the stages in AI service processing which helps highlight *the Problem of Control*. The focus of their work, however, is only upon the GDPR and is further complicated by the new obligations imposed by the AI Act. We will include this new dimension in our analysis.

In Chapter Seven we identified six key concerns of *the Problem of Control*:

⁸³⁰ Cobbe and Singh (n 828).

1. The lack of a conceptual framework onto which the division of processing into stages can be applied.
2. The weakening of legal certainty in data processing relationships as actors, their responsibilities, and liabilities cannot be easily identified.
3. The undermining of consent as a lawful basis for processing personal data.
4. The violation of the Data Protection Principles of 'Fairness' and 'Transparency' through the complexity of data processing relationships.
5. The obscuring of data commodification as a societal issue.
6. The limiting of individual control of personal data through opaque data sharing relationships.

Throughout this chapter we will evaluate the impact that AI Services have on each of these difficulties.

2. Defining AI

Even as references to AI have become ubiquitous in media and industry, we nevertheless lack a clear definition for this term. Its origins can be traced to Computer scientist John McCarthy who coined the phrase 'artificial intelligence' at the Dartmouth Conference of 1955.⁸³¹ In this first context the term was used to describe the act of equipping computer systems with the capability to mimic human brain functions. The goal was to allow these systems to tackle a wide range of cognitive tasks in various environments, a concept known as human-imitative AI.⁸³² However, the term as used in contemporary discourse lacks a precise definition. Generally, AI is understood to be a subfield within computer science

⁸³¹ Wiggins and Jones (n 114) 126–127.

⁸³² Christian Meurisch and Max Mühlhäuser, 'Data Protection in AI Services: A Survey' (2022) 54 ACM Computing Surveys 1, 2.

that focuses on creating ‘intelligent computer systems’⁸³³ or is associated ‘with the automation of intelligent behaviour.’⁸³⁴

In this thesis the definition followed is that given in the AI Act.

‘AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.⁸³⁵

The term AI is often used interchangeably with ML, which allows systems to emulate aspects of human intelligence, though they are not sentient themselves. ML is a technique for finding patterns in data and building models that represent them. ML models and their outputs are probabilistic. They are derived from a statistical representation of training data, and they have some degree of error or uncertainty in their representation and outputs.⁸³⁶ These models can be applied to new data to perform tasks such as classification, prediction, and decision making. For example, a model can be trained to identify certain objects in images by statistically ‘learning’ the features that distinguish them. After training, the model can classify objects in new images. The performance and operation of an ML model depend on how it is designed – factors such as the selection, cleaning, and processing of the data used for training, testing, and analysis; the ML methods,

⁸³³ Stuart J Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (3rd edn, Pearson 2016) 1–5.

⁸³⁴ George F Luger and William A Stubblefield, *Artificial Intelligence: Structures and Strategies for Complex Problem Solving* (2nd edn, Benjamin/Cummings Pub Co 1993).

⁸³⁵ AI Act, Article 3(1).

⁸³⁶ Junfei Qiu and others, ‘A Survey of Machine Learning for Big Data Processing’ (2016) 2016 EURASIP Journal on Advances in Signal Processing 67.

configurations, and parameters used to construct the statistical model; as well as any post-processing (corrections and adjustments of model outputs). ML is often contrasted with traditional software engineering, where the functionality and outcomes are explicitly programmed.⁸³⁷

A subset of ML is 'Neural Networks', which include 'Deep Learning' ('DL') algorithms.⁸³⁸ These networks are constructed to resemble the neural pathways of the human brain, creating artificial synapses for data transmission. Within these networks, 'nodes' act as synthetic neurons. Each node connects to others, possessing specific weights and thresholds, and only passes on information to subsequent layers if its output exceeds this predefined threshold. If not, the node remains dormant.⁸³⁹ DL facilitates 'computational models that are composed of multiple processing layers to learn representations of data with multiple levels of abstraction.'⁸⁴⁰ Notably, DL significantly reduces the need for handcrafted feature engineering, thus diminishing the reliance on domain-specific expertise.⁸⁴¹

Finally, it is crucial to distinguish between AI and automation, though they are often mentioned in tandem. AI represents a specific type of automation involving complex algorithms that enable machine learning. In contrast, 'automation' is a broader term that denotes any system, process, or apparatus set to function

⁸³⁷ Cobbe and Singh (n 828) 4. Natalie A Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' 14 <<https://ssrn.com/abstract=3899991>> accessed 24 March 2024; Meurisch and Mühlhäuser (n 832) 3.

⁸³⁸ Qiu and others (n 836) 3.

⁸³⁹ Daniel J Solove, 'Artificial Intelligence and Privacy' (1 February 2024) 10.

⁸⁴⁰ Yann LeCun, Yoshua Bengio and Geoffrey Hinton, 'Deep Learning' (2015) 521 *Nature* 436.

⁸⁴¹ *ibid.*

autonomously. Not all automation is dependent on data, and not all data-driven automation utilises the algorithms typically associated with AI.⁸⁴²

3. The Challenge of AI Data Harvesting

AI systems pose unique challenges to the principles of Data Protection Law both through the data they utilise and the results they produce. Input-related dilemmas are rooted in data acquisition complexities, encompassing both the contentious practice of scraping – which entails the unauthorised extraction of online data – and more agreeable methods of data procurement. Current regulations largely fail to effectively regulate either approach.⁸⁴³

Data harvesting is not a new issue, but the rise of AI services has intensified the need for more frequent and extensive scraping. This data is primarily harvested via two routes: scraping the internet or repurposing data from customers and users. This insatiable demand for data puts immense pressure on existing privacy laws. In some cases, AI manages to sidestep many privacy protections, while in others, strict enforcement of laws could severely limit data availability, starving AI of the fuel it needs to operate effectively.⁸⁴⁴

ML algorithms, particularly those operating on neural networks and deep learning, feed on vast amounts of data sourced from the internet. A controversial example is Clearview AI, which has created a leading facial recognition tool by amassing billions of photos from various online sources without consent.⁸⁴⁵ This

⁸⁴² Solove, 'Artificial Intelligence and Privacy' (n 839) 10.

⁸⁴³ *ibid* 6–7.

⁸⁴⁴ *ibid* 23.

⁸⁴⁵ Kashmir Hill, *Your Face Belongs to Us: A Secretive Startup's Quest to End Privacy as We Know It* (1st edn, Random House 2023).

amounts to a clear flouting of the established data protection principles including lawful processing, transparency, consent, and purpose limitation. As a result, complaints have been filed with data protection authorities in France, Austria, Italy, Greece, and the United Kingdom. France,⁸⁴⁶ Austria,⁸⁴⁷ and the UK have all found against Clearview AI. However, no fine was issued in Austria,⁸⁴⁸ and the fine issued by the UK's Supervisory Authority, the ICO, has subsequently been overturned on appeal.⁸⁴⁹

In a similar vein, in March 2023 the Italian Data Protection Regulator, *Garante per la protezione dei dati personali* ('GPDP') blocked the use of OpenAI's ChatGPT in Italy citing its mass data scraping operation. The regulator concluded that 'there appears to be no legal basis underlying the massive collection and processing of personal data in order to "train" the algorithms on which the platform relies.'⁸⁵⁰

Current regulatory approaches to scraping publicly available data are inconsistent. The GDPR does not exempt publicly available data from its provisions. In contrast US state privacy laws have shown greater leniency in this

⁸⁴⁶ European Data Protection Board, 'Facial Recognition: The French SA Imposes a Penalty Payment on CLEARVIEW AI | European Data Protection Board' (11 May 2023) <https://edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en> accessed 4 February 2024.

⁸⁴⁷ 'Clearview AI Data Use Deemed Illegal in Austria, However No Fine Issued' <<https://noyb.eu/en/clearview-ai-data-use-deemed-illegal-austria-however-no-fine-issued>> accessed 4 February 2024.

⁸⁴⁸ *ibid.*

⁸⁴⁹ Kashmir Hill, 'Clearview AI Successfully Appeals \$9 Million Fine in the U.K.' *The New York Times* (18 October 2023) <<https://www.nytimes.com/2023/10/18/technology/clearview-ai-privacy-fine-britain.html>> accessed 4 February 2024.

⁸⁵⁰ GPDP (Garante per la protezione dei dati personali), 'Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori' <<https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9870847>> accessed 4 February 2024.

realm. For instance the California Consumer Privacy Act ('CCPA')⁸⁵¹ does not apply to 'publicly available information'. Under the CCPA, this term covers a broad-spectrum including data on government records to information disseminated across various media platforms or shared by individuals without audience restrictions. Similarly, states like Utah⁸⁵² and Virginia⁸⁵³ follow the CCPA's lead with comparable exemptions in their own privacy laws. In contrast Colorado narrows the scope significantly, only exempting governmental data and information that individuals deliberately make public.⁸⁵⁴ Connecticut's stance aligns with Colorado's but extends the exemption to include data that the media circulates.⁸⁵⁵

Beyond scraping, AI also complicates the notion of consensual data collection. Even express consent, as required by the GDPR, does not ensure meaningful understanding of the implications of this processing. The advent of AI adds another layer of complexity, rendering the illusion even more elaborate. In the case of generative AI, applications are frequently undefined. Those utilising generative AI tools may employ them for an array of purposes, ranging from harmless to harmful. In this context, consent morphs into open-ended authorisation, granting *carte blanche* for almost any action. As such, AI makes the fiction of consent even more apparent, as users do not fully comprehend what they are agreeing to in reality.

⁸⁵¹ The California Consumer Privacy Act as Amended November 3, 2020, by initiative Proposition 24. Cal. Civ. Code § 1798.140(v)(2).

⁸⁵² SB 227, Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101(29)(b) (2022).

⁸⁵³ Virginia Consumer Data Protection Act Code § 59.1-571 (2021).

⁸⁵⁴ Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1303, 17(b).

⁸⁵⁵ SB 6, Connecticut Personal Data Privacy and Online Monitoring Act Public Act No. 22-15(2022) § 1(25).

Thus, before conducting our analysis on roles and accountability in AI supply chains we must note that three of the consequences of the *Problem of Control* as identified in Chapter Seven have already been heightened. First, (I) AI services contribute to the undermining of consent as individuals cannot understand the implications of allowing their data to be processed within the AI context. Furthermore, (II) the Data Protection Principles of 'Fairness' and 'Transparency' are undermined through the complexity of AI processing chains. Finally, (III) individual control is hollowed out as personal data is used for undefined and opaque purposes. This reality must guide us as we analyse AI service processing chains and the accountability of actors within them.

4. AI Service Types

AI Services come in two main forms. In the first model (i) AI Service providers offer technical environments and resources to enable customers to conduct their own machine learning operations. In the second more common form (ii) AI Service providers give access to pre-built models that customers can integrate into their applications or use freely. Some services may represent a hybrid of the above, such as those involving prebuilt or partially trained models that can be tailored by the customer through additional ML operations.⁸⁵⁶

This thesis focuses specifically on the second and most prominent form of AI Service. In this regard we follow Cobbe and Singh in using the term AI Services to refer to commercial offerings that allow access to generalised pre-built models as a service.⁸⁵⁷ This process involves customers transmitting input data to providers, who then apply the AI model to these inputs and return the outcomes to the

⁸⁵⁶ Cobbe and Singh (n 828) 4–5.

⁸⁵⁷ *ibid* 4.

customers. A key advantage of AI Services is that they can be easily accessed through cloud platforms, without requiring complex contractual negotiations or high upfront costs.⁸⁵⁸

In reality, the processing chain of a particular application may comprise both AI and non-AI components, potentially sourced from various suppliers. In many cases, an AI component might be a single part of a much larger and intricate chain for a specific application, which could integrate a variety of AI and non-AI Services. Participants in these chains can typically be classified as either 'upstream' or 'downstream', although this categorisation can become less clear when a participant plays multiple roles in the chain. It is important to note that AI Services also have their own supply chains, which might include processes such as data collection and labelling. Companies which utilise AI Services might also offer their own products to their clientele.⁸⁵⁹

5. Actors within AI Processing Chains

AI Service processing typically comprises a minimum of two entities: (a) the AI Service provider and (b) the application client who utilises the service, often referred to as 'customers' or 'tenants' in cloud computing terminology.⁸⁶⁰ We will

⁸⁵⁸ Kornel Lewicki and others, 'Out of Context: Investigating the Bias and Fairness Concerns of "Artificial Intelligence as a Service"', *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2023) <<https://doi.org/10.1145/3544548.3581463>> accessed 24 March 2024.

⁸⁵⁹ See Artem Perepelitsyn and others, 'Technological Stack for Implementation of AI as a Service Based on Hardware Accelerators' [2022] 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT), Dependable Systems, Services and Technologies (DESSERT), 2022 12th International Conference on 1.

⁸⁶⁰ Cobbe, Veale and Singh (n 604); Smuha and others (n 837); Cobbe and Singh (n 828).

follow the language of the AI Act and refer to these as AI providers and AI deployers.⁸⁶¹

To access AI Services, deployers remotely initiate a request to the provider. This requires an initial inputting of data. This data is subsequently analysed by the provider with the resulting analysis returned to the customer. Models are accessed via an Application Programming Interface ('API'), a common tool in software development that facilitates functionality through 'calls' or requests with specified input parameters to the desired service, software, database, or library, subsequently receiving tailored responses. In the context of AI Services, API calls are usually executed over a network, connecting customer applications with the provider's servers. Requests may be transmitted from or through customer equipment. This equipment is not necessarily owned by the customer, instead users often employ other cloud services for deployment support. Alternatively, requests may be transferred directly from the customer's application executing on an active third party's equipment (device or cloud) to the AI provider's server, which then sends the responses. In all instances, the customer's application orchestrates this interaction. The duration of this process largely depends on the nature of the service, often taking milliseconds to complete.⁸⁶²

6. Stages of AI Service Provision

The provision of AI Services involves a continuous flow of information between clients and service providers. This process chain can be dissected into several stages, as enumerated by Cobbe and Singh. Our analysis aims to provide an

⁸⁶¹ See [Chapter Five, Section 2.6.2 AI Act: Accountability Regime](#). These terms will be used interchangeably with providers and deployers throughout this chapter.

⁸⁶² Cobbe and Singh (n 828) 6.

overview of the AI Service process chain and its stages as is represented in *Figure 17* below.

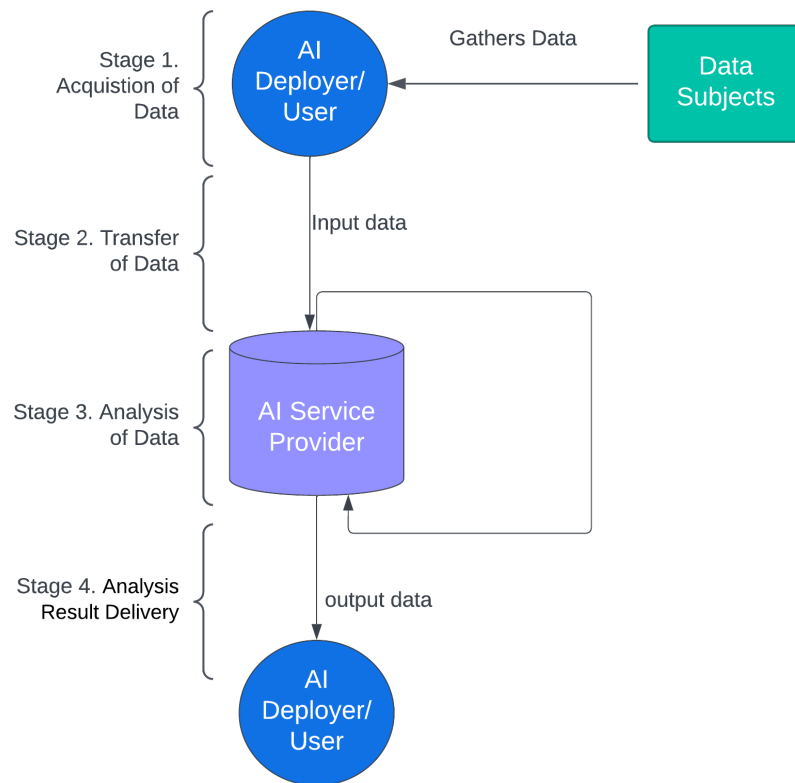


*Figure 17. AI Service Chain Based on Cobbe and Singh*⁸⁶³

6.1 Stage 1. Data Acquisition

The initial phase of the AI Service processing chain is the gathering of input data and any necessary pre-processing conducted by AI deployers. Examples of data acquisition methods include third-party data input to the client's application, collecting usage or behavioural data, monitoring physical spaces using cameras or sensors, or purchasing data from data brokers. It is crucial to note that data collection does not always require storage or aggregation and may include real-time sensor readings or video streams. Additionally, the data collected may not

⁸⁶³ *ibid.*

necessarily encounter any equipment owned or managed by the deployer. Stage One is represented in *Figure 18* below:

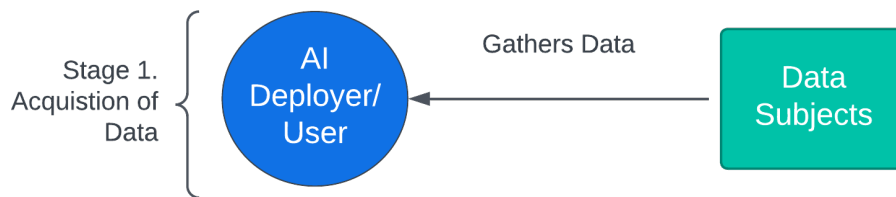


Figure 18. AI Service Processing Chain (Stage 1)

6.2 Stage 2. Data Transfer

The second stage involves deployers transmitting input data to AI providers via a networked API request. This transfer could involve direct transmission of input data from third-party end-users of a deployer application to the service provider, bypassing the client's managed server. Alternatively, the data transfer may originate from the client themselves. Stage Two is represented in *Figure 19* below:

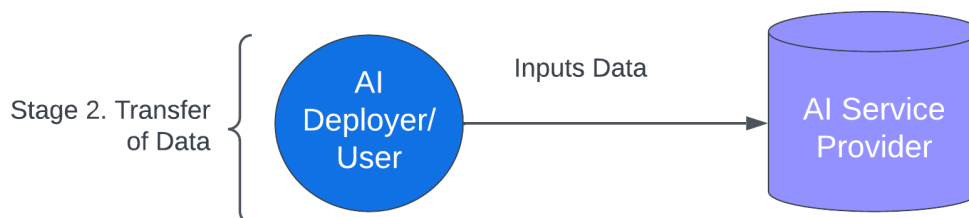


Figure 19. AI Service Processing Chain (Stage 2)

6.3 Stage 3. Data Analysis

In this phase, the service provider employs machine learning algorithms to analyse the input data, leveraging one or more pre-trained models. These models are developed using datasets amassed by the AI provider and are frequently updated to enhance accuracy, rectify identified issues, and achieve other objectives. Stage Three is represented in *Figure 20* below:

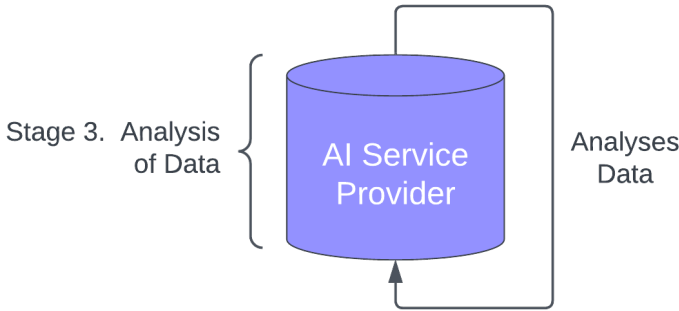


Figure 20. AI Service Processing Chain (Stage 3)

6.4 Stage 4. Data Transfer

The final stage involves AI providers returning the analysis results to clients through API responses over a network. As results are typically sent to the requesting party, it is possible for output data to be directly transferred from the provider to the third-party end-users of the deployer’s application, bypassing their managed equipment. Stage Four is represented in Figure 21 below:

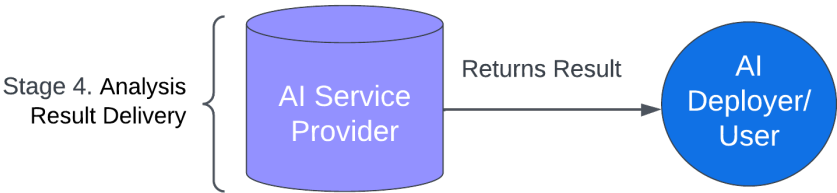


Figure 21. AI Service Processing Chain (Stage 4)

6.5 Cumulative Outcome

The AI Service process chain can be conceptualised as a loop in which data circulates between deployers and providers. Following the completion of the chain, clients may conduct their own analyses or process the service outputs further. The output data enables clients to determine the functionality of their applications. These outputs can be exhibited on a website or app interface, trigger

additional application functionalities, be stored in a database, inform device operations, provide insights into application usage, or be transferred to another party.⁸⁶⁴

providers may engage in additional data processing beyond the primary AI Service

chain to serve various purposes such as monitoring and enhancing service performance, updating models, or examining customer usage for billing or enforcing terms of service.⁸⁶⁵ A common feature of AI Services is the use of deployer input data itself for supplementary processing to refine the models that underpin a provider's core products. This supplementary processing contributes to the improvement of providers' models, subsequently enhancing the functionality of individual customers' applications.⁸⁶⁶ Although specific information about AI provider's usage of customer data is limited, publicly available information indicates that major providers employ supplementary processing using customer data in some form.⁸⁶⁷ A noteworthy example is Google which updated its privacy notice in 2023 to allow for the collection of personal information for AI training purposes.⁸⁶⁸

⁸⁶⁴ *ibid* 6–7.

⁸⁶⁵ Lewicki and others (n 858).

⁸⁶⁶ Cobbe and Singh (n 828) 7.

⁸⁶⁷ Jess Weatherbed, 'Google Admits It's Training AI on Scraped Web Data' (*The Verge*, 5 July 2023) <<https://www.theverge.com/2023/7/5/23784257/google-ai-bard-privacy-policy-train-web-scraping>> accessed 5 February 2024; Matt G Southern, 'Google Updates Privacy Policy To Collect Public Data For AI Training' (*Search Engine Journal*, 3 July 2023) <<https://www.searchenginejournal.com/google-updates-privacy-policy-to-collect-public-data-for-ai-training/490715/>> accessed 5 February 2024.

⁸⁶⁸ [Chapter Nine, Section 3. The Challenge of AI Data Harvesting.](#)

7. Roles and Accountability in AI Services

Despite the complexity of AI models, deployers nevertheless hold a pivotal role in the orchestration of the processing chain. They should be considered to be controllers under the GDPR as they delineate both the objectives and the mechanisms of processing operations. In the case of a client deploying an AI service for image recognition purposes on a cloud platform. The client decides that the rationale of the service is to identify and classify various objects in a series of images (the purpose). Simultaneously, they also determine the specific AI model to be used and the data set upon which the model will be trained (the means). Consequently, the deployer exercises control over the entire AI service processing chain, thereby acting as a data controller.

The role of the AI provider, however, requires greater exploration. Cobbe and Singh maintain that a provider which solely analyses supplied input data and returns these outputs to clients is to be considered a processor like in the case of most cloud services.⁸⁶⁹ In the case of a client deploying an AI for natural language processing tasks. The provider analyses the text data supplied by the customer, performs the required processing, and then delivers the results back to the customer. Additionally, the provider may process customer data for billing purposes, implement security protocols to protect data integrity, and comply with applicable data privacy regulations. In this scenario, the deployer establishes the purpose of the data processing and acts as a controller while the provider operates solely as a processor.

⁸⁶⁹ Cobbe and Singh (n 828) 11. See [Chapter Ten, Section 10.5 Roles under EU Data Protection Law](#).

This simple division of roles over the course of the AI Service Processing chain is represented in *Figure 22* below.

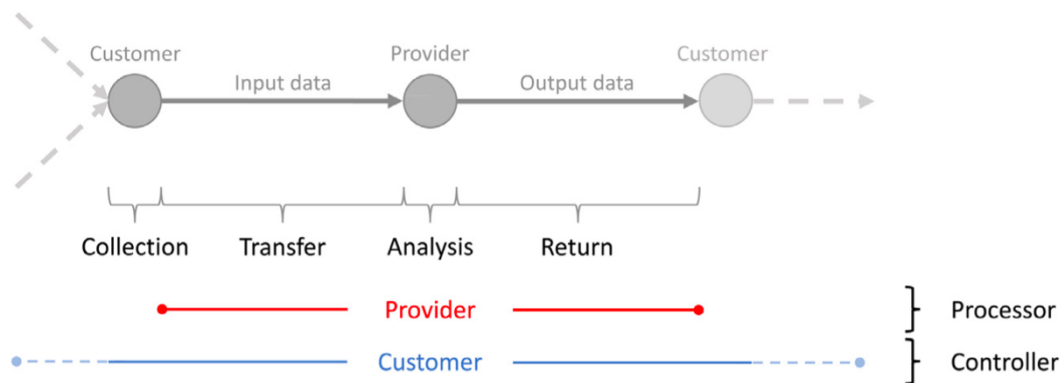


*Figure 22. Simple Division of Roles in AI Service Processing Chain*⁸⁷⁰

However, Cobbe and Singh note that should the AI provider utilise the input or output data for supplementary objectives, such as enhancing or modifying their models or systems, this would constitute a separate act of data processing for which the provider acts as a data controller. In this case the AI provider may be seen as determining the purposes of processing as per the definition of controllership under the GDPR.⁸⁷¹

As such the vital legal question is whether (and to what extent do) AI providers utilise personal data for objectives beyond those imperatives for delivering the desired service to their clients. Auxiliary data processing does not form an integral part of the AI Service processing sequence itself. Instead, it establishes a distinct processing pathway, with purposes designated by the AI provider for its own economic benefit. This separate processing purpose would occur during the transfer and analysis stages of the AI Service processing chain.

⁸⁷⁰ *ibid.* 6.

⁸⁷¹ *ibid.* 13-15.

Per the phase-based processing approach outlined by the CJEU in *Fashion ID*,⁸⁷² even in this case AI providers would not exert influence over the data collection phase, as this task is performed by the client prior to the AI provider's involvement. Likewise, providers would not impact the return stage, as the output data is dispatched to the client at a point in the chain that is logically detached from and subsequent to the provider's auxiliary processing. A provider might conduct auxiliary processing on a copy of the output data to improve its own models after the primary analysis is complete.⁸⁷³

When AI providers engage in supplementary processing, they partake in determining the means of processing during the transfer and analysis stages of the AI Service chain. The processing at these stages then essentially supports dual objectives: firstly, delivering the AI service to the deployer and secondly, enabling the provider's supplementary processing.⁸⁷⁴

Even though the AI Service processing chain and any supplementary processing are distinct, the operations carried out during the transfer and analysis stages of the AI Service sequence contribute to that processing and thus fulfil that secondary purpose. AI providers not only determine the rationale for processing at these stages, but also the method by which this purpose is pursued. Following the principles established in the cases examined in Chapter Six we must conclude that the AI provider exerts sufficient influence over the processing operations to be considered a joint controller.

⁸⁷² See [Chapter Six, Section 7. CJEU Decision in Fashion ID](#).

⁸⁷³ *ibid.*

⁸⁷⁴ Cobbe and Singh (n 828) 9–13. Cobbe, Veale and Singh (n 604) 8–9.

Nonetheless, considering the CJEU's decision in *Fashion ID*, entities cannot act as controllers for processing operations that either precede or follow those for which they determine the purposes or means.⁸⁷⁵ Hence, AI providers do not act as controllers for any processing that occurs after the analysis stage, since the transmission of output data and its subsequent use by clients does not facilitate providers' ancillary processing. Instead, they serve as processors during this return phase.

The assertion that providers who partake in secondary processing act as controllers during specific stages of the AI Service processing sequence could potentially represent a significant deviation from the legal stance observed in traditional cloud services. Such services typically do not involve such supplementary processing, and this potential change arises directly from these processing activities performed by the providers themselves.

This more complex assignment of roles is represented in *Figure 23* below.

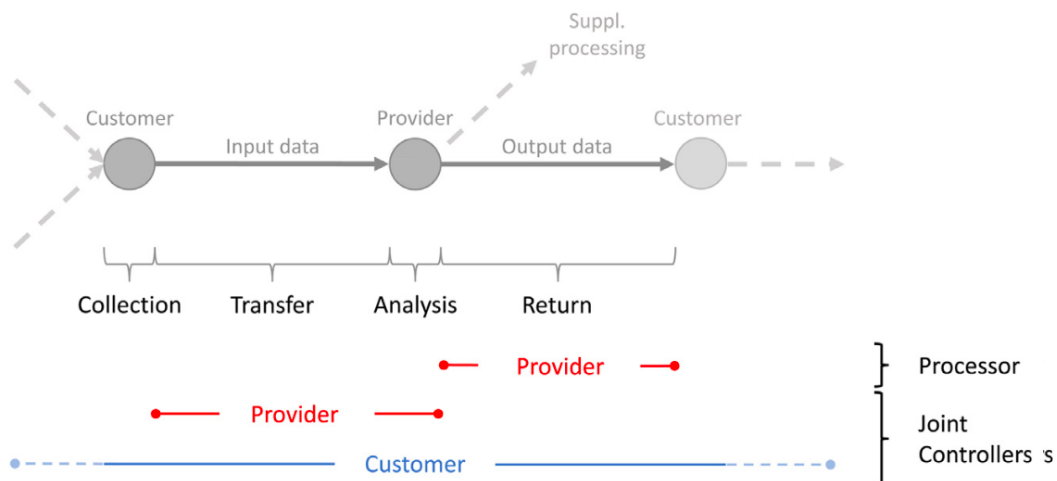


*Figure 23. Division of Roles in Service Processing Chain per Cobbe and Singh*⁸⁷⁶

⁸⁷⁵ See [Chapter Six, Section 7. CJEU Decision in Fashion ID](#).

⁸⁷⁶ Cobbe and Singh (n 828) 14.

While this division of roles heightens the implications of *the Problem of Control* it is nevertheless still a simplified model. In reality, AI Service processing chains are far more complex.

8. The Increasing Complexity of AI Service Processing Chains

Algorithmic supply chains often disperse the production, deployment, and utilisation of AI technologies among numerous stakeholders. These stakeholders' operations are interdependent, impacting one another as they work with a range of both AI and non-AI technology, such as data centres, servers, cloud services, networks, data sources, and content delivery networks, all managed by different entities. The synergy of these actors, each contributing to enable, support or facilitate others, yields a specific result. It is noteworthy that each participant in the supply chain may lack knowledge of others in the sequence. This is more likely if actors are several links apart. However, their role within the processing chain relies on the actions of others both preceding and succeeding their involvement.⁸⁷⁷

In Chapter Seven,⁸⁷⁸ we noted that the CJEU's 'fragmented' or 'phase orientated' approach to data processing does not seem compatible with the framework of the GDPR itself.⁸⁷⁹ This becomes even clearer in the case of AI supply chains where all processing activities are intrinsically interlinked. Each actor performs tasks to meet others' requirements, such as processing specific data or providing the infrastructure needed for application implementation. The mutual reliance among various participants engaged in the creation, execution, and operation of AI systems implies that they cannot be seen as isolated, independent entities. Rather,

⁸⁷⁷ Cobbe, Veale and Singh (n 604) 4.

⁸⁷⁸ See [Chapter Seven, Section 2. Framing and Linguistic Problems](#).

⁸⁷⁹ see Mahieu, van Hoboken and Asghari (n 692) 96.

their roles, relationships, and influence on AI systems are best comprehended within the supply chain context.⁸⁸⁰ The interplay of mutual dependency in algorithmic supply chains, their structural organisation, the significance of each participant, and the propagation of issues, are crucial factors when considering algorithmic responsibility.

An indicative example of a typical AI supply chain featuring multiple actors is represented in *Figure 24* below. In this scenario an application developer (1) sends input data to an AI service (2). Another AI Service (3) plays multiple key roles within the supply chain providing infrastructure support (3A) for an AI service offered by (2), providing an AI service (3B) to a cloud service provider (4); and providing infrastructure (3C) for application deployment. This work is complemented by entities (5) and (6).

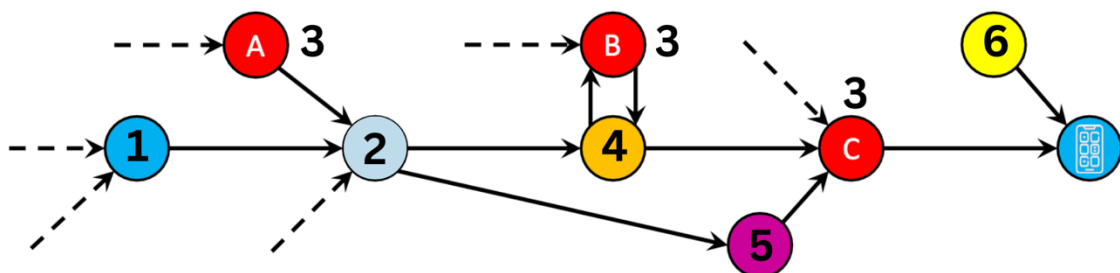


*Figure 24. Indicative Complex AI Supply Chain*⁸⁸¹

Allocating roles and responsibility to a scenario such as that presented in *Figure 24* demands a great degree of intricacy. The controller-based model at the core of Data Protection Law can acknowledge multiple actors involved in processing chains. Yet there is no intuitive way to map the roles of controller, joint-controller,

⁸⁸⁰ Cobbe, Veale and Singh (n 903) Altered for more clarity.

⁸⁸¹ Based on Cobbe, Veale and Singh. *ibid.*

and processor to many AI Service chains. As such AI Services magnify the challenge to legal certainty which results from the *Problem of Control*.

As noted above, AI Service deployers are likely classified as data controllers, becoming the primary party responsible for compliance and accountability. Conversely, providers may be considered processors, fulfilling a subsidiary role, acting solely under a controller's instruction, and carrying minimal obligations. However, this distribution of legal roles and responsibilities does not accurately depict the real dependencies and power dynamics between AI providers and their customers.

The AI providers who exert control over their technologies, frequently play a pivotal role in supply chains and are of systemic importance. They often present their customers with inflexible contracts and, for the most part, determine AI-driven functionality in customers' applications through their production processes. In contrast, their customers are often small companies without AI expertise, which usually do not have access to the provider's systems or control over them, nor knowledge of their operations.⁸⁸²

Even in instances where providers are likely controllers for service aspects—such as using customer data for service improvement—they often aim to downplay their responsibility by declaring themselves as processors in their service agreements. The CJEU has consistently ruled that factual circumstances take precedence over contractual arrangements. Additionally, regulators have also challenged the claimed assignments of legal roles in other types of data-driven

⁸⁸² *ibid* 5–7.

supply chains. Nevertheless, contesting providers' claims would necessitate litigation or regulatory investigation.

Furthermore, considering that joint controllers must agree on the division of controllers' duties and responsibilities among themselves, it is unclear how joint controllership can function when the concerned parties may not even be aware of each other or have any direct relationship.

The stance of the CNIL and Information Commissioner of Slovenia⁸⁸³ in extending the role of joint controllership to cloud service providers is thus a valuable precedent in this case. If other Supervisory Authorities and the Courts follow in this direction, then greater responsibility may be consistently placed in the hands of those entities which are best resourced to deal with the complexities involved.

9. Complementing and Competing Obligations

Beyond the complexity already presented it is entirely possible for two entities to hold contrasting obligations under the AI Act as well as the GDPR. As is standard practice a small business might be forced to agree to the role of data controller in order to use the services of a multinational software provider. Under the GDPR the small business will take on the major responsibilities and liabilities. However, should the service in question be covered by the AI Act, the small business will assume the less onerous obligations of an AI deployer as opposed to the multinational software provider which will hold the role of AI provider.

As such the actors will be party to two complementing and competing relationships of control as illustrated in *Figure 25* and *Figure 26* below:

⁸⁸³ See [Chapter Eight, Section 6](#).

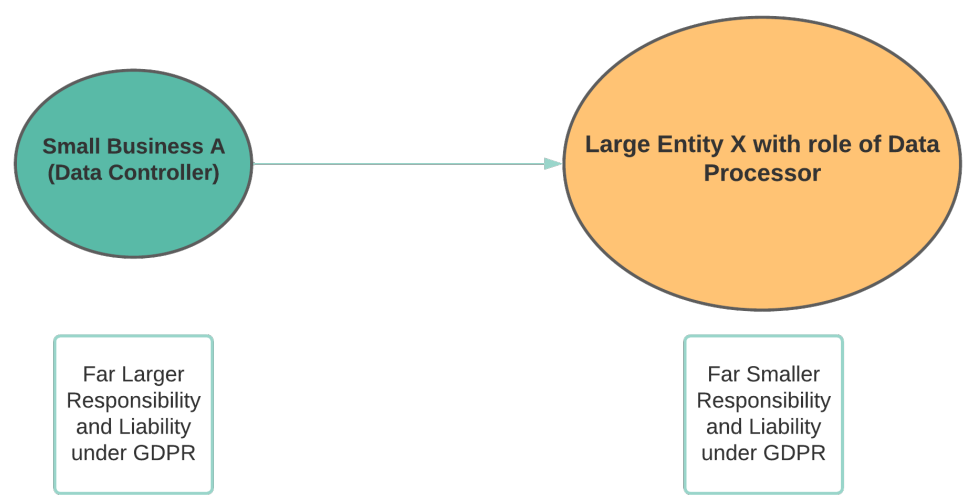


Figure 25. Complementing and Competing Relationship under AI Act (Part 1)

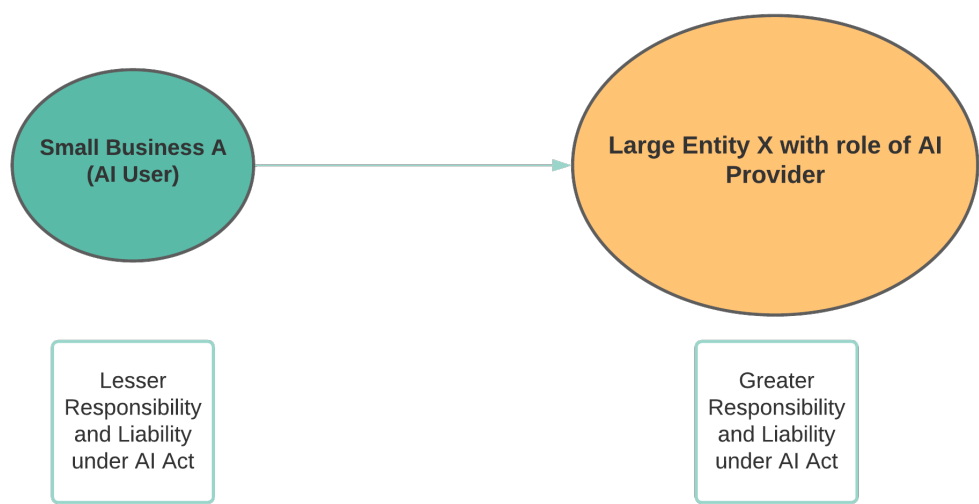


Figure 26. Complementing and Competing Relationship under AI Act (Part 2)

However, we may question the applicability of even the AI Act to account for the complexity of AI supply chains. It is clear that a simplistic categorisation of AI provider and deployer does not encapsulate the interconnectedness and dynamism of these processing chains, where the responsibilities of creation, deployment, and utilisation are dispersed amongst various entities.⁸⁸⁴ Under such

⁸⁸⁴ Cobbe, Veale and Singh (n 604) 8.

conditions, the AI Act might impose obligations on entities far removed from the production process to guarantee adherence to legal prerequisites related to training and testing, accountability, and risk management in AI production. This could encourage entities that are inherently incapable of assuring compliance to feign their ability to do so.⁸⁸⁵ Moreover, regulatory frameworks that hold downstream supply chain entities accountable for design and development may fail to adequately regulate those who bear factual responsibility for production and who gain financially from potentially illegal application uses.⁸⁸⁶

The idea of the ‘accountability horizon’⁸⁸⁷ may serve as a useful framing device for understanding the problem of allocating and sharing responsibility. This term refers to the furthest extent of visibility or understanding that an actor possesses. It is contingent on the specific actor and the supply chain involved. Generally, entities within the supply chain will be cognizant of their direct interactions, and perhaps of the subsequent interactions of other closely placed actors. However, they might struggle to comprehend the intricacies of data flows and relationships beyond these proximate stages.⁸⁸⁸

Furthermore, the division of responsibilities for creation and deployment amongst multiple actors necessitates that each party possesses only a fragment of the whole chain, even if they are aware of the entities that exist both upstream and downstream from them. As a consequence, AI providers, who are in charge of the production phase, might lack awareness of the contexts and application scenarios

⁸⁸⁵ Veale and Zuiderveen Borgesius (n 523).

⁸⁸⁶ Cobbe, Veale and Singh (n 604) 8–9.

⁸⁸⁷ *ibid.*

⁸⁸⁸ Singh, Cobbe and Norval (n 731). Cobbe, Norval and Singh (n 603).

downstream of their position.⁸⁸⁹ Conversely, those tasked with the deployment and utilisation of AI typically do not have access to models or detailed information about their specification, training, testing, and verification. This situation often leaves these actors with a limited understanding of the capabilities and constraints of the systems they are using.

10. Conclusion

Nowhere are the limits of the accountability framework of Data Protection Law challenged as much as in the case of AI Services. Indeed, AI supply chains are characterised by multiple actors who jointly realise the technology's outputs and functionality. Allocating roles and responsibility in the type of recurring complex AI supply chains presented in this chapter is an immensely difficult task.

The cumulative result is an amplification of five of the key consequences of *the Problem of Control* identified in Chapter Seven:

1. The weakening of legal certainty in data processing relationships as actors, their responsibilities, and liabilities are even more difficult to determine in AI supply chains.
2. The undermining of consent as a lawful basis for processing personal data, as individuals cannot understand the implications of allowing their data to be processed within the AI context.
3. The violation of the Data Protection Principles of 'Fairness' and 'Transparency' through the unique complexity of data processing relationships and power differentials in AI supply chains.

⁸⁸⁹ Lewicki and others (n 858).

4. The obscuring of data commodification as a societal issue as key AI providers are able to leverage their market position to use and reuse personal data in unknown ways. This is all the more concerning for large actors which have already established an ecosystem of data commodification.
5. The hollowing out of the individual control which is central to the right to data protection as personal data is used for undefined and incomprehensible purposes in AI training models.

We thus find ourselves in agreement with Solove who claims:

The rise of AI has made it emphatically clear that the individual control model is doomed. AI is far too vast and complicated for individuals to understand and to assess the impact on their privacy. Instead of trying to provide individuals with control over their data, the law should bring the collection and use of data under control.⁸⁹⁰

In rectifying these problems attention should be given to dominant providers, which have become increasingly integrated into the majority of AI Services. Moreover, if governance and accountability mechanisms aim to hold those responsible for developing, deploying, and using AI technologies to account for their functions and effects, the dynamism of supply chains must be urgently addressed.

⁸⁹⁰ Solove, 'Artificial Intelligence and Privacy' (n 839) 20.

PART III: RECOMMENDATIONS AND CONCLUSION

Chapter Ten: Addressing the Problem of Control

1. Introduction

In Part II we set out *the Problem of Control*. Chapter Six outlined the history of the controller based accountability model and how its boundaries have been stretched through the case law of the CJEU. Six concerns emanating from the CJEU's rulings on the boundaries of controllership were outlined and explored in Chapter Seven. Thereafter the impacts of the *Problem of Control* were assessed through two illustrative examples in Chapters Eight and Nine. We have seen that the collective effect of these outcomes has compromised the court's original objective of providing 'complete and effective' protection, undermining the very goals that inspired its initial rulings.

In this chapter we review potential solutions to the *Problem of Control*. Four recommendations as found in literature are presented: (I) extending responsibilities for processors; (II) applying a non-controller-based accountability model; (III) moving to a *de minimis* threshold for control in the form of orchestration; and (IV) allowing flexibility in judicial and regulatory action.

Finally, we offer one immediate mitigation for *the Problem of Control* by providing a defined taxonomy of data processing relationships. Smaller entities and individual users currently face the task of unravelling intricate data processing operations, frequently depending on the guidance of specialised consultants. This dependence on expertise can be perceived as a deterrent, akin to a regressive tax, imposing a high cost of regulatory compliance that potentially hampers

innovation. Such a barrier undermines the key legislative objective of fostering an inclusive digital market. By introducing a well-articulated taxonomy that delineates the various roles in data processing relationships, we can facilitate compliance efforts for those bound by the GDPR.

Furthermore, a clear model of roles within typical personal data processing scenarios can serve a broad spectrum of stakeholders, delivering significant practical benefits to researchers, regulatory bodies, technology developers, SMEs, and private individuals.

2. Extended Responsibilities for Processors

Blume⁸⁹¹ and Van Alsenoy⁸⁹² both argue for greater responsibilities to be placed upon processors. For the latter this specifically focuses upon the requirement for Data Protection by Design and Default under the GDPR.⁸⁹³ In this way the provider of a processing service (typically the processor) would bear the responsibility for structuring its services and capabilities in a manner that fosters adherence to data protection norms. Meanwhile, the customer of the processing service (typically the controller) would be tasked with tailoring these services and features suitably. Additionally, regulators may mandate that providers of processing services validate their conformity with the Principle of Data Protection by Design and Default.

In contrast, Blume argues for not merely the application of just Data Protection by Design and Default obligations, but responsibility for all the principles of Data

⁸⁹¹ Blume (n 693).

⁸⁹² van Alsenoy (n 127) 642.

⁸⁹³ GDPR, Article 25.

Protection Law. It is contended that this is especially beneficial in resolving the issue of knowledge and capacity differentials in cloud service providers. While a change in obligations for processors may be in order, however, both Blume and Van Alsenoy fail to account for power differentials. Instead, we may look for more targeted solutions by not focusing on all processors, but rather on larger actors in particular.

In considering these power differentials it is worth bearing in mind obligations found under the other legal instruments cited in Chapter Five.⁸⁹⁴ The AI Act provides less onerous obligations for AI deployers as opposed to AI providers. However, dividing these roles is not always clear in reality. As has been noted in Chapter Nine a simplistic categorization of provider and deployer does not encapsulate the interconnectedness and dynamism of AI supply chains, where the responsibilities of creation, deployment, and utilisation are dispersed amongst various entities. Under such conditions, the AI Act might impose obligations on entities far removed from the production process.

A more useful framework may be found in the Digital Service Act ('DSA') and Digital Markets Act ('DMA'). Both legal instruments place added obligations and restrictions on the actions of systemically large actors. The DSA places higher obligations upon Very Large Online Platforms ('VLOPs') – Entities with 45 million active monthly users in the EU. While the DMA targets large scale online platforms identified as 'gatekeepers.'⁸⁹⁵ The criteria for gatekeepers are established under Article 3 (1) of the DMA.

1. An undertaking shall be designated as a gatekeeper if:

⁸⁹⁴ See [Chapter Five, Section 2. Legislative Expansion](#).

⁸⁹⁵ Van Cleynenbreuge (n 500). See also Gutermuth, Italianer and Thiry (n 500).

- (a) it has a significant impact on the internal market.
- (b) it provides a core platform service which is an important gateway for business users to reach end users; and
- (c) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.

Utilising these terms and creating a regime with higher data protection obligations for systemically large and important actors may allow for a mitigation of *the Problem of Control*.

In its July 2023 ruling in *Meta Platforms and Others*,⁸⁹⁶ the CJEU extended the power of a competition authority within a member state to examine whether an undertaking's conduct complies with rules other than those relating to competition law. Importantly this included the rules on the protection of personal data laid down by the GDPR in the context of the abuse of a 'dominant position' in a particular market.

Moreover, as discussed in Chapter Five,⁸⁹⁷ we have also seen the potential for complementary enforcement mechanisms through the European Commission's investigation into Meta's change of terms and conditions. This inquiry followed successful challenges to Meta's legal basis for processing personal data for personalised advertising. In response to these challenges, Meta introduced a novel 'pay or okay' subscription model in November 2023 for users in the EEA. This model presents users with a choice: continue using Meta's services free of charge while consenting to personalised advertising, or opt for a subscription that excludes the use of personal data for ad targeting. This development has prompted multifaceted regulatory responses. The privacy advocacy group NOYB

⁸⁹⁶ Case C-252/21 *Meta Platforms and Others* (General terms of use of a social network) [2023] EU:C:2023:537.

⁸⁹⁷ See [Chapter Five, Section 2.7 Legislative Expansion: Conclusion](#).

(None of Your Business) has filed a GDPR complaint against Meta's new model.⁸⁹⁸ Concurrently, the European Commission has initiated an investigation under the Digital Markets Act to scrutinise this approach.⁸⁹⁹ This complementary approach may in time allow for a more complete linking between power relationships and data protection responsibilities. However, this is still a patchwork solution and may in fact create greater confusion in the short-term. The potential for regulatory complexity to stifle both innovation and undermine certainty over actors' responsibilities has been emphasised in the Draghi report on 'The Future of European Competitiveness' published in September 2024.⁹⁰⁰ Thus we may accept this as a direction with the potential to alleviate *the Problem of Control*. Nonetheless, we must take care not to replace one complexity with another in the name of clarity.

3. Non-Controller Based Accountability

Wong⁹⁰¹ argues for the move towards a non-controller-based accountability framework as an alternative to the system of EU Data Protection Law. Defending this argument Wong notes the examples of Canada,⁹⁰² New Zealand,⁹⁰³ and Singapore.⁹⁰⁴ All of these have implemented data protection systems that do not use the controller-centric responsibility model. Canada and Singapore use

⁸⁹⁸ 'Noyb Files GDPR Complaint against Meta over "Pay or Okay"' (n 537).

⁸⁹⁹ European Commission, 'Commission Sends Preliminary Findings to Meta over Its "Pay or Consent" Model for Breach of the Digital Markets Act.' (n 538).

⁹⁰⁰ European Commission, 'The Future of European Competitiveness. Part A | A Competitiveness Strategy for Europe'.

⁹⁰¹ Wong (n 11).

⁹⁰² Personal Information Protection and Electronic Documents Act ('PIPEDA') S.C. 2000, c. 5 (Canada).

⁹⁰³ Privacy Act 2020, Version as of 6 December 2023 (New Zealand).

⁹⁰⁴ Personal Data Protection Act 2012, ('PDPA') 2020 Revised Edition (Singapore).

'organisation', while New Zealand utilises 'agency'. Although at first glance these designations might appear analogous to the notion of a controller, they do not in fact hold substantive equivalence. This is because they do not perform the function of 'allocating responsibility'. Instead, each label is in fact a shorthand encompassing all entities that fall within the scope of their respective data protection regimes. To illustrate, under the New Zealand Privacy Act, 'agency' signifies 'any person or body of persons, corporate or unincorporate, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a department.' Similarly, the term 'organisation' as used under the Singapore PDPA covers 'any individual, company, association or body of persons, corporate or unincorporated'.

Wong maintains that the advantages of these systems are threefold. Firstly, (i) non-controller-centric responsibility structures sidestep issues of complexity as they do not rely on the difficult idea of a controller to delegate responsibilities. Therefore, in such systems, there is no requirement to pinpoint who 'determines the purposes and means of the processing of personal data'. Rather, the attribution of responsibility is more streamlined as specific data protection duties are linked to particular kinds of data processing operations.⁹⁰⁵

Furthermore, (ii) non-controller-based models avoid problems of accountability allocation. This is because they do not depend on the concept of joint controllership, thereby relieving collaborating entities involved in data processing from the need to distribute responsibility among themselves. These non-controller-centric systems are typically unconcerned with whether and how entities are cooperatively processing personal data, as obligations are individually

⁹⁰⁵ Wong (n 11) 385–386.

imposed. For instance, if Entity A shares personal data with Entity B, Entity A will be obligated by the rules concerning its disclosure of the personal data, while separately, Entity B will be obligated by rules relating to the collection of the personal data. Each actor must only be concerned with the specific obligations that are individually imposed on it by the applicable data protection framework.⁹⁰⁶

Finally, (iii) non-controller systems provide a more targeted attribution of responsibility. Data protection obligations are not collectively imposed on controllers; instead, various sets of data protection obligations are allocated based on the type of processing operation involved. This targeted attribution of responsibility contributes to ensuring that the entity assigned an obligation is actually capable of fulfilling it. For instance, within non-controller systems, the obligation to provide access to personal data and the obligation to correct inaccurate personal data are only imposed on the entity who actually holds, possesses, or controls that personal data. This entity is in the best position to fulfil these access and rectification obligations.⁹⁰⁷

Implementing such a model would necessitate significant amendments to the GDPR. However, it may be possible to avoid a wholesale rewriting of Data Protection Law. For instance, Van Alsenoy⁹⁰⁸ notes that it is entirely possible to rewrite the liability provisions under Article 82 of the GDPR without reference to a controller or processor. In the GDPR's rendering the first three provisions of the Article 82 reads as follows:

⁹⁰⁶ *ibid.*

⁹⁰⁷ *ibid.*

⁹⁰⁸ van Alsenoy (n 182) 640 (emphasis found in the original).

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
2. **Any controller** involved in processing shall be liable for the damage caused by processing which infringes this Regulation. **A processor** shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed **to processors** or where it has acted outside or contrary to lawful instructions **of the controller**.
3. **A controller or processor** shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

A revised version is posited by Van Alsenoy which would read:

1. Any person who has suffered material or immaterial damage as a result of an infringement of the Regulation shall have the right to receive compensation...
2. Every party involved in the processing shall be liable for the damaged caused by his own processing activities as well as processing undertaken by others on its behalf, taking into account the following limitations:
 - (a) a party who exclusively processes the data in accordance with the instructions of another party and on his behalf shall only be liable insofar as the damages are a result of a failure to comply with articles [list of provisions otherwise relevant to processors].
 - (b) **Any party** involved in the processing may be exempted from liability insofar as he can prove that the damages are the result of an event which cannot in any way be attributed to him.

Although amendments would be required, these may not be as drastic as first anticipated. Nevertheless, we must be clear that this approach calls for a complete

overhaul of Data Protection Law's accountability regime necessitating considerable legislative will and cohesive action. As such this solution may be seen as an unlikely path for the moment.

4. Moving to a Model of Control as Orchestration

Finck provides another solution, calling for a new test in the form of a 'de minimis threshold of control' to be required for an actor to be rendered a controller under the GDPR.⁹⁰⁹ Finck maintains that such a requirement is in fact consistent with the language within Articles 24 and 25 of the GDPR which imply that an entity denoted as a data *controller* must possess tangible *control* over the processing of personal data. Moreover, the historical analysis in Chapter Six of this thesis demonstrates that to earn the designation of a data 'controller', a party should have actual power over the data itself and the means utilised for its processing.⁹¹⁰

To combat perpetually extending circles of controllers, case law should harken back to the fundamental concept of the 'controller' and institute an exception for parties lacking significant influence over data processing. This can be achieved by setting a higher bar for determining which entities hold influence over the means and purposes of processing.⁹¹¹

This idea is already clear in the CJEU decision of *Jehovan todistajat* where appeal is made to a conceptual ideal of controllership as defined through an orchestrating role in the processing of data. However, the court's approach has been inconsistent at best. Indeed, such reasoning is not possible in *Fashion ID*, where the actors

⁹⁰⁹ Finck (n 338) 346–347.

⁹¹⁰ See [Chapter Six, Section 2. Controller Based Accountability: Historical Origins](#).

⁹¹¹ *ibid*.

which have been added as joint controllers render little influence over the processing in question. Moreover, in its most recent ruling on controllership in *IAB Europe* the CJEU reaffirmed the orchestration conception of controllership after having almost completely negated it in its previous decision just two months earlier in *Belgian State*. Indeed, through *Belgian State*, controllership has been disconnected from any notion of determination or *control*. We are thus forced to grapple with the role of orchestration as a decisive threshold for accountability

Future case law should establish a minimal threshold of orchestrating influence over the processing necessary to be eligible as a data controller. According to this criterion, only entities that dictate the purposes and means beyond merely selecting a platform or service and facilitating someone else's processing should be considered controllers.⁹¹² This proposal aligns more closely with the GDPR protective rationale as it would bolster transparency and legal certainty, thus enhancing accountability. Moreover, it more accurately reflects the realities of political economy. Data Protection Law imposes numerous risk-management mechanisms aiming to curtail the inherent hazards that surface when personal data is processed. These risks should be imposed solely on those who possess actual decision-making power over the processing of personal data and who derive its primary fruit.

This approach would require a change in judicial approach and a revision of the scope of joint-controllership applied in earlier cases including *Fashion ID* and *Belgian State*. However, many of the key principles of the Court's jurisprudence on controllership could still be maintained within the orchestration framework. This approach may be the clearest path towards addressing *the Problem of Control*,

⁹¹² *ibid.*

however it relies upon either judicial inclination to undo its past work, or concerted legislative action to curtail the scope of controllership.

5. Flexibility in Judicial and Regulatory Action

A further approach to dealing with unreasonable and excessive legal consequences resulting from the broad application of data protection law could be mitigated through a flexible interpretation and enforcement of the law, while still ensuring robust and comprehensive protection for individuals. Such an approach is referred to as ‘site-level flexibility’ and is found in pragmatic judicial rulings of the type seen in *GC and Others* discussed in Chapter Seven.⁹¹³ In *GC*, the Court faced a critical decision: either declare Google Search’s data processing—and by extension its business model—as incompatible with the law, or find a way to accommodate it. The Court opted for the latter, transforming what was meant to be an *ex ante* prohibition into an *ex post* right. This approach represents a tailored interpretation of the law, crafted specifically to accommodate a business model that otherwise would not align with the legal framework.⁹¹⁴

An alternative approach involves regulatory discretion in complaint handling and enforcement. While risk-based regulation has gained traction in other fields, allowing regulators to prioritise resources based on perceived threats, its application in data protection is limited.⁹¹⁵ The GDPR mandates that regulators must handle all complaints ‘to the extent appropriate,’ suggesting some discretion in the depth of investigation but not in whether to address complaints at all. This

⁹¹³ See [Chapter Seven, Section 3. Diminishing Legal Certainty](#).

⁹¹⁴ Lynskey, ‘Complete and Effective Data Protection’ (n 32) 336.

⁹¹⁵ Karen Yeung and Lee A Bygrave, ‘Demystifying the Modernized European Data Protection Regime: Cross-disciplinary Insights from Legal and Regulatory Governance Scholarship’ (2022) 16 *Regulation & Governance* 137, 146.

is reinforced by a data subject's right to judicial remedy if regulators fail to handle complaints or provide timely updates.

The concept of responsive regulation, as proposed by Ayres and Braithwaite, suggests a tiered approach to enforcement, starting with persuasion and escalating to penalties if necessary.⁹¹⁶ While this aligns with the idea of 'complete independence' granted to data protection authorities under the EU Charter, it may conflict with certain GDPR provisions. The regulation seems to favour a more direct approach to sanctions, with administrative fines intended to be 'effective, proportionate and dissuasive' for each infringement.⁹¹⁷

The GDPR's language is consistent with formal corrective action for significant infringements, limiting the scope for informal or amicable resolutions, especially in transnational cases. This is further supported by the limited mentions of amicable dispute resolution in the GDPR text. Indeed, such dispute resolution appears just once in the recitals, and even then, it is limited to disputes that are localised in nature or effect.⁹¹⁸ Moreover, the legal framework appears to create a gap in accountability where complaints are handled but no legally binding decision is issued. This suggests that the legislators did not anticipate widespread flexible enforcement of the rules. Nevertheless the role of regulatory discretion has been affirmed shortly before the completion of this thesis. On 26 September 2024 the CJEU issued its ruling in *Land Hessen*⁹¹⁹ finding that a Supervisory Authority is not mandated to use its corrective powers in every instance of non-compliance

⁹¹⁶ Ian Ayres and John Braithwaite, 'Responsive Regulation: Transcending the Deregulation Debate' in Martin Lodge, Edward C Page and Steven J Balla (eds), *The Oxford Handbook of Classics in Public Policy and Administration The Oxford Handbook of Classics in Public Policy and Administration*, vol 1 (Oxford University Press 2016) 35.

⁹¹⁷ The GDPR, Article 83(1).

⁹¹⁸ *ibid.* Recital 131.

⁹¹⁹ *Case C-768/21 - TR v Land Hessen [2024] EU:C:2024:785.*

with Data protection Law. Moreover, the Court maintained that Supervisory Authorities are not required to impose financial penalties for all infractions. Thus there is clear judicial leeway for flexibility on the part of Regulators.

Constraints on regulatory discretion raise broader normative questions about the balance between strict rule application and practical enforcement. On one hand, a rigid enforcement approach ensures consistency and may strengthen the deterrent effect of the law. On the other, it might lead to an overwhelming number of cases and potentially disproportionate outcomes in minor infringements.⁹²⁰

However, the practical reality is that such elasticity brings its own set of challenges that cannot be overlooked. Indeed flexible interpretation and enforcement of Data Protection Law have raised concerns about its effectiveness and long-term implications. The CJEU's approach in cases like *GC*, where it accommodated Google Search's business model by reinterpreting prohibitions as ex post rights, demonstrates the complex interplay between law and technology. While this provides a 'safety valve' against disproportionate extension of obligations, it also risks creating incentives for technological designs that circumvent legal compliance.⁹²¹ The Court's approach in *GC* suggests that technologies designed in ways that make data protection compliance impossible may avoid legal scrutiny. This approach could encourage the 'move fast and break things' model of technological development, potentially undermining the comprehensive application of data protection guarantees. Questions arise about how this

⁹²⁰ Lynskey, 'Complete and Effective Data Protection' (n 32) 335.

⁹²¹ Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022) 141.

interpretation might apply to emerging technologies like blockchain or AI systems such as ChatGPT.⁹²²

The effectiveness of flexible enforcement is also uncertain. While the success of Data Protection Law should not be measured solely by fines issued, evidence suggests that European regulators have made limited use of their full range of corrective powers.⁹²³ The lack of empirical evidence on whether flexible enforcement leads to more effective protection raises concerns, especially in cases where formal enforcement drops significantly in favour of informal interactions between regulators and the regulated community .

For instance, Lynskey highlights the fact that the UK's Information Commissioner's Office handled 40,000 complaints in 2021-2022 but issued only four fines totalling £663,000, with no other enforcement notices or penalties.⁹²⁴ This approach, particularly in cases involving significant privacy breaches, raises questions about whether informal enforcement adequately protects fundamental rights.⁹²⁵

Moreover, a policy of flexible interpretation and application of Data Protection Law raises significant concerns over compatibility with core legal principles, particularly in the context of fundamental rights protection. This approach challenges the law's internal morality, which requires generality, public

⁹²² Lynskey, 'Complete and Effective Data Protection' (n 32) 336.

⁹²³ European Data Protection Board (EDPB), 'Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities' (n 742) 14.

⁹²⁴ Information Commissioner's Office (UK), 'Information Commissioner's Annual Report and Financial Statements 2021-22 July 2022 HC 392' 33 <<https://ico.org.uk/media/about-the-ico/documents/4021039/ico-annual-report-2021-22.pdf>> accessed 28 September 2024.

⁹²⁵ Lynskey, 'Complete and Effective Data Protection' (n 32) 337–338.

promulgation, and congruence between official action and declared rules.⁹²⁶ In data protection, where foreseeability is crucial for justifying any interference with fundamental rights and fostering public trust, this flexibility becomes particularly problematic. While the data protection framework has never been entirely inflexible, given the principle of proportionality and risk-management obligations, the introduction of the ‘responsibilities formula’ by the CJEU marks a qualitative shift. This formula, which calibrates the law's application to the powers of the data controller, introduces uncertainty about how rules apply to different actors. Quelle proposes addressing the ambiguity in the responsibilities formula by interpreting it through the lens of risk assessment.⁹²⁷ However, Lynskey contends that while this approach might strengthen the formula's connection to the GDPR in certain contexts, it falls short when applied to provisions that do not explicitly reference risk. Instead, this partial solution could further exacerbate the unpredictability of the regime's application, potentially undermining not only its efficacy but also its transparency and predictability. This critique highlights the challenges in reconciling flexible interpretations with the need for legal certainty in data protection regulation. Unlike other scalable elements of the regime, such as risk-management requirements, this formula lacks clear guidance or legislative footing.⁹²⁸

While flexibility in Data Protection Law may offer some benefits, it also presents significant challenges to legal certainty, equal application, and effective protection of fundamental rights. Striking a balance between adaptability and robust enforcement remains a critical challenge for the future of data protection

⁹²⁶ Per Fuller (n 726).

⁹²⁷ Claudia Quelle, ‘GC and Others v CNIL on the Responsibility of Search Engine Operators for Referring to Sensitive Data: The End of “Right to Be Forgotten” Balancing?’ (2019) 5 *European Data Protection Law Review* 438.

⁹²⁸ Lynskey, ‘Complete and Effective Data Protection’ (n 32) 339.

regulation. As such it would require far greater exploration of judicial and regulatory flexibility to ensure legal certainty and consistent rights protection in this approach. The one key advantage of this approach is that much of this clarity could be provided by the EDPB itself without requiring more demanding legislative change. As such site-level flexibility remains an avenue allowing for some mitigation without allowing for complete clarity.

6. Towards a Taxonomy of Control in Data Processing Relationships

Beyond the solutions offered already, this chapter outlines a taxonomy of data processing relationships. This catalogue may, in and of itself, provide some mitigation to *the Problem of Control*. Understanding relationships of control may have significant practical impacts for researchers, regulators, technology developers, SMEs, and private individuals. Having clearly defined models of all parties present in common data sharing scenarios may also benefit those caught within a complex network of data processing relationships.

Specifically, through being able to consult a taxonomy of data control relationships those trying to comply with their responsibilities under the GDPR will be better able to do so. Indeed, absent clear models and use cases for data relationships, small businesses and even private individuals are often forced to either navigate intricate legal and factual relationships for themselves or are left to rely upon the services of professional consultants. This reality amounts to a regressive form of taxation whereby the entry cost of compliance for all businesses dealing with data would be sufficiently high as to stifle innovation for all but the largest firms.

This taxonomy may assist in lowering the transparency burdens for compliance and thus level the knowledge tax in effect. What is more, controllers carrying out DPIA as mandated by the GDPR will have predefined models which can be used to fully understand risks.⁹²⁹ Even the innovative uses of technology which require DPIAs often also rely upon prebuilt tools for data hosting, information gathering, and user interface. The challenges emerging from these tools and their specific data control relationships are recurrent, even when the result of a system is unique. Moreover, by developing a taxonomy of use cases for data sharing relationships it will also be possible to cultivate a library of appropriate processes and safeguards to better protect individual rights and freedoms.

7. The Taxonomy

7.1 Archetypal Models

Olsen and Mahler propose a classification scheme to represent the diverse relationships possible between controllers and processors.⁹³⁰ Their model is presented in *Figure 27* below.

⁹²⁹ See [Chapter Five, Section 5.10 Risk Assessment](#).

⁹³⁰ Thomas Olsen and Tobias Mahler, 'Identity Management and Data Protection Law: Risk, Responsibility and Compliance in "Circles of Trust" – Part II' (2007) 23 Computer Law & Security Review 415. See also van Alsenoy (n 127) 78.

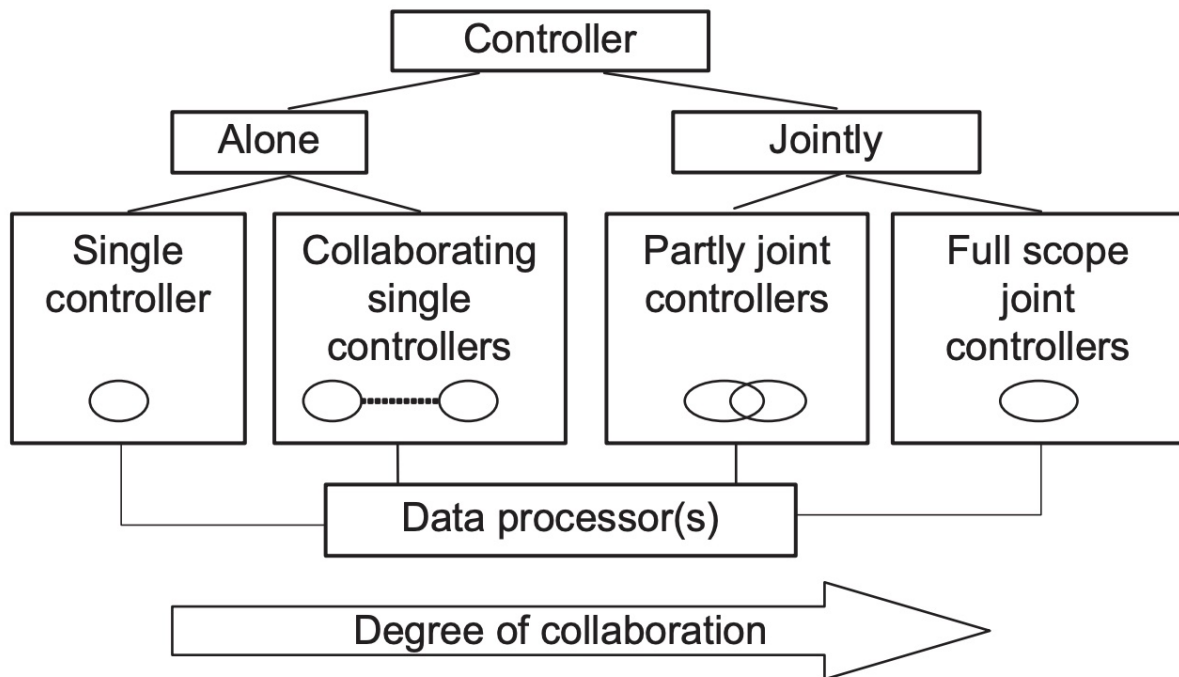


Figure 27. Collaboration Between Controllers per Olsen and Mahler

7.1.1 Sole Controller

Following on from the historic context of data processing relationships presented in Chapter Six,⁹³¹ the simplest models are those of a single controller and processor as is represented in *Figure 28* below.

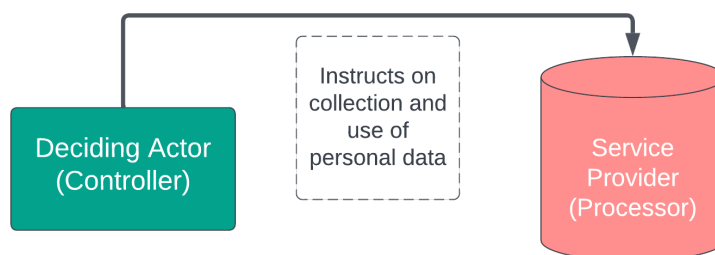


Figure 28. Archetypal Data Processing Relationship

⁹³¹ See [Chapter Seven, Section 7.3 Historical Models](#).

The controller may conduct the processing independently or employ the assistance of a processor. Provided that the processor operates exclusively on the directives given by the controller, there would be minimal ambiguity regarding which party bears the legal responsibility for ensuring adherence to Data Protection Law.

As has been noted in Chapter Four,⁹³² a processor may commission further sub-processors if the terms governing the data controller-processor agreement so allows.

These sub-processors are bound by the scope and terms of the original agreement.

7.1.2 Collaborating Sole Controllers

In this scenario, collaboration exists between two or more controllers, however, this does not amount to a joint controllership relationship. Such is the case, when collaborating controllers do not collectively determine the methods and procedures for data processing.

Both the WP29⁹³³ and the EDPB⁹³⁴ illustrate this scenario with the example of a travel agency sharing its customers' personal data. Information must be shared with an airline and a hotel chain for the purpose of arranging a travel package. The airline and hotel validate the availability of requested seats and rooms. Thereafter, the travel agency dispenses travel documentation and vouchers to its clientele. Each participating entity processes the data to execute their respective

⁹³² See [Chapter Four, Section 3. Actors and Accountability](#).

⁹³³ Article 29 Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' 19–20.

⁹³⁴ European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339) 20–21.

activities using their own resources. In this context, the travel agency, the airline, and the hotel function as separate data controllers, each processing data for their individual objectives, negating the existence of joint controllership.

7.1.3 Partly Joint-Controllers

The third scenario conceptualised by Olsen and Mahler⁹³⁵ is one in which the objectives and methods of certain processing operations are determined collectively by multiple controllers. Meanwhile, other processing functions are performed independently, under the exclusive control of a single controller.

Van Alsenoy argues that this iteration of 'partial joint control' can be perceived as a blend of 'collaborative sole controllers' and 'fully joint controllers'.⁹³⁶ Nevertheless, it should be underscored that the authority each joint controller holds may differ. The exertion of control may be 'symmetrical' or 'asymmetrical'. The 'co-controllers' could share decision-making power equally, or there could exist a preeminent party amongst them.

Elaborating on the previous travel agency example, both the WP29⁹³⁷ and the EDPB⁹³⁸ explain that if the travel agency and the hotel utilise a shared online portal to interact with their customers, they may be deemed joint controllers for those processing operations executed on the jointly managed portal. However, they would be considered separate controllers in relation to additional processing

⁹³⁵ Olsen and Mahler (n 930) 420.

⁹³⁶ van Alsenoy (n 127) 79.

⁹³⁷ Article 29 Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (n 933) 20.

⁹³⁸ European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339) 21.

conducted beyond the scope of the shared online portal. This is consistent with the phase-based approach outlined by the CJEU in *Fashion ID*.⁹³⁹

7.1.4 Fully Joint Controllers

Fully joint controllers collaboratively determine the means and purposes of all data processing operations. Nonetheless, if the partnership between the organisations results in the creation of a new entity that functions as a data controller, this scenario would then represent a case of a single data controller, potentially incorporating aspects of joint control.

7.2 Defined Examples

Entrenched in EU Law since the 1995 Directive, the application of the roles of controller, processor and joint controller have already been the subject of important exploration through case law and guidance. It must be reiterated at this juncture that control is a ‘functional concept’ which must always be determined by a ‘factual rather than a formal analysis.’⁹⁴⁰

The following subsections present a clear articulation of defined use cases of control in data processing relationships. These have either been defined by the Courts or by Guidance. Noteworthy in this regard is The Article 29 Working Party issued guidance on the concepts of controller and processor in its Opinion 1/2010 (WP169)⁹⁴¹ under the 1995 Directive. This has been updated and superseded by

⁹³⁹ See [Chapter Six, Section 7. CJEU Decision in Fashion ID](#).

⁹⁴⁰ European Data Protection Board, ‘Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021’ (n 339) 10. At par 20.

⁹⁴¹ Article 29 Working Party, ‘Opinion 1/2010 on the Concepts of “Controller” and “Processor”’ (n 933).

the European Data Protection Board's 2021 Guidelines on the Concepts of Controller and Processor in the GDPR.⁹⁴²

7.2.1 Controllership Stemming from Legal Provision

Clear Legal Stipulation of Data Controller Role

The EDPB explains that in certain situations, control may be derived from explicit legal authority.⁹⁴³ For instance, the authority or the precise parameters for its appointment may be outlined in national or Union legislation. This is clearly stipulated by the GDPR, which states that 'when the processing's goals and methods are dictated by Union or Member State law, the controller or its specific nomination criteria may be established by Union or Member State law.'⁹⁴⁴ In instances where legislation has distinctly pinpointed the controller, it becomes the decisive factor in determining who functions as the controller. This assumes that the law-making body has identified the entity with true control power as the controller. In several countries, national law mandates public entities to manage specific processing operations using personal data as part of their responsibilities.

⁹⁴⁵

Inferred Legal Stipulation of Data Controller Role

However, it is more usual for the law to stipulate a task or assign a duty to an entity to gather and process certain data, rather than explicitly naming the controller or defining the guidelines for its appointment. In such situations, the processing's objective is typically dictated by the law. The entity lawfully

⁹⁴² European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339).

⁹⁴³ *ibid* 10–11.

⁹⁴⁴ GDPR, Article 4(7).

⁹⁴⁵ European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339) 10–11.

nominated to fulfil this goal or public function usually assumes the role of the controller. When an entity assigned with specific public duties which necessitate the collection of some personal data, initiates a database or registry to accomplish those public duties, they are indirectly deemed the controller by the law. Broadly, the law may also mandate both public and private entities to retain or provide certain data. These entities would typically be perceived as controllers in relation to the processing required to fulfil this obligation.⁹⁴⁶

The EPDB provides the example of national legislation imposing a responsibility on municipal bodies to dispense social welfare benefits based on the financial standing of their citizens. To administer these payments, the municipal entity is required to collect and process data related to the financial conditions of the applicants. While the law does not explicitly declare that these municipal entities are the controllers of this data processing, it is inherently inferred from the legal stipulations.⁹⁴⁷

As has been discussed in Chapter Six, the question of inferred legal controllership was clarified by the CJEU in *Belgian State*.⁹⁴⁸ In its ruling, the Court explained that under the GDPR, the determination of a controller can be made either explicitly or implicitly through national law.⁹⁴⁹ In the latter case even where the designation of controllership is not made clearly, it may be understood from the legal provisions that define the roles, tasks, and powers of the entities involved. In this implicit

⁹⁴⁶ *ibid* 11.

⁹⁴⁷ *ibid*.

⁹⁴⁸ See [Chapter Six, Section 9. CJEU Decision in Belgian State](#).

⁹⁴⁹ *ibid*. at [30].

scenario, it is essential that the purposes and means of data processing, as well as the designation of the controller, are inferred with ‘sufficient certainty.’⁹⁵⁰

7.2.2 Controllership Based on Factual Circumstances

When control does not stem from legal provisions, the identification of a party as a controller requires an examination of the factual circumstances surrounding the data processing. This necessitates considering all pertinent facts to ascertain whether a specific entity has a decisive influence on the processing of the personal data under scrutiny. This factual evaluation underscores that the role of a controller is not derived from its inherent nature, but from its specific activities within a particular context. Therefore, an entity may function as a controller for some data processing operations and concurrently as a processor for others, with the classification needing to be assessed for each specific data processing activity.⁹⁵¹

In practical scenarios, certain processing activities naturally correspond with an entity's role or responsibilities, leading to obligations from a data protection perspective. Traditional roles or professional expertise that typically imply certain responsibilities can aid in identifying the controller. Generally, when an entity engages in the processing of personal data as part of its interaction with its employees, customers, or members, and can factually determine the purpose and means of processing, it will act as a controller.⁹⁵²

⁹⁵⁰ *ibid.*

⁹⁵¹ European Data Protection Board, ‘Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021’ (n 339) 11–12.

⁹⁵² *ibid.*

Processor Acting as Controller

A processor violates the GDPR when it exceeds the directions of the controller and begins to establish its own objectives and methods of processing. In relation to this processing, the processor is then regarded as a controller and may face penalties.⁹⁵³

The EPDB provides the example of a service provider offering marketing solutions to illustrate this point. In the scenario a company enters into an agreement with a marketing agency to carry out promotional activities for the company's clients, the agency is identified as a processor. However, if the marketing agency opts to utilise the client's customer data for other objectives, such as advancing their own business operations, it transforms its role into that of a data controller for these specific processing operations. This deviation would result in the marketing agency breaching the GDPR with its processing for this newly added purpose.⁹⁵⁴

Processor Acting with Limited Autonomy

The EDPB provides the use case of an employer engaging a different firm for the management of its employees' salary payments.⁹⁵⁵ The employer typically delivers precise directives concerning the payment recipients, the amounts, the dates, the chosen bank, the data retention duration, and the data to be disclosed to the tax authorities. In this context, data processing is performed for the employer's objective of salary payment to its employees, and the payroll management firm cannot employ the data for its individual purposes. The manner in which the payroll management firm should execute the processing is essentially unambiguous and strictly defined. However, the payroll management firm can

⁹⁵³ GDPR, Article 28(10)

⁹⁵⁴ *ibid* 25.

⁹⁵⁵ *ibid* 14.

make decisions on certain finer aspects of the processing, such as software selection or access distribution within its organisation. As long as the payroll management firm does not contradict or exceed the employer's instructions, this does not change its role as a processor. This scenario is represented in *Figure 29* below.



Figure 29. Service Provider Acting with Limited Autonomy

Processor Acting with High Autonomy

The EDPB provides the use case of a client engaging a law firm to advocate for it in a conflict. The law firm must process personal data relevant to the case. The motive behind processing this data stems from the firm's responsibility to represent the client in court, though this obligation does not specifically focus on personal data processing. The firm exercises a considerable degree of independence without any directives from the client company concerning personal data processing. Consequently, the processing conducted by the legal firm is associated with the functional role of the firm, thereby designating it as the controller for this processing.⁹⁵⁶ This scenario is represented in *Figure 30* below.

⁹⁵⁶ *ibid* 12.

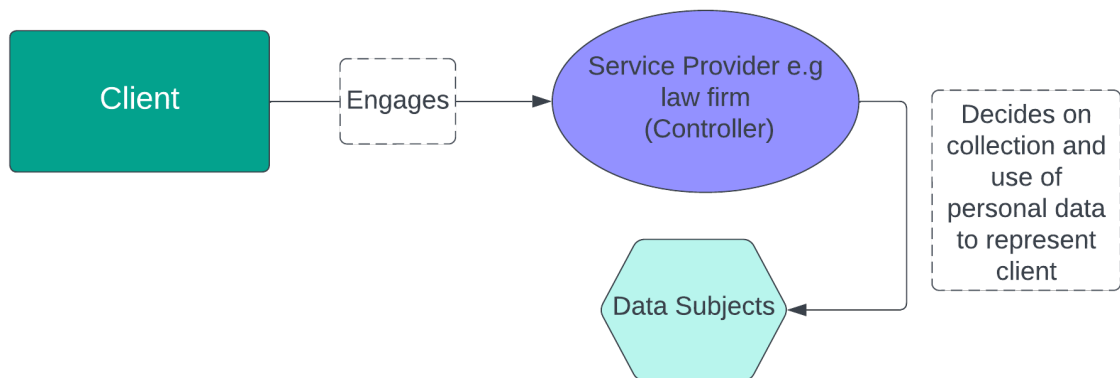


Figure 30. Service Provider Acting with Significant Autonomy

While the example provided by the EDPB refers specifically to a law firm, the roles defined will be relevant for any similar situation in which a client hires a second entity to complete a task with (i) an equally high degree of independence and (ii) without any directives concerning the processing of personal data.

7.3 Multiple and Joint Controllers

7.3.1 Separate Controllership

The EDPB extends the payroll case with the scenario where following instructions from the employer, the payroll administrator transfers information to a specific bank, enabling the actual salary payments. This activity includes personal data processing by the bank, which it performs in the context of its banking activities. As part of this activity, the bank independently determines what data must be processed to offer the service and the required data storage duration among other issues. Neither the employer, nor the payroll administrator hold any influence on the bank's data processing purpose and means. Thus, the bank acts as a controller

for this processing. The personal data transmission from payroll administration is considered a data transfer between two controllers.⁹⁵⁷

7.3.2 Separate Co-Controllershship

The involvement of multiple parties in a shared processing activity does not inherently lead to them being labelled as joint controllers. The instances below serve as a non-exhaustive, but defined list of situations where joint controllership does not apply.

Scenario 1

In the first instance, when two entities share the same data or data set, but they do not jointly decide on the purpose or method of processing, this would be considered as data transmission between separate controllers.

The EDPB offers an instance where a business accumulates and manages personal data of its employees for the administration of salaries and health insurance. A national regulation also mandates that the business forward all salary-related data to the tax authorities to augment fiscal monitoring. Despite the fact that both the business and tax authorities handle the same salary data, the absence of jointly determined objectives and means related to this data processing would categorise both entities as distinct data controllers.⁹⁵⁸

⁹⁵⁷ European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339).

⁹⁵⁸ *ibid* 22.

Scenario 2

Furthermore, when several entities use a shared database or common infrastructure, but each determines its own purposes independently, joint controllership will also be ruled out.

The EDPB cites the instance of a corporate group utilising a single database for client and prospect management. This database is stored on the parent company's servers, making the parent company a processor serving the other companies for data storage. Each group entity enters and processes its own clients' and prospects' data for its exclusive purposes. Also, each entity independently decides on access, retention periods, and the correction or deletion of their clients' and prospects' data. Thus, the entities are not privy to each other's data. Here, the mere use of a shared group database does not necessarily result in joint controllership. In these scenarios, each company operates as a separate controller.⁹⁵⁹

Scenario 3

Moreover, there are circumstances where different actors sequentially process the same personal data across a series of operations, with each player determining independent purposes and methods within their segment of the operation chain. If there is no joint participation in setting the objectives and procedures of the same processing operation or set of operations, joint controllership must be ruled out, and each actor should be seen as sequential, independent controllers. This legal reality has been reinforced by the Court's finding in *Belgian State*,⁹⁶⁰ discussed in Chapter Six.⁹⁶¹

⁹⁵⁹ *ibid* 23.

⁹⁶⁰ See *Belgian State* at [42].

⁹⁶¹ See [Chapter Six, Section 9. CJEU Decision in Belgian State](#).

The EPDB provides the example of a public body, Authority A, which is legally tasked with conducting significant analysis and statistics on the evolution of the country's employment rate. To fulfil this task, numerous other public entities are legally obligated to submit specific data to Authority A. Additionally, Authority A opts to use a particular system to handle the data, including its collection, necessitating that other entities use this system for their data disclosure. In this scenario, Authority A would be the sole controller of the processing for the purpose of analysing and recording employment rate statistics in the system because it establishes the purpose and the means. However, other public entities, as controllers of their individual processing activities, are responsible for verifying the accuracy of the data they initially processed and subsequently submitted to Authority A.⁹⁶²

7.3.3 Simple Joint-Controllership

The EDPB cites an example where several institutions opt to engage in a joint research project, utilising the pre-existing platform of one of the participating institutes. Each institute inputs the personal data it possesses into the platform for the purpose of the joint research. Each also utilises the data provided by the others through the platform for conducting the research. In this instance, all institutes are deemed joint controllers for the personal data processing that involves storing and disclosing information from this platform. Indeed, they have jointly decided the processing purpose and the means to be used (the existing platform). However, each institute is an individual controller for any other processing that may be executed outside the platform for their respective aims.⁹⁶³

⁹⁶² European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339) 23.

⁹⁶³ *ibid* 21.

7.3.4 Fragmented Joint-Controllershship

Per the CJEU's ruling in *Fashion ID*⁹⁶⁴ an entity cannot be considered a joint controller for activities which occur before or after the event for which they help collectively define the means and purpose for processing.

The EDPB uses the example of a recruitment agency to illustrate this dynamic. Company X collaborates with Company Y to assist in staff recruitment. Company X scouts for potential candidates among the applications that Company Y receives directly and those that exist in its own database. This database is solely created and maintained by Company X for its personal benefit, which includes better job-candidate matches and increased revenues. Despite no formal joint decision, Companies X and Y mutually engage in processing data to find suitable candidates based on parallel decisions: Company X's choice to establish and manage the service and Company Y's decision to augment the database with the applications it directly collects. These decisions, being complementary, indispensable, and critical for the candidate-seeking process, signify that both companies act as joint controllers in this specific context. However, Company X exclusively controls the data processing required for database management, while Company Y independently handles all subsequent hiring processes, such as arranging interviews, finalising contracts, and managing HR data, for its own objectives.⁹⁶⁵

⁹⁶⁴ See [Chapter Six, Section 7. CJEU Decision in Fashion ID](#).

⁹⁶⁵ European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339) 22.

7.5 Semi-Defined and Undefined Models

The domains of social media and cloud computing have been given some clarity through either Case Law or EDPB Guidance, although not all scenarios for their use have been covered in full. As such we may refer to these domains as semi-defined models. Moreover, our analysis of smart home devices and AI processing chains in Chapters Eight and Nine provides some further clarity on these areas. These have been incorporated into this taxonomy.

7.5.1 Cloud Computing

The US Department of Commerce's National Institute of Standards and Technology ('NIST') has set out a commonly used definition of cloud computing. According to this classification five essential features are necessary for a cloud service. These features are: (i) on-demand self-service, (ii) broad network access, (iii) resource pooling, (iv) rapid elasticity, and (v) measured service.⁹⁶⁶ The NIST definition has had an impact on legislation aimed at regulating this domain. The EU's NIS Directive⁹⁶⁷ defines 'cloud computing services' as:

Services that enable access to a scalable and elastic pool of shareable computing resources. These computing resources include resources such as networks, servers or other infrastructure, storage, applications and services.⁹⁶⁸

Cloud computing enables customers to outsource part of their IT infrastructure and its maintenance. Rather than buying their own hardware and software,

⁹⁶⁶ Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology* (Computer Security Division Information Technology Laboratory National Institute of Standards and Technology 2011) 1.

⁹⁶⁷ Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194 ('NIS Directive').

⁹⁶⁸ *ibid.* Art 4 (19).

customers depend on the services of the cloud provider. This avoids the high initial costs that might otherwise be required to set up and operate complex computing equipment. Furthermore, customers can adjust their usage quickly as their needs change. For their part, providers allocate and reallocate resources from a shared pool that can be used interchangeably by other customers.⁹⁶⁹

Three main models are usually distinguished within cloud services:

- IaaS (Infrastructure as a Service): basic computing resources such as processing power and storage.
- PaaS (Platform as a Service): environments for developing and deploying software applications and services.
- SaaS (Software as a Service): end-user applications delivered over the internet.⁹⁷⁰

The main actors involved in the operation of cloud computing services are:

1. Cloud customers
2. Cloud end-users
3. Cloud providers, including:
 - Application providers
 - Platform providers
 - Infrastructure providers⁹⁷¹

⁹⁶⁹ W Kuan Hon, Christopher Millard and Ian Walden, 'Who Is Responsible for "personal Data" in Cloud Computing?--The Cloud of Unknowing, Part 2' (2012) 2 International Data Privacy Law 3. van Alsenoy (n 127) 468.

⁹⁷⁰ Kuan Hon, Millard and Singh (n 700) 6.

⁹⁷¹ van Alsenoy (n 127) 472–479.

The simplest relationship between these parties is reflected in *Figure 31* below. The central party is the cloud service customer, who utilises a cloud facility to provide a utility to end users.⁹⁷²

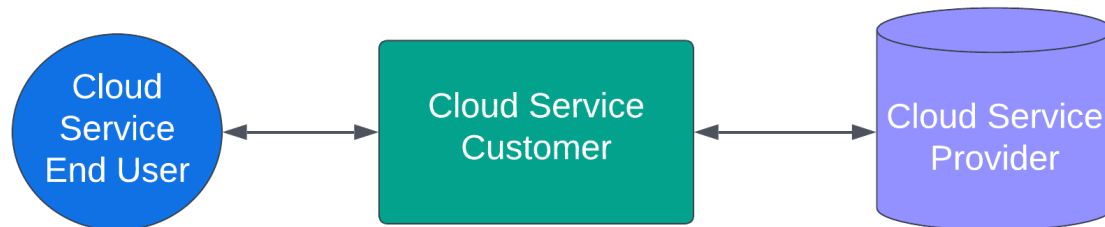


*Figure 31. Actors within Simple Cloud Service Processing Chain*⁹⁷³

In this standard scenario, it is cloud service customers and end users who hold the role of controller. This is reflected both in EDPB guidance⁹⁷⁴ and within the contractual terms for large cloud service providers. AWS's terms of service make clear that in the vast majority of instances it is the Cloud customer who acts as the controller.⁹⁷⁵

However, AWS accepts that it will still maintain the role of controller in a very limited number of circumstances.

AWS as a data controller – When AWS collects personal data and determines the purposes and means of processing that personal data – for example, when AWS stores account information (e.g. email addresses provided during the account registration) for account registration, administration, services access, or contact information for the AWS

⁹⁷² Cobbe and Singh (n 828).

⁹⁷³ *ibid* 3.

⁹⁷⁴ European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (n 339) 27.

⁹⁷⁵ 'GDPR - Amazon Web Services (AWS)' (n 707).

account to provide assistance through customer support activities – it acts as a data controller.⁹⁷⁶

This division of roles is common to a variety of major Cloud Service Providers including Microsoft⁹⁷⁷ and Google.⁹⁷⁸ In the majority of circumstances Cloud Service Providers of all varieties will hold the role of processor. In contrast, where the Cloud Service Provider utilises data for its own purposes it acts as a controller.

⁹⁷⁹

However, in its 2012 'Recommendations'⁹⁸⁰ the French Supervisory Authority, the CNIL, maintained that in certain situations a cloud service provider will in fact act as a joint controller. The CNIL argued that in instances where customers cannot issue directives to a cloud provider or ascertain the efficiency of its data safety measures, the cloud provider should be designated as a joint controller as it 'contributes to the definition of the purposes and means for personal data processing'.⁹⁸¹ It is also suggested by the CNIL that this would only apply to instances of PaaS and SaaS servers and not IaaS providers. The entire evaluation of the CNIL is dealt with briefly in its guidance document, and the Supervisory Authority did not provide further details on this assertion.

More recently this finding has been supported by the Slovenian Supervisory Authority. In its 1 June 2022 ruling, the Information Commissioner (Slovenia)

⁹⁷⁶ *ibid.*

⁹⁷⁷ Microsoft, 'Microsoft Products and Services Data Protection Addendum (DPA)' (n 708) 7.

⁹⁷⁸ Google Cloud DPA Section 5 'Cloud Data Processing Addendum' (n 709).

⁹⁷⁹ European Data Protection Supervisor (n 710).

⁹⁸⁰ Commission nationale de l'informatique et des libertés (CNIL) (n 811).

⁹⁸¹ *ibid* 5.

found that a particular cloud computing provider decided on the essential means of processing. As such it was to be considered a controller.⁹⁸² The provider in question aimed to alleviate the technical burden for its clientele, allowing them to concentrate wholly on the contents of the requested data. As such, the clients of the cloud computing service had minimal impact on the technical and organisational strategies employed by the provider in the data management process.⁹⁸³

The Information Commissioner (Slovenia) found that the clients of the cloud computing provider could not ensure technical compliance with the GDPR. The cloud provider was functioning as a controller to the extent that it decided the technical methodologies by which data was requested, managed, and disseminated, as well as the engagement of sub-processors. The cloud computing provider and its clients, both deciding the purposes and processing means, were therefore in a joint controllership relationship.⁹⁸⁴

A summary of the Data Processing Roles applicable to the actors in cloud service provision relationships is provided in *Table 7* below.

Table 7. Cloud Service Provider Actors and their Data Protection Roles

⁹⁸² Information Commissioner (Slovenia) (n 813).

⁹⁸³ GDPRhub, 'IP (Slovenia) - 0612-23/2019/19 — GDPRhub', <[https://gdprhub.eu/index.php?title=IP_\(Slovenia\)_-_0612-23/2019/19&oldid=27260](https://gdprhub.eu/index.php?title=IP_(Slovenia)_-_0612-23/2019/19&oldid=27260)>.

⁹⁸⁴ Bogdan Ivanišević and Marija Stojanovic, 'Cloud Provider a Joint Controller? Slovenian Regulator Joins CNIL in Saying Yes' (*Lexology*, 15 August 2022) <<https://www.lexology.com/library/detail.aspx?g=243478c5-13c2-435c-a1c3-cecc51d1204c>> accessed 13 March 2024.

Actor	Role in General per EDPB in General Terms	Accountability per CNIL and Information Commissioner (Slovenia)
Cloud Service Customers	Controller	Controller
Cloud Service Application Providers (SaaS)	Processor	May be Joint Controller
Cloud Service Platform Providers (PaaS)	Processor	May be Joint Controller
Cloud Service Infrastructure Providers (IaaS)	Processor	Processor

7.5.2 Social Media Networks

Schneier has outlined a classification system for social media networks, which identifies six categories of personal data processed.⁹⁸⁵ These are presented in *Table 8* below.

Table 8. Social Media Data Categories

Data Type	Description	Example
Service Data	Data offered to a social media provider in order to access the social media services.	An individual's legal name, date of birth, and email address.

⁹⁸⁵ Bruce Schneier, 'A Taxonomy of Social Networking Data' (2010) 8 IEEE Security & Privacy 88.

Disclosed Data	Data which users post on their own individual profile pages.	Blog entries, images, or videos.
Entrusted Data	Data which social media users place on the profile pages of other users.	Wall posts, comments, or replies.
Incidental Data	Data about a social media user or third party that has been uploaded by another user.	A photograph featuring a third party.
Behavioural Data	Data which relates to the activities of social media users within the network.	Data on how an individual engages with certain types of content.
Derived Data	Data that is inferred from other social media data.	A user is a member of Group X thus Attribute Y is assumed to be held by the user.

Van Alsenoy identifies the core actors of relevance for study within social media services.⁹⁸⁶ These have been compared to those outlined by the EDPB in its Guidelines 8/2020 on the Targeting of Social Media Users.⁹⁸⁷ A total of six key actors have been identified from both for the purpose of this thesis. Their characteristics and roles are explored in the following sections.

1. Social Media Provider

⁹⁸⁶ van Alsenoy (n 127) 395.

⁹⁸⁷ European Data Protection Board, 'Guidelines 08/2020 on the Targeting of Social Media Users' (2021) 8.

2. Social Media User
3. Page Administrator
4. Targeter
5. Third-Party Application Provider
6. Third-Party Website Operator

Social Media Providers

Social media providers act as controllers. The EDPB specifically notes that the social media provider cannot qualify as a processor under the GDPR as these actors determine both the purposes and means of their individual data processing activities. Their primary goal is to deliver a social networking service that produces revenue. Besides the operations that are strictly essential for providing the social media service, the provider also determines a variety of supplementary processing activities, which include those designed to facilitate targeted advertising.⁹⁸⁸

The role of the social media provider becomes more challenging to discern in the context of user generated and disseminated content.⁹⁸⁹ Sartor argues that it is inappropriate to assign controllership for user generated content to social media providers. He explains that these organisations exert minimal influence when users are uploading content.⁹⁹⁰ Even though social media platforms might motivate certain kinds of sharing, each user makes an independent decision whether to disseminate specific content. Furthermore, it is not reasonable to expect social media providers to be able meet the controller's obligations in relation to

⁹⁸⁸ *ibid* 15.

⁹⁸⁹ van Alsenoy (n 127) 411.

⁹⁹⁰ Giovanni Sartor, 'Liabilities of Internet Users and Providers' in Marise Cremona (ed), *New Technologies and EU Law* (Oxford University Press 2017).

user-shared data. In contrast, Van Alsenoy *et al.* contend that it is possible to attribute controllership to the social media platform itself for user generated content alongside social media users. It is argued that the social media provider ought to be considered a controller regarding its social networking service ‘in its entirety’. Indeed, once data has been uploaded, the social media provider initiates operations on it, facilitating the sharing of information (e.g., storage, analysis, dissemination, access control).⁹⁹¹ For these processing activities, the provider has independently predetermined the ‘purposes and the means, irrespective of the social media users. Given that the sharing of personal data amongst contacts is a core element of its service, these commentators conclude that the social media provider operates as a joint-controller concerning the distribution of content across its platform even though the impetus to share this content originated from one of its users.’⁹⁹²

Social Media Users

Social media users are generally considered data subjects under the GDPR, regardless of their registration status with the platform. The EDPB points out that ‘both individuals that are and that are not registered with the social media providers may be considered ‘data subjects’ within the meaning of GDPR insofar as the individual is directly or indirectly identified or identifiable.’⁹⁹³

⁹⁹¹ Brendan Van Alsenoy and others, ‘Social Networks and Web 2.0: Are Users Also Bound by Data Protection Regulations?’ (2009) 2 *Identity in the Information Society* 65, 70.

⁹⁹² van Alsenoy (n 127) 412.

⁹⁹³ European Data Protection Board, ‘Guidelines 08/2020 on the Targeting of Social Media Users’ (n 987) 9.

The question of whether social media users may also act as controllers must however be explored. Wong,⁹⁹⁴ Helberger and Hoboken⁹⁹⁵, and Van Alsenoy *et al.*⁹⁹⁶ hold that in theory every social media user will act as a controller when processing the personal data about others online. However, when it comes to defining the methods of data processing, users of social media generally lack substantive decision-making power. While they may adjust some minor features or settings, their influence over how the processing is conducted is fundamentally limited. Nevertheless, every user of social media typically exercises the choice of whether to share specific information using the platform. In this respect, users maintain some degree of control over the means of their data processing when they entrust data about others to the audience of a social media network. The influence exercised by users over the platform generally covers any content they decide to upload and any processing operations they initiate independently. Their control does not encompass the entirety of the social media platform, but only those processing operations where they can effectively determine the objectives and methods. Users of social media platforms might be regarded as controllers under the GDPR when they disclose personal data about others via the platform. Companies and organisations are, in principle, subject to the same responsibilities as those required of controllers in any other context.

The role of private individuals as users depends on whether their use of social media falls within the scope of the personal use exemption. The limitations of the household exemption to sharing of personal information via online means have

⁹⁹⁴ Rebecca Wong, 'Social Networking: A Conceptual Analysis of a Data Controller' (2009) 14 Communications Law 142.

⁹⁹⁵ Natali Helberger and Joris van Hoboken, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers' (2010) 11 Computer Law Review International 101.

⁹⁹⁶ Van Alsenoy and others (n 991).

already been tested in the *Lindqvist* decision discussed in Chapter Eight.⁹⁹⁷ In its ruling the CJEU clarified that the household exemption must ‘be interpreted as relating only to activities which are carried out in the course of private or family life of individuals,’ however this ‘is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.’⁹⁹⁸ Thus outside disclosure of personal information to ‘an indefinite number of persons’ would no longer fall under the household exemptions.

Page Administrator

As noted in Chapter Six⁹⁹⁹ in *Wirtschaftsakademie* the Court ruled that the administrator of a ‘fan page’ on Facebook must be seen as participating in defining the objectives and methods of personal data processing. According to the arguments presented to the CJEU, the establishment of a fan page necessitates the administrator setting certain parameters, which subsequently impacts the processing of personal data for the purpose of generating statistics based on the traffic to the fan page.¹⁰⁰⁰ As such, the administrator has been clearly established as a joint controller together with the social media platform provider.

Targeters

In all instances the targeting party assumes the role of a controller. It is this party which sets the purposes and means of data processing, by actively acquiring and sending the personal data of relevant individuals to the social media provider for

⁹⁹⁷ Case C-101/01 *Lindqvist v Åklagarkammaren i Jönköping* [2003] EU:C:2003:596 (n 803). See [Chapter Eight, Section 6. The Disappearing Household Exemption.](#)

⁹⁹⁸ *ibid.* at [47].

⁹⁹⁹ See [Chapter Six, Section 5. CJEU Decision in Wirtschaftsakademie.](#)

¹⁰⁰⁰ *Wirtschaftsakademie* at [36].

advertising reasons. Correspondingly, the social media provider also takes on the role of controller as it has made the decision to utilise the personal data it has obtained from the social media user in order to facilitate the displaying of ads by the targeting party to a selected audience.¹⁰⁰¹

A joint controller relationship exists when the social media provider and the targeting party concurrently decide on the purposes and means of a processing activity. In this context, these processing activities include uploading unique identifiers associated with the intended audience, executing the matching process, selecting the targeting criteria, displaying the advertisement, and performing any reporting that relates to the targeting campaign.

In instances of geo-location-based targeting, the targeter exerts a decisive influence over the processing of personal data by setting the parameters of ad targeting in line with its business objectives. For example, aligning the targeting with the operating hours of a restaurant and the geo-location of individuals in proximity to the restaurant within this time frame. The social media provider, in contrast, has accumulated information about the user's location with the specific purpose of enabling such location-based targeted advertising. Consequently, joint control is established between the targeter and the social media platform with regards to the collection and analysis of the user's location data, as well as the display of the advertisement, with the aim to target the user with the ad.¹⁰⁰² In the context of pixel-based targeting, both the party aiming to target, and the social media service provider participate in defining the goals and methodologies pertaining to the processing of personal data. This collaborative process eventually leads to the presentation of the advertisement to the user. Thus, joint

¹⁰⁰¹ *ibid.* 20-25

¹⁰⁰² *ibid.* 24.

control is established in relation to the gathering of personal data and its transmission via pixels, in addition to the matching and subsequent display of the advertisement to the user on the social media platform.¹⁰⁰³

Third Part Application Providers

In its *Opinion on Social Networking*, WP29 clarified that application providers will also be controllers if they develop applications which run as an addition to the social media platform. Similar to social media providers, most application providers aim to offer specific services that generate revenue, whether directly or indirectly. The nature of this service will vary depending on the application's intended function, which could include gaming, content streaming, location sharing, or crowd funding. Hence, application providers decide the aims of data processing that takes place while offering their services. They also set the means of their data processing, deciding which user data to gather and how it will be subsequently managed. Besides deciding on the activities essential for delivering the app's functionality, application providers can elect to carry out additional processing activities, including those meant to facilitate targeted advertising.¹⁰⁰⁴

The extent of control exercised by application providers generally covers any processing conducted to support the application's function. It also encompasses any processing carried out by the application provider to facilitate targeted advertising. For instance, revealing a user's location to support contextual advertising. Any other subsequent utilisation of personal data by the application provider will generally also be within the scope of its control. While application

¹⁰⁰³ *ibid.* 22-23.

¹⁰⁰⁴ Article 29 Working Party, 'Opinion 5/2009 on Online Social Networking Adopted on 12 June 2009, 01189/09/EN WP 163' 5 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf> accessed 28 June 2023.

developers enjoy considerable flexibility in determining how to handle personal data processing, they are typically limited by two crucial factors: (I) the terms and conditions for application developers, and (II) the access control model upheld by the social media platform.¹⁰⁰⁵

Third-party application providers function as separate controllers. They establish their own purposes and means for their personal data processing. Once access is permitted, an application provider will generally collect the data and transfer it to its own servers for additional processing.¹⁰⁰⁶

Third Party Website Operators

As has been noted in Chapter Six,¹⁰⁰⁷ the CJEU ruled in *Fashion ID* that a website operator will be considered a joint controller with a social media platform when it embeds a social media plugin on its website. However, the court further ruled that collective accountability is limited to the collective purpose.¹⁰⁰⁸ It is only in this processing that the two actors are to be considered joint controllers. It thus follows that an entity cannot be considered a joint controller for activities which occur before or after the joint/collective event for which they collectively define the means and purpose for processing.

Summary of Roles

A summary of the Data Processing Roles applicable to the actors in social media networks is provided in *Table 9* below.

¹⁰⁰⁵ van Alsenoy (n 127) 427–428.

¹⁰⁰⁶ *ibid.* 428–429.

¹⁰⁰⁷ See [Chapter Six, Section 7. CJEU Decision in Fashion ID.](#)

¹⁰⁰⁸ *Fashion ID* at [107].

Table 9. Social Media Actors and their Roles under the GDPR

Actor	Data Processing Role
Social Media User – Private Individual	• Data Subject in most uses. • Controller when the Household Exemption under Article 2(2)(c) of the GDPR cannot be applied.
Social Media User – Company/Organisation	• Controller – the Household Exemption under Article 2(2)(c) of the GDPR is not relevant.)
Social Media Provider	• Controller for most operations. • <u>May</u> also be a Controller for User Generated Content
Page Administrators	• Joint Controller with Social Media Provider

Targeters – Pixel Based Targeting	Joint Controller with Social Media Provider
(Third-Party) Application Providers	Separate Controllorship
(Third-party) Website Operators	Joint Controllorship for activities which transmit data to social media platforms per <i>Fashion ID</i>.

7.5.3 Smart Home Devices

The issue of smart home devices has been explored in depth in Chapter Eight. Here we reproduce the findings of the relationships present in *Table 10* below.

Table 10. Smart Home Devices Actors and Data Processing Roles

Actor	Data Processing Role
Smart Home Device User – Closed System <u>Without</u> Third Party Access	Released from the obligations of the GDPR through the Household Exemption.
Smart Home Device User –System <u>With</u> Third Party Access	Controller unable to avail of the Household Exemption

Smart Home Device Supplier	General Holding: Processor Inferred Position of CNIL and Information Commissioner (Slovenia): Joint-Controller

7.5.4 AI Service Processing Chains

In Chapter Nine the undefined realm of AI processing chains was analysed. In most cases, clients of AI services are seen as data controllers, taking on the main role of ensuring compliance. On the other hand, providers, who often hold significant power in these dealings, are seen as processors. Yet, the actual dynamics are quite different. These providers exert significant influence over AI operations. Numerous clients, especially smaller businesses without advanced AI understanding, remain without a clear view of their provider's framework. Lacking knowledge and understanding, these clients cannot be seen as holding any real authority over these AI systems.

In spite of the pivotal role these providers play, they frequently downplay their part, identifying themselves simply as processors in contractual terms. A constructive approach to address this discrepancy can be drawn from the stance of the CNIL and the Slovenian Information Commissioner, who see cloud service providers as joint controllers. If this viewpoint gains broader support, it could lead to more accountability for the entities best equipped to handle it.

However, this approach does not resolve the situation where entities are oblivious to one another or never interact directly. This scenario has become increasingly prevalent in AI processing chains.

Moreover, the regulatory framework adds another layer of complexity. As an example, under the GDPR, a small company collaborating with a tech giant might be labelled as a data controller. But, when we look at the AI Act, this same company is an AI deployer, the entity with fewer duties. At the same time, the tech firm will be categorised as an AI provider and thus hold greater responsibilities. This is a relationship defined by complementing and competing obligations.

8. Conclusion

This chapter serves as a supplement to the analyses conducted in the preceding sections of this thesis, presenting four potential mitigations to the problem of control as found in the literature. The solutions explored were (I) extending responsibilities for processors; (II) applying a non-controller-based accountability model; (III) moving to a *de minimis* threshold for control in the form of orchestration; and (IV) allowing flexibility in judicial and regulatory action. Of the four resolutions explored each was found to have benefits and limitations.

(I) Blume and Van Alsenony advocate for increased obligations to be shouldered by processors, yet both overlook the issue of power imbalances. A more nuanced approach might focus on imposing stricter regulations not on all processors, but specifically on major players in the industry. The Digital Service Act and Digital Markets Act provide illustrative examples by imposing additional duties and constraints on dominant digital entities. Moreover, we have also seen the potential for complementary enforcement mechanisms through the European Commission's investigation into Meta's change of terms and conditions. We must however be mindful of the potential complexity of overlapping enforcement

approaches as has already been highlighted in the Draghi report. A complex problem cannot be untangled by weaving a new web of complications.

(II) Wong calls for a more radical approach in a transition towards a non-controller accountability framework. An accountability regime focussing upon specific obligations for specific processing acts without reference to controllership may allow for greater clarity if carried out with efficiency. It is important to recognize that this proposed approach would require a comprehensive restructuring of Data Protection Law's accountability framework. Such a transformation would demand significant political commitment and coordinated legislative efforts across relevant jurisdictions.

(III) To address the issue of expanding controller definitions, jurisprudence should revisit the fundamental concept of 'controller' and establish an exception for parties with minimal influence over data processing. This can be achieved by raising the threshold for determining entities that significantly influence processing means and purposes. The CJEU's approach to this concept has been inconsistent. While some decisions, like *Jehovan todistajat*, appeal to a conceptual ideal of controllership defined by an orchestrating role, others, such as *Fashion ID* and *Belgian State*, have broadened the scope to include actors with limited influence. Future case law should establish a minimum threshold of orchestrating influence necessary for controller status. This approach would enhance transparency, legal certainty, and accountability, aligning more closely with the GDPR's protective rationale and reflecting economic realities. It would also ensure that risk-management mechanisms are imposed only on those with actual decision-making power over data processing. This approach necessitates a shift in judicial perspective and potential legislative action to redefine the scope of controllership.

(IV) A flexible interpretation and enforcement of data protection law by courts and regulators could mitigate excessive legal consequences arising from its broad application. This approach, however, raises normative questions about balancing strict rule application with practical enforcement. While rigid enforcement ensures consistency and deterrence, it may lead to an overwhelming caseload and disproportionate outcomes for minor infractions. Flexibility in Data Protection Law offers benefits but challenges legal certainty, equal application, and effective rights protection. Striking a balance between adaptability and robust enforcement remains crucial. This approach requires further exploration of judicial and regulatory flexibility to ensure legal certainty and consistent rights protection. Its key advantage is that the European Data Protection Board could provide much-needed clarity without extensive legislative changes, offering some mitigation without complete resolution of the issues at hand.

Finally, a fifth (V) solution has been offered in the form of a systematic taxonomy of data processing relationships as they pertain to EU Data Protection Law. The significance of this taxonomy lies in its dual contribution: firstly, it provides a clearer understanding of the intricate facets of *the Problem of Control*, as discussed in Part II, by outlining these relationships in a tangible manner. Secondly, it contributes to the growing knowledge base of Data Protection Law, and aids in alleviating the issues associated with *the Problem of Control*.

While the impacts of these complexities may initially appear to be confined to the technology sector, they transcend industry boundaries, impacting actors across a diverse spectrum. Even small-scale businesses or non-commercial entities could face these difficulties daily creating a need for expertise and guidance.

This taxonomy may provide invaluable insights for stakeholders such as researchers, regulators, technology developers, small and medium enterprises,

and even private individuals. This resource could potentially lower the hurdles to compliance and democratise the knowledge tax involved in adhering to Data Protection Law.

Moreover, the catalogue can serve as a resource for data controllers conducting Data Protection Impact Assessments under Article 35 of the GDPR, offering predefined models to identify and understand privacy risks. The resulting 'library' of procedures and safeguards associated with recurrent data sharing relationships may prove instrumental in addressing the unique challenges these relationships present.

Chapter Eleven: Conclusion

1. Research Problem

In this thesis we have sought to define *the Problem of Control* in EU Data Protection Law. This challenge emerges from the controller-based accountability framework of the GDPR. Under this model the chief onus for obligations falls upon controllers and joint controllers, while secondary responsibility is placed upon processors. Thus, being able to precisely discern relationships of control is necessary in order to allocate accountability and liability. Yet, data processing relationships are increasingly complex woven with multiple participants and data exchanges.

Our concern surrounds the difficulty in defining these relationships and the parties within them. A challenge which has been heightened through a series of CJEU judgments, the cumulative findings in these cases have stretched the definition of ‘controllership’ to new limits. The rapid rise of AI systems has further intensified these hurdles, bringing novel challenges to this framework. The evolution of this technology has marked a leap into a realm of technological innovation previously relegated to the pages of science fiction.

The accountability model of EU Data Protection Law operates under the unspoken presumption that the controller can in fact control the processing activities. This is no longer the case. Instead both *control* and *controllership* have been rendered void of meaning. As neither data subjects nor data controllers themselves hold any true form of power over information.

The key findings of our analysis are presented in the following sections.

2. The Rise of Data Protection Law

We have highlighted both privacy and data protection as rights which have emerged and evolved in relation to technological and societal change.

In 1890, Warren and Brandeis articulated their foundational understanding of the right to privacy as a direct reaction to the technological leaps of their era.¹⁰⁰⁹ The rise of photographic tabloid journalism meant that what once were impenetrable walls of retreat were now suddenly rendered porous, revealing all. This unforeseen intrusion into personal domains prompted Warren and Brandeis to champion legal reforms as a bulwark against such invasions.

In contrast, by the 1970s new concerns underpinned the formation of Data Protection Law within Europe.¹⁰¹⁰ The haunting spectres of the Third Reich and the USSR, along with transformative advances in automated data processing, kindled deep-seated fears of a monolithic state equipped with exhaustive knowledge and control. The radically different experience of Warren and Brandeis from that of European policy makers in the 1970s cannot be understated. The two lawyers penned their article more than a decade before the Wright brothers' first flight and almost three decades prior to the societal and technological upheaval which emerged from the ruins of WWI. Furthermore, their articulation of a right to privacy was made before the modern administrative state which grew in its capacity in response to the global financial crash of 1929. In these changes the individual was forced to reimagine her relationships to others, especially the state which had previously left her with far greater anonymity.

¹⁰⁰⁹ See [Chapter Two, Section 2.1 Early Formulations](#).

¹⁰¹⁰ See [Chapter Two, Section 3.1 Technological and Societal Context](#).

Yet a similar lacuna separates the emerging challenges of the 2020s from the context of Hesse in 1970 and even those leading to the adoption of the Data Protection Directive in 1995. Our digital age, underpinned by widespread internet usage, has reshaped interactions at the individual, societal, and political levels. For liberal democracies, there remains the enduring task of balancing liberties while ensuring the rights of individuals. This task has been exacerbated by the growth of a global industry in which personal data is commodified for profit.

3. The Nature and Ambitions of the Data Protection Regime

The evolution of Data Protection Law has been characterised by two distinct yet complementary paradigms. The first, the 'Societal Protection Model,' is rooted in the desire to safeguard society through regulatory oversight.¹⁰¹¹ This approach is enshrined in Article 8(3) of the CFREU, which mandates that compliance with data protection rules be subject to control by an independent authority. Concurrently, a second paradigm has emerged, the 'Individual Control Model.'¹⁰¹² This approach focuses on empowering data subjects through a regime of individual rights. Article 8(2) of the CFREU exemplifies this model by explicitly guaranteeing the rights of access and rectification.

In the context of the GDPR, the concept of protection has become inextricably linked with the notion of *control*, reflecting the central role that data autonomy plays in contemporary information privacy theory. However, the GDPR's approach is not limited to individual control; rather, it incorporates a diverse range of regulatory mechanisms to legitimise data processing. This multifaceted

¹⁰¹¹ See [Chapter Three, Section 3.2 The Societal Protection Model](#).

¹⁰¹² See [Chapter Three, Section 3.1 The Individual Control Model](#).

strategy results in a legal framework that balances individual choice with broader societal protection measures.

The efficacy of both the Individual Control and Societal Protection models hinges on a clear accountability system. Data subjects exercise their rights against controllers, a relationship that forms the cornerstone of the European Data Protection Regime. This system aims to empower individuals and ensure responsible data handling. However, its effectiveness is contingent upon an unambiguous delineation of the controller's role.

Independent SAs, responsible for overseeing Data Protection Law's application and enforcement, exercise their powers based on the level of responsibility assigned to actors, particularly controllers. These authorities are crucial in ensuring compliance, investigating breaches, and imposing sanctions. However, their ability to function effectively depends on a precise understanding of controllership in various data processing scenarios. Without clear demarcation of the controller's role, SAs risk misdirecting their powers or deploying them ineffectively. They may pursue incorrect actors or struggle to allocate responsibility in complex data processing chains, wasting resources, and eroding public trust in the regulatory system.

Furthermore, when controllership boundaries are unclear, data subjects face uncertainty in directing their requests and complaints, impeding their ability to exercise rights and maintain control over personal information. This lack of clarity creates a substantial barrier to individual empowerment, potentially undermining the core objectives of the data protection framework.

Ultimately, the importance of defining the controller's role extends beyond the operational aspects of Data Protection Law. It is fundamental to rights protection

and power balance in the digital age. Failure to provide a clear and consistent understanding of controllership risks creating a landscape where individuals are disempowered and regulators are hindered in their efforts to protect citizens' privacy and autonomy. This underscores the critical need for precise and adaptable definitions of controllership in evolving digital ecosystems.

4. An Expanding Regime

We have shown that the EU data protection framework of the 2020s represents a significant evolution from its predecessors, characterised by both expanded scope and increased depth. This enhanced regime constitutes a crucial component of a broader regulatory ecosystem governing online services, digital markets, and data exchange within the EU. Furthermore The fundamental concepts, roles, and responsibilities initially introduced through the 1995 Directive have undergone significant expansion through judicial interpretation. Consequently, the comprehensive Data Protection Regime of the 2020s can be understood as the product of both legislative initiatives and evolving jurisprudence, reflecting the EU's commitment to adapting its regulatory framework to the complexities of our digital age.

In response to new challenges a litany of legal instruments has been introduced by the European Union. These include the Digital Services Act, the Digital Markets Act, the Data Governance Act, the Data Act, and the AI Act. With the GDPR at the centre, these form a comprehensive scheme for the regulation of personal information, digital innovation, and online services in Europe as has been documented in Chapter Five.¹⁰¹³ A key theme emerging from our analysis is the creation of 'complementing and competing' obligations and enforcement

¹⁰¹³ See [Chapter Five, Section 2. Legislative Expansion.](#)

mechanisms across these various legislative instruments. Examples include overlapping obligations for cookie usage under both the ePrivacy Directive and the GDPR, and the dual regulation of personal data processing within AI services under both the GDPR and the AI Act, creating a complex regulatory landscape for businesses.

Complementary enforcement has also emerged as a significant trend, as demonstrated by the European Commission's investigation into Meta's data processing practices. Meta's introduction of a 'pay or okay' model in response to regulatory challenges has prompted actions under both the GDPR and the Digital Markets Act, illustrating the multifaceted nature of digital regulation in the EU.

Furthermore, the diversity of accountability models employed by these laws challenges the notion that the GDPR's controller-based model is the sole approach to safeguarding digital rights.

Additionally, the foundational concepts, roles, and responsibilities initially established by the 1995 Directive have undergone substantial expansion through judicial interpretation. The core concepts of data protection are now broadly defined, with exceptions narrowly construed. The expansive definition of 'personal data' has been particularly influential, leading to data protection becoming an almost ubiquitous legal framework, applicable to an ever-increasing range of activities.¹⁰¹⁴ As Purtova suggests, data protection may now be seen as the 'law of everything'.¹⁰¹⁵

¹⁰¹⁴ See [Chapter Five, Section 3.1 The Expanded Scope of Personal Data](#)

¹⁰¹⁵ Purtova (n 31).

This judicial expansion has also elevated the standard for international data transfers, particularly in light of the *Schrems I* and *II* judgments.¹⁰¹⁶ These cases exposed inherent contradictions in EU data transfer regulation and highlighted the gap between the EU's aspirations for global data protection and the practical limitations of its regulatory approach. The CJEU's interpretation of 'essential equivalence' as the standard for adequate protection in third countries has set a high bar for international data transfers, creating significant challenges for globally operating businesses.

In addition, The responsibility for assessing data protection regimes now extends beyond the European Commission and Supervisory Authorities, encompassing a broader range of stakeholders and processes. The revised Standard Contractual Clauses issued by the European Commission in June 2021 mandate that controllers identify and address any infringements on the 'essence' of EU fundamental rights in third-country data transfers. This new obligation demands an unprecedented level of expertise from controllers, further underscoring the importance of clearly delineating accountability roles within the EU Data Protection Regime.

5. The Problem of Control

Our investigation has demonstrated that the controller-based accountability model, which traces its origins to the nascent data protection laws of the 1970s and 1980s, has become increasingly strained in the face of modern data processing realities. The complexity of contemporary data flows, often involving numerous parties and intricate transfer mechanisms, has rendered the clear delineation of roles and responsibilities exceptionally challenging.

¹⁰¹⁶ See [Chapter Five, Section 3.2 The Requirements for International Transfers of Data](#).

Central to the European Data Protection Regime are the twin ambitions of protecting individual rights and freedoms while simultaneously fostering innovation and expanding the digital market. These goals, explicitly articulated in both the European Commission's initial proposal for the GDPR and the final text of the Regulation itself, have shaped the development of the accountability framework.¹⁰¹⁷ The increasing complexity of data processing relationships has led us to conclude that the controller of the early 1980s bears little resemblance to the form found in the early 2020s.

What is more, through a series of landmark cases including *Wirtschaftsakademie Schleswig-Holstein*, *Jehovan todistajat*, *Fashion ID*, *NVSC*, and *IAB Europe*, the CJEU has reshaped the boundaries of controllership in unprecedented ways. In three of these cases - *Jehovan todistajat*, *NVSC*, and *IAB Europe* - the Court appealed to a conceptual ideal of controllership defined by an orchestrating role in data processing. However, this reasoning has been inconsistently applied, as evidenced in *Wirtschaftsakademie* and *Fashion ID*, where entities designated as joint controllers exert minimal influence over the processing in question.

Furthermore, a controller can be identified as such even without reaping any 'benefits of joint effort'. In other words, an entity might be deemed a joint controller even if they do not have access to any of the processed data. While in *Belgian state*, we are confronted with a controller which not only does not enjoy access to the data in question, but by virtue of its own legal mandate cannot exercise any influence over it. The hollowing out of this concept would thus appear to be complete as the term controller is now devoid of functional meaning. Moreover, it has been severed from its legal definition as the entity which 'determines the purposes and means of the processing of personal data'.¹⁰¹⁸

¹⁰¹⁷ See [Chapter Three, Section 3 The Ambitions of the EU Data Protection Regime](#).

¹⁰¹⁸ The GDPR, Article 4(7). Emphasis added.

Perhaps most critically, we have observed that while EU Data Protection Law has committed itself to a model of individual control over personal information, the reality of modern data ecosystems has rendered this goal largely unattainable. The advent of complex data flows that intertwine numerous actors has muddied the waters of who truly controls and processes data. This opacity is further compounded by the rise of AI systems, which process vast amounts of data in ways that are often beyond the comprehension of the average user. As a result, individuals find themselves enmeshed in a web of data processing relationships where their ability to manage and oversee their personal data is significantly diminished, if not altogether illusory.

The consequences are numerous. In the first instance (I) legal certainty is weakened as actors, their responsibilities, and liabilities, cannot be easily identified. (II) These uncertainties impact the lawful grounds under which personal data may be processed. Under Article 6 of the GDPR, a lawful basis for processing personal data must be found.¹⁰¹⁹ Where consent is relied upon to justify processing data, the integrity of this consent may be challenged as being insufficiently specific and informed to constitute a legal basis for processing under the GDPR.

(III) Even where lawful grounds to process data do exist, the complexity of data processing relationships will undermine the key data protection principles of 'Fairness' and 'Transparency' found under Article 5 of the GDPR.¹⁰²⁰ Furthermore, (IV) uncertainty in data processing relationships ultimately obscure the

¹⁰¹⁹ See [Chapter Four, Section 5.1 Lawfulness](#).

¹⁰²⁰ See [Chapter Four, Section 5. Principles](#).

pervasiveness of data commodification, making it both harder to understand and respond to as a societal problem.

Finally, (V) the goal of gaining control over personal data is undermined through obscure and increasingly complex processing chains, which can no longer be understood by individuals. At our boldest, we may claim that both *control* and *controllership* have been rendered void of meaning. Neither data subjects nor data controllers themselves hold any true form of power over information, while Supervisory Authorities find their powers misplaced against the wrong actors. This is the real crisis at the heart of the EU's Data Protection Regime.

6. Domains Where the Problem Manifests

This thesis has presented two illustrative cases of *the Problem of Control*. Chapter Eight examined the erosion of the home's status as a physical and legal sanctuary, precipitated by the proliferation of smart home devices. This case study is particularly significant as it challenges long-established legal principles. Despite the traditional exemption of the home from both interference and legal obligations in Privacy and Data Protection Law, *the Problem of Control* nonetheless permeates this domain, highlighting the far-reaching implications of modern technology on conventional legal constructs.

In contrast, Chapter Nine delved into the relatively uncharted territory of AI Service Chains for Data Protection Law. The intricate nature of AI supply chains, with creation, deployment, and utilisation distributed across numerous interconnected stakeholders, presents a formidable challenge to the accountability framework of Data Protection Law. This exploration addressed the fundamental question posed at the outset of this thesis: whether the ambitions of Data Protection Law can still be effectively realised with the tools developed thus far.

6.1 Smart Surveillance and the Disappearing Home

One cannot overlook the deep-seated implications of smart home surveillance devices on the traditionally established boundaries between private and public domains. These devices have eroded the distinct boundaries once attributed to personal and communal spaces.

Moreover, manufacturers of such products often represent themselves merely as processors in the context of the GDPR. However, drawing upon the precedents set by the CNIL and Slovenia's Information Commissioner in relation to cloud computing, there exists a persuasive argument to classify these product manufacturers as joint controllers.¹⁰²¹

This paradigm shift in categorisation is not confined solely to manufacturers. Regular household users, now integrating these surveillance tools into their daily lives, will find themselves inadvertently positioned as controllers or joint controllers under the GDPR framework. The protective umbrella of the household exemption, once thought to be steadfast, now appears increasingly tenuous.¹⁰²² Such a situation leaves these users confronting unexpected responsibilities and liabilities. Like Zuboff, we may pose the question of who is to benefit from the 'immense new stores of knowledge and therefore new power' created by smart home devices?

We are further reminded of Jeremy Bentham's conception of the Panopticon—a structural design for prisons, allowing all inmates to be observed by a single

¹⁰²¹ See [Chapter Eight, Section 6. The Disappearing Household Exemption](#).

¹⁰²² *ibid.*

watchman without the inmates ever knowing if and when they are being observed.¹⁰²³ Bentham's Panopticon serves as a useful, if overused metaphor, in the current discourse on digital surveillance, underscoring the profound interplay between visibility, power, and control.

Advances in online data collection and analysis technologies has created a modern, digital panopticon wherein individuals' online activities can be tracked, analysed, and stored with unprecedented detail and scope. In this virtual panopticon, the role of the singular watchman is assumed by tech corporations, data brokers, and even governmental entities, perpetually monitoring digital interactions.

Similar to the prisoners within Bentham's Panopticon, modern data subjects find themselves embedded within a system of visibility which they can neither fully comprehend nor control. The obscured and asymmetrical nature of this system engenders a profound power dynamic where the watchers hold substantial sway over the watched. It appears that this influence has at last permeated the walls of the home, fulfilling Warren and Brandeis' warning that 'what is whispered in the closet shall be proclaimed from the house-tops.'¹⁰²⁴

7.2 AI Supply Chains and the Limits of the Controller Based Responsibility Model

The limits of Data Protection Law's accountability framework are most fiercely tested in the case of AI Service networks. Supply chains in AI Services are intricate

¹⁰²³ Jeremy Bentham, *The Panopticon Writings* (Ed. M. Božovič) (Verso Books 2010). See also Maša Galič, Tjerk Timan and Bert-Jaap Koops, 'Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation' (2017) 30 *Philosophy & Technology* 9. And Igo (n 53) 225.

¹⁰²⁴ Warren and Brandeis (n 77) 195.

with the creation, deployment, and use of technologies spread across many interconnected stakeholders. This complex web encompasses diverse components, such as data sources, cloud services, and networks each of which may be managed by different entities.

It is important to note that within this vast network, many participants will not be aware of each other, especially if they are not directly connected. However, these participants are not stand-alone entities; their tasks, interrelationships, and influence on AI functionality must be understood within the context of this supply chain. Such mutual dependencies highlight the challenge of allocating clear roles and responsibilities in AI processing chains. The standard model of Data Protection Law acknowledges multiple actors but fails to provide a straightforward application for roles like controller, joint-controller, and processor within the AI context.

Typically, AI service clients might be viewed as data controllers, shouldering the primary responsibility for compliance. Meanwhile, providers, often powerful entities in these supply chains, might be viewed as mere processors. However, the reality is that providers wield considerable influence over AI functionalities. Many clients, usually smaller firms lacking AI proficiency, do not have insights or control over the provider's systems. Despite the provider's significant role, they often diminish their responsibility, labelling themselves as processors in service agreements.

Once more a useful precedent in minimising this result comes from the CNIL and Slovenian Information Commissioner's stance on recognizing cloud service providers as joint controllers. Should this stance gain widespread acceptance, it would ensure greater accountability is placed on the entities best equipped to respond to it.

Yet even this change would not address the scenario where parties, who might be joint controllers, are unaware of each other's existence or have no direct interactions. This is a scenario most likely to emerge in AI processing chains. The regulatory landscape further complicates matters. For instance, a small business could be labelled as a data controller under the GDPR when collaborating with a large software firm. However, under the AI Act, this same business might be considered a mere deployer while the software firm is deemed an AI provider.

Yet even the AI Act's simpler responsibility model fails to address the fluidity and interconnectedness of processing chains. The straightforward classification of AI provider and deployer does not encapsulate the dynamism of supply chains, where the responsibilities of creation, deployment, and utilisation are dispersed amongst various entities. Under such conditions, the AI Act might impose obligations on entities far removed from the production process to guarantee adherence to legal prerequisites related to training and testing, accountability, and risk management in AI production.

The result is the intensification of five of the major repercussions of *the Problem of Control* as outlined in Chapter Seven. Firstly, (I) legal clarity is significantly compromised within AI supply chains as it becomes increasingly complex to pinpoint the roles, responsibilities, and liabilities of involved parties. Moreover, (II) the concept of consent, crucial for lawful data processing, becomes problematic in AI environments where the full extent of data usage is not comprehensible to individuals.

Additionally, (III) the principles of 'Fairness' and 'Transparency,' foundational to Data Protection, are breached due to the exceptional complexity and power imbalances present in AI operations. As a result, (IV) the issue of data

commodification is further obscured. This is compounded as dominant AI providers exploit their market position to manipulate personal data in opaque ways.

Finally, (V) the core tenet of individual autonomy within data protection rights is eroded as personal data is harnessed for AI training in ways that are neither defined nor understandable to data subjects.

In this domain more than any other it seems apparent that the ambitions of the control account of privacy and the goal of ensuring legal certainty may no longer be achieved with the tools which we have thus far developed.

7. Complete and Effective Protection

The European data protection framework aims to establish a comprehensive system of safeguards for personal data. This approach has led the CJEU to apply a broad definition to the role of controller so as to ensure ‘effective and complete protection’ of data subjects.¹⁰²⁵ This expansive interpretation seeks to create a pervasive culture of compliance across diverse entities and contexts. The strategy has shown some success, empowering regulators to address systemic issues more effectively. However, this approach raises questions about the proportionality of compliance burdens and the capacity of smaller entities to navigate complex regulatory requirements. The power imbalance between multinational corporations and smaller joint controllers creates situations where compliance with GDPR requirements may be inherently challenging. Article 26, which

¹⁰²⁵ *Google Spain* at [34]; a close variation of this phrasing appears in *Jehovan todistajat* at [66], *Wirtschaftsakademie* at [45], *Belgian State* at [28], and *IAB Europe* at [55]. It is interesting that in *NVSC* the CJEU only appeals to ‘effective protection’ but does not mention the ideal of complete protection, see *NVSC* at [29].

mandates that joint controllers delineate their respective responsibilities, further complicates this landscape, potentially becoming a legal fiction or a widely disregarded provision when applied to relationships between large technology platforms and smaller entities.

The expansive interpretation of Data Protection Law, driven by the aim of preventing human rights infringements, has become subject to increased scrutiny. Advocate General Bobek suggests that the current interpretation is ‘gradually transforming the GDPR into one of the most de facto disregarded legislative frameworks under EU law’.¹⁰²⁶ This sentiment is echoed in academic discourse, with scholars suggesting that the law’s extensive scope may exceed its capacity for effective compliance and enforcement.¹⁰²⁷

Likewise, the broad scope of the law’s application presents notable challenges for regulators tasked with its interpretation and enforcement. The introduction of the GDPR has led to a marked increase in cases handled by regulators, straining their capacity to manage the increased demand for their services. Furthermore, the diversity of the regulated community, including individuals, charities, political parties, public authorities, and commercial organisations, creates additional challenges for regulators. Achieving a coherent interpretive framework across this heterogeneous group is inherently difficult. Regulators must address a wide array of issues, from systemic concerns in data-centric industries to interpersonal disputes involving smart home devices. This breadth of contexts makes it challenging to provide comprehensive and authoritative guidance applicable to all situations. Open-ended legal principles, such as fairness, are interpreted

¹⁰²⁶ *C-245/20 X and Z v Autoriteit Persoonsgegevens* [2021] EU:C:2021:822, *Opinion of AG Bobek* (n 736).

¹⁰²⁷ See Bygrave and Tosoni (n 319) 13; Koops (n 739); Nolan (n 280) 142.

differently depending on the context, with national regulators adopting divergent interpretations.

The ability to interpret these open-ended principles effectively can be disproportionately challenging for smaller entities and individuals, who often lack the expertise and resources required for proper compliance. Larger organisations may have dedicated legal teams to navigate the nuances of data protection law, whereas smaller actors may struggle to understand and apply abstract principles like fairness. This disparity in capacity further complicates the regulatory landscape and underscores the need for additional support mechanisms to ensure that data protection laws are applied equitably across different sectors and scales of operation.

Ultimately, The CJEU's expansive approach to controllership creates two key challenges for effectiveness. First, in many instances, the law's requirements are practically impossible to comply with in full. Second, the law's broad reach has expanded the diversity of the regulated community, making it harder for all parties to develop a common understanding of the rules and complicating regulators' ability to effectively oversee the wide range of data processing activities under their supervision.

This critique highlights a potential paradox: while the Court justifies its expansive application of the law on human rights grounds, this quest for comprehensive coverage may inadvertently undermine the law's effectiveness and the attainment of these very objectives. As Lynskey notes, 'we must query whether data protection law can be both complete *and* effective'.¹⁰²⁸

¹⁰²⁸ Lynskey, 'Complete and Effective Data Protection' (n 32) 318. Emphasis in the original.

8. Potential Solutions

In Chapter Ten we presented four potential mitigations to *the Problem of Control* found in the literature, supplementing the analyses conducted in earlier sections of this thesis.

The first approach, (I) advocated by Blume and Van Alsenony, suggests increasing obligations for processors. However, this overlooks power imbalances in the industry. A more nuanced approach might focus on imposing stricter regulations specifically on major industry players, similar to the Digital Service Act and Digital Markets Act's treatment of dominant digital entities. Moreover, we have also seen the potential for complementary enforcement mechanisms through the European Commission's investigation into Meta's 'pay or ok' model. We must however be mindful of the potential complexity of overlapping enforcement approaches as has already been highlighted in the Draghi report. Indeed, we must take care not to replace one complexity with another in the name of clarity.

(II) Wong's more radical proposal calls for a transition towards a non-controller accountability framework. This approach, focusing on specific obligations for processing acts without reference to controllership, could potentially offer greater clarity. However, it would require a comprehensive restructuring of Data Protection Law's accountability framework, demanding significant political commitment and co-ordinated legislative efforts.

The third solution (III) proposes revisiting the fundamental concept of 'controller' in jurisprudence. This involves elevating the threshold for determining significant influence over processing means and purposes. The CJEU has shown inconsistency in this area, with some decisions like *Jehovan todistajat* emphasising

an orchestrating role as a requirement for designation as a controller, while others such as *Fashion ID* and *Belgian State* have included actors with limited influence. Future jurisprudence should establish a minimum threshold of orchestrating influence for controller status. This approach would improve transparency, legal certainty, and accountability, aligning with the GDPR's protective aims and economic realities. It would also ensure that risk-management obligations are imposed only on those with actual decision-making power. Implementing this approach requires a shift in judicial perspective and possible legislative action to redefine the scope of controllership.

The fourth solution (IV) suggests a flexible interpretation and enforcement of data protection law by courts and regulators.. This approach raises questions about balancing strict rule application with practical enforcement. While rigid enforcement ensures consistency and deterrence, it risks overwhelming caseloads and disproportionate outcomes for minor infractions. This approach necessitates further exploration of judicial and regulatory flexibility to maintain legal certainty and consistent rights protection. A key advantage of this solution is that the EDPB could provide clarity without extensive legislative changes, offering partial mitigation of issues. However, this approach does not completely resolve the underlying problems, highlighting the need for continued refinement of data protection enforcement strategies.

This thesis concludes by presenting a fifth solution (V) in the form of a comprehensive taxonomy for control relationships within EU Data Protection Law as a pragmatic mitigation to *the Problem of Control*.

When stakeholders have access to well-defined data processing models, their efforts to comply with GDPR requirements become more straightforward. Without such clear guides, SMEs and individuals often find themselves

navigating convoluted legal terrains independently or incurring the cost of hiring specialist consultants. Such a requirement for mandating expertise in this area may be seen as a regressive form of taxation whereby the entry cost of compliance for all businesses dealing with data would be sufficiently high to stifle innovation for all but the largest firms. This ultimately undermines the market supporting aims of the EU's digitally focused regulations.

Furthermore, actors conducting DPIAs can employ these established models, leading to a deeper understanding of related risks. It is worth noting that cutting-edge technological solutions requiring DPIAs often depend on standardised platforms for data management, information capture, and user engagement. Despite unique end outcomes, these tools present consistent challenges regarding data control. The creation of this taxonomy paves the way for a repository of best practices and safety measures tied to these recurring data-sharing dynamics. While the existence of a comprehensive taxonomy may not in itself ensure that the goal of providing individual control is achieved. It can nevertheless allow for greater legal certainty and bolster transparency.

9. Further Research

9.1 Comparative studies

Moving to non-controller-based models of accountability has been highlighted as one potential solution to *the Problem of Control* in Chapter Ten. Further in-depth comparative law research into these models is warranted to determine their value and shortcomings. As has been noted in Chapter Six,¹⁰²⁹ the clearest antecedent to the GDPR's controller-based responsibility model is found in the OECD

¹⁰²⁹ See [Chapter Six, Section 2. Controller Based Accountability: Historical Origins](#)

Guidelines of 1980 and the Council of Europe's Convention 108. As the OECD represents far more than European states and Convention 108 was open to ratification by states outside of Europe it stands to reason that a host of other national and regional laws place key accountability responsibilities on controllers. This includes OECD members like Korea;¹⁰³⁰ Convention 108 Parties like Argentina¹⁰³¹ and Uruguay;¹⁰³² as well as states outside of the OECD and Convention 108 such as Brazil,¹⁰³³ and Kenya.¹⁰³⁴

A comparative law study on the role of controller in these jurisdictions may provide invaluable insight into the nature of *the Problem of Control*. Specifically, we may be better able to determine whether the limits of controllership are a result of a uniquely expansive EU interpretation of this role or if this is an issue inherent in the role itself.

Moreover, starting in 2018 a host of Privacy Laws have been passed at the state level in the United States. Perhaps the most well-known, the Californian CCPA¹⁰³⁵ employs a unique accountability model focusing on 'businesses' as the parties

¹⁰³⁰ South Korea uses the comparable term 'personal information controller' defined in Article 2(5) as 'a public institution, corporate body, organisation, individual, who, by itself or through a third party, processes, i.e., collects, generates, connects, interlocks, records, stores, retains, processes, edits, searches, outputs, corrects, restores, uses, provides, discloses, destroys, or otherwise handles personal data to administer personal data files for official or business purposes'. Personal Information Protection Act 2011 (as amended in 2023) (South Korea).

¹⁰³¹ Bill 87/2023 Bill for the Protection of Personal information 'Proyecto de Ley de Protección de Datos Personales' (2023) (Argentina).

¹⁰³² Although the term controller is not used an equivalent role is to be found under Article 4(K). Law No. 18331 on the Protection of Personal Data and Habeas Data Action (Uruguay).

¹⁰³³ General Data Protection Law 'Lei Geral de Proteção de Dados Pessoais' ('LGPD') As amended by Law No. 13,853/2019) (Brazil).

¹⁰³⁴ The Data Protection Act No. 24 of 2019 (Kenya).

¹⁰³⁵ The California Consumer Privacy Act as Amended November 3, 2020, by initiative Proposition 24. Cal. Civ. Code § 1798.140(v)(2).

responsible for upholding its provisions. In contrast, twelve state laws employ the controller model first introduced in the OECD Guidelines of 1980. These laws are at a nascent stage with only four having entered legal force at the time of writing.¹⁰³⁶ Of these, only the Virginia Consumer Data Protection Act¹⁰³⁷ has been in force for more than one year. As such the role of controller in these laws has had little time to be refined through jurisprudence, guidance, and academic analysis. In the near future, however, the role of the controller in these laws should be included in the larger comparative study outlined above.

9.2 Risk Assessment

A recurring motif in both the GDPR and the AI Act is an emphasis on risk assessment. Under the GDPR controllers are required to assess risks to data subjects in deciding upon the impacts of data breaches,¹⁰³⁸ evaluating new processing operations,¹⁰³⁹ ensuring the security of data processing,¹⁰⁴⁰ and appraising the protection of fundamental rights in international data transfers.¹⁰⁴¹ While the AI Act itself is defined as a risk based legal instrument.¹⁰⁴² It further imposes obligations for both conformity risk assessment and fundamental rights impact assessments. Risk assessment is a specialised field and difficulties in appropriately measuring probability are common.¹⁰⁴³ Further research on risk

¹⁰³⁶ The laws of Virginia, Colorado, Utah, and Connecticut.

¹⁰³⁷ Virginia Consumer Data Protection Act Code § 59.1-571 (2021).

¹⁰³⁸ GDPR, Articles 33 and 34.

¹⁰³⁹ *ibid.* Article 35.

¹⁰⁴⁰ *ibid.* Article 32.

¹⁰⁴¹ European Data Protection Board, 'Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data.' (2021).

¹⁰⁴² See [Chapter Five, Section 2.6 The AI Act](#).

¹⁰⁴³ See for instance Sven Ove Hansson, 'Risk Assessment', *The Routledge Companion to Environmental Ethics* (Routledge 2022); Madeleine Hayenhjelm and Jonathan Wolff, 'The Moral Problem of Risk Impositions: A Survey of the Literature: The Moral Problem of Risk Impositions'

analysis in the fields of Privacy, Data Protection and AI Law is necessary to strengthen certainty. Moreover it may assist in empowering individuals to exercise greater control of the uses to which their data is employed.

To this end taxonomies of recurring risks in this domain may be especially helpful. Through such work it may be possible to (i) identify commonly occurring areas of risk, (ii) standardise templates for the documentation of impact assessments for the deployment of technologies in specific circumstances, (iii) recommend common risk mitigation controls and auditing processes, and (iv) apply a ‘design pattern’ approach to any new use cases or emerging technologies which researchers, practitioners, technology designers and implementers may apply.¹⁰⁴⁴

9.3 Data Harvesting and Controllorship

Although briefly addressed in Chapter Nine,¹⁰⁴⁵ the issue of data harvesting merits greater studying in its own right. Machine learning algorithms, especially those based on neural networks and deep learning, rely heavily on extensive data sets. The approach to regulating the scraping of publicly available data varies. While the GDPR does not exempt publicly available data from its scope, laws in the United States, like the CCPA, offer more flexibility regarding such data. This variability underscores the inconsistency in regulatory approaches across jurisdictions.

(2012) 20 *European Journal of Philosophy* E26; Nate Silver, *The Signal and the Noise: Why so Many Predictions Fail - but Some Don't* (2020 edn, Penguin Books 2020); Robert L Winkler, ‘Uncertainty in Probabilistic Risk Assessment’ (1996) 54 *Reliability Engineering & System Safety* 127; Bouk (n 55).

¹⁰⁴⁴ See Delaram Golpayegani and others, ‘Towards a Taxonomy of AI Risks in the Health Domain’, 2022 *Fourth International Conference on Transdisciplinary AI (TransAI)* (IEEE 2022) <<https://ieeexplore.ieee.org/document/9951508/>> accessed 6 March 2024 and Joshua Hovsha and Daragh O Brian, ‘Drone Use Cases and Their Privacy Impacts: A Taxonomy’ (2023) 27 *Tilburg Law Review* 60.

¹⁰⁴⁵ See [Chapter Nine, Section 3. The Challenge of AI Data Harvesting](#).

Even express consent, as required by the GDPR, does not ensure meaningful understanding of the implications. The advent of AI adds another layer of complexity, rendering the illusion even more elaborate. In the case of generative AI, applications are frequently undefined. Those utilising generative AI tools may employ them for an array of purposes, ranging from harmless to harmful. In this context, consent morphs into open-ended authorisation.

In order to strengthen individual autonomy and bring greater social protection this intersection of privacy, data protection, and AI law must be addressed.

10.4 The Impacts of the DSA and the DMA

One solution to *the Problem of Control* is the imposition of stricter regulations on larger processors. The Digital Service Act and Digital Markets Act were cited as illustrative in levying additional duties and constraints on dominant digital entities.¹⁰⁴⁶ However, both legal instruments are relatively new, with the DMA entering force in May 2023, while the DSA's rules have only entered into full effect on 17 February 2024. As such the value of these regulations cannot yet be known. Research on their impacts and interpretation in jurisprudence may yield further insight into whether this model is appropriate for adoption in Data Protection Law.

¹⁰⁴⁶ See [Chapter Ten, Section 2. Extended Responsibilities for Processors.](#)

Bibliography

Books

- Arendt H, *The Origins of Totalitarianism* (Kindle edn, Penguin 2017)
- Aristotle, *Aristotle's Politics Translated and with an Introduction, Notes, and Glossary* by Carnes Lord (Carnes Lord tr, 2nd edn, University of Chicago Press 2013)
- Bentham J, *The Panopticon Writings* (Ed. M. Božovič) (Verso Books 2010)
- Bieker F, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law* (Asser Press 2022)
- Black J, *Rules and Regulators* (Clarendon Press; Oxford University Press 1997)
- Bok S, *Secrets: On the Ethics of Concealment and Revelation* (Vintage Books 1989)
- Borgwardt E, *A New Deal for the World: America's Vision for Human Rights* (Harvard University Press 2007)
- Bouk DB, *How Our Days Became Numbered: Risk and the Rise of the Statistical Individual* (Paperback edn, University of Chicago Press 2018)
- Bradley M, *The World Reimagined: Americans and Human Rights in the Twentieth Century* (Cambridge University Press 2016)
- Browne S, *Dark Matters: On the Surveillance of Blackness* (Duke University Press 2015)
- Bygrave LA, *Data Privacy Law: An International Perspective* (Oxford University Press 2014)
- Cooley TM, *A Treatise on the Law of Torts, or the Wrongs Which Arise Independently of Contract* (3rd Edition, Callaghan & company 1906)
- Costello RÁ, *Privacy Law in Ireland* (Bloomsbury Publishing 2023)
- De Gregorio G, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022)
- de Tocqueville A, *Democracy in America: The Complete and Unabridged Volumes I and II*. Translated by H. Reeve. (Bantam Classics 2000)
- —, *Ancien Regime and the Revolution*. Translated by G. Bevan (Penguin 2008)
- DeCew JW, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press 1997)

Dent N, *Rousseau* (Routledge 2008)

Didier E, Porter TM and Sen PV, *America by the Numbers: Quantification, Democracy, and the Birth of National Statistics* (The MIT Press 2020)

Dunn J, 'Practising History and Social Science on "Realist" Assumptions:', *Political Obligation in its Historical Context: Essays in Political Theory*. (Cambridge University Press 1980)

— —, 'The Identity of the History of Ideas', *Political Obligation in its Historical Context: Essays in Political Theory*, edited by J. Dunn (Cambridge University Press 1980)

— —, *The History of Political Theory and Other Essays*. (Cambridge University Press 1996)

Eisenstein E, *The Printing Revolution in Early Modern Europe* (Cambridge University Press 1993)

Flynn B, *The Philosophy of Claude Lefort: Interpreting the Political* (Northwestern University Press 2005)

Foucault M, *Discipline and Punish: The Birth of the Prison* (2nd ed, Vintage Books 1995)

Fuller LL, *The Morality of Law* (Revised edn, Yale University Press 1969)

Gandy OH, *The Panoptic Sort: A Political Economy of Personal Information* (Oxford University Press 2021)

González Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer International Publishing 2014)

— —, *Study on the Essence of the Fundamental Rights to Privacy and to the Protection of Personal Data* (European Data Protection Supervisor 2023)

Hansson SO, *The Routledge Companion to Environmental Ethics* (Routledge 2022)

Hartzog W, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018)

Hellman JJ, *Privacy and Information Systems: An Argument and an Implementation* (Rand Corporation 1970)

Hill K, *Your Face Belongs to Us: A Secretive Startup's Quest to End Privacy as We Know It* (1st edn, Random House 2023)

Hogan G and others, *Kelly: The Irish Constitution* (5th edn, Bloomsbury Professional 2018)

Igo SE, *The Averaged American: Surveys, Citizens, and the Making of a Mass Public* (Harvard University Press 2008)

Bibliography

- —, *The Known Citizen* (Harvard University Press 2018)
- Kittler FA, *Gramophone, Film, Typewriter* (Stanford University Press 1999)
- Lefort C, *Democracy and Political Theory*. Trans. D. Macey. (Polity Press 1988)
- Luger GF and Stubblefield WA, *Artificial Intelligence: Structures and Strategies for Complex Problem Solving* (2nd edn, Benjamin/Cummings Pub Co 1993)
- Lynskey O, *The Foundations of EU Data Protection Law* (Oxford University Press 2015)
- McCoy AW, *Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State* (University of Wisconsin Press 2009)
- Merchant EK, *Building the Population Bomb* (Oxford University Press 2021)
- Mounk Y, *The People vs. Democracy* (Harvard University Press 2018)
- Moyn S, *The Last Utopia: Human Rights in History* (Harvard University Press 2012)
- Muhammad KG, *The Condemnation of Blackness: Race, Crime, and the Making of Modern Urban America* (Harvard University Press 2019)
- Murphy MH, *Surveillance and the Law: Language, Power, and Privacy* (Routledge, Taylor & Francis Group 2020)
- Naughton J, *From Gutenberg to Zuckerberg* (Quercus 2012)
- Newman AL, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Cornell University Press 2008)
- Nissenbaum H, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford Law Books 2010)
- O'Brien DM, *Privacy, Law, and Public Policy* (Praeger 1979)
- Orvell M, *American Photography* (Oxford University Press 2003)
- Porcedda MG, *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis* (Hart 2023)
- Posner RA, *The Economics of Justice* (Harvard University Press 2003)
- Regan PM, *Legislating Privacy: Technology, Social Values, and Public Policy* (The University of North Carolina Press 2000)
- Reus-Smit C, *Individual Rights and the Making of the International System* (Cambridge University Press 2013)

Bibliography

- Richardson M, *The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea* (Cambridge University Press 2017)
- Rosen J, *The Unwanted Gaze: The Destruction of Privacy in America* (1st Vintage Books ed, Vintage Books 2001)
- Rossler B, *The Value of Privacy* (Polity Press 2005)
- Rousseau J-J, *The Social Contract* (Wordsworth Classics 1762)
- Russell SJ and Norvig P, *Artificial Intelligence: A Modern Approach* (3rd edn, Pearson 2016)
- Seipp DJ, *The Right to Privacy in American History* (Harvard University, Program on Information Resources Policy 1978)
- Siedentop L, *Inventing the Individual: The Origins of Western Liberalism* (Belknap Press of Harvard University Press 2014)
- Silver N, *The Signal and the Noise: Why so Many Predictions Fail - but Some Don't* (2020 edn, Penguin Books 2020)
- Skowronek S, *Building a New American State: The Expansion of National Administrative Capacities, 1877-1920* (Cambridge University Press 1982)
- Solove DJ, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press 2004)
- —, *Understanding Privacy* (Harvard University Press 2010)
- Tooze A, *Statistics and the German State, 1900-1945: The Making of Modern Economic Knowledge* (Cambridge University Press 2001)
- Van Alsenoy B, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia 2019)
- Waldman AE, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge University press 2021)
- Westin AF, *Privacy and Freedom* (Scribner 1967)
- Westin AF and Baker MA, *Databanks in a Free Society* (Quadrangle Books 1972)
- Wiggins C and Jones ML, *How Data Happened: A History from the Age of Reason to the Age of Algorithms* (First edition, W W Norton & Company 2023)
- Wittgenstein L, *Philosophical Investigations* (Basil Blackwell 1968)
- Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019)

Portions of Edited Volumes

Alhadeff J, Van Alsenoy B and Dumortier J, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions' in Daniel Guagnin and others (eds), *Managing Privacy through Accountability* (Palgrave Macmillan 2012)

Ayres I and Braithwaite J, 'Responsive Regulation: Transcending the Deregulation Debate' in Martin Lodge, Edward C Page and Steven J Balla (eds), *The Oxford Handbook of Classics in Public Policy and Administration The Oxford Handbook of Classics in Public Policy and Administration*, vol 1 (Oxford University Press 2016)

Benn SI, 'Privacy, Freedom, and Respect for Persons' in Ferdinand David Schoeman (ed), *Philosophical Dimensions of Privacy* (1st edn, Cambridge University Press 1984)

Bennett CJ and Bayley RM, 'Privacy Protection in the Era of "Big Data": Regulatory Challenges and Social Assessments' in Bart van der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016)

Blume P, 'An Alternative Model for Data Protection Law: Changing the Roles of Controller and Processor' (2015) 5 *International Data Privacy Law* 292

Boardman R and Fenelon J, 'Territorial and Material Scope of the General Data Protection Regulation' in Eduardo Ustaran (ed), *European Data Protection* (2nd edn, IAPP Publications 2019)

Bognetti G, 'The Concept of Human Dignity in European and US Constitutionalism' in Georg Nolte (ed), *European and US Constitutionalism* (Cambridge University Press 2005)

Bygrave LA and Tosoni L, 'Article 4(1): Personal Data' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020)

De Hert P and Gutwirth S, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009)

de Terwangne C, 'Article 5: Principles Relating to Processing of Personal Data' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020)

Dobson I and Johns F, 'Legal Research as Qualitative Research' in Mike McConville and Wing Hong Chui (eds), *Research Methods For Law* (2nd edn, Edinburgh University Press 2017)

Drechsler L and Kamara I, 'Essential Equivalence as a Benchmark for International Data Transfers After Schrems II', in Eleni Kosta, Ronald Leenes, and Irene Kamara (eds.), *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022)

Filippidis M, 'Data Processing Principles' in Eduardo Ustaran (ed), *European Data Protection* (2nd edn, IAPP Publications 2019)

Georgieva L and Kuner C, 'Article 9: Processing of Special Categories of Personal Data' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020)

Gerstein RS, 'Intimacy and Privacy' in Ferdinand D Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press 1984)

Hamilton L, 'The Power of the Past: The Future of Intellectual History in South Africa' in Peter Vale, Lawrence Hamilton and Estelle Prinsloo (eds), *Intellectual Traditions in South Africa: Ideas, Institutions and Individuals* (University of KwaZulu-Natal Press 2014)

Hubert D, 'The Responsibility to Protect: Preventing and Halting Crimes Against Humanity' in Robert I Rotbert (ed), *Mass Atrocity Crimes: Preventing Future Outrages* (Brookings Institution Press)

Kranenborg H, 'Article 2: Material Scope' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020)

Kremer J, 'On the End of Freedom in Public Spaces: Legal Challenges of Wide-Area and Multiple-Sensor Surveillance Systems', *Surveillance, counter-terrorism and comparative constitutionalism* (Routledge 2014)

Lock T, 'Articles 51-54', in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds.), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, (Oxford University Press 2019)

Macmillan M, 'Data Protection Concepts' in Eduardo Ustaran (ed), *European Data Protection* (3rd edn, IAPP Publications 2023)

McMullan K, 'Legislative Framework' in Eduardo Ustaran (ed), *European Data Protection* (2nd edn, IAPP Publications 2019)

Moore D, 'Article 23: Restrictions', in Christopher Kuner, Lee Bygrave, Christopher Docksey and Laura Drechsler (eds.), *The EU General Data Protection Regulation: A Commentary*. (Oxford University Press 2020)

Nemitz P, 'Article 82 GDPR, Margin Number 7', in Ehmann and Selmayr, *Data Protection Regulation*, (2nd edn, CH Beck 2018)

Bibliography

Porcedda MG, 'On Boundaries. Finding the Essence of the Right to the Protection of Personal Data.' in Ronald Leenes and others (eds), *Privacy and Data Protection: The Internet of Bodies* (Hart Publishing 2018)

Rotbert RI, 'Deterring Mass Atrocity Crimes: The Cause of Our Era,'" in Robert I Rotbert (ed), *Mass Atrocity Crimes: Preventing Future Outrages* (Brookings Institution Press 2010)

Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009)

Rudgard S, 'Origins and Development of European Data Protection Law' in Eduardo Ustaran (ed), *European Data Protection* (2nd edn, IAPP Publications 2019)

Skinner Q, 'Meaning and Understanding in the History of Ideas', in Q. Skinner (ed), *Visions of Politics Volume I: Regarding Method*, (Cambridge University Press 2002)

Taekema S, 'Relative Autonomy, A Characterisation of the Discipline of Law' in Bart van Klink and Sanne Taekema (eds), *Law and method: interdisciplinary research into law* (Mohr Siebeck 2011)

Tosoni L and Bygrave LA, 'Article 4(2): Processing' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020)

Wrigley S, "'When People Just Click": Addressing the Difficulties of Controller/Processor Agreements Online' in Marcelo Corrales Compagnucci, Mark Fenwick and Helena Haapio (eds), *Legal Tech, Smart Contracts and Block Chain, Perspectives In Law, Business and Innovation* (Springer Nature 2019)

Zanfir-Fortuna G, 'Article 82: Right to Compensation and Liability', in Christopher Kuner, Lee Bygrave, Christopher Docksey and Laura Drechsler (eds.), *The EU General Data Protection Regulation: A Commentary*. (Oxford University Press 2020)

Journal Articles and Conference Papers

Allen AL, *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*, vol 21 (Rowman & Littlefield Publishers 2003)

Angel MP and Calo R, 'Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy' (2024) 124 *Columbia Law Review* 507

Baloup J, 'The Data Governance Act: New Rules for International Transfers of Non-Personal Data Held by the Public Sector' (*European Law Blog*, 10 June 2021) <<https://europeanlawblog.eu/2021/06/10/the-data-governance-act-new-rules-for-international-transfers-of-non-personal-data-held-by-the-public-sector/>> accessed 16 November 2023

Bibliography

- Battaglia D, 'Coming in at an Unusual Angle: Exo-Surprise and the Fieldworking Cosmonaut' (2012) 85 *Anthropological Quarterly* 1089
- Bezanson RP, 'The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990' (1992) 80 *California Law Review* 1133
- Bratman B, 'Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy' (2001) 69 *Tennessee Law Review* 623
- Brkan M, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core' (2018) 14 *European Constitutional Law Review* 332
- Bygrave LA, 'Core Principles of Data Protection' (2001) 7 *Privacy Law and Policy Reporter* 169
- Calo MR, 'The Boundaries of Privacy Harm' (2011) 86 *Indiana Law Journal* 1131
- Chen J and others, 'Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllorship and the Household Exemption' (2020) 10 *International Data Privacy Law* 279
- Cobbe J, Norval C and Singh J, 'What Lies beneath: Transparency in Online Service Supply Chains' (2020) 5 *Journal of Cyber Policy* 65
- Cobbe J and Singh J, 'Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges' (2021) 42 *Computer Law & Security Review* 105573
- Cobbe J, Veale M and Singh J, 'Understanding Accountability in Algorithmic Supply Chains' (SocArXiv 2023) <<https://osf.io/p4sey>> accessed 10 March 2024
- Cohen JE, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 *Stanford Law Review* 1373
- Costello RÁ, 'Warren and Brandeis and the Right to Privacy's Hollow Core.' [2015] *Kings Inns Law Review*
- —, 'Impacts of AdTech on Privacy Rights and the Rule of Law' [2020] *Technology and Regulation* 11
- —, 'Genetic Data and The Right to Privacy: Towards a Relational Theory of Privacy?' (2022) 22 *Human Rights Law Review* 1
- —, 'Schrems II: Everything Is Illuminated' (2020) 5 *European Papers* 1045
- Davenport T and Kalakota R, 'The Potential for Artificial Intelligence in Healthcare.' (2019) 6 *Future Healthcare journal* 94
- De Hert P and Papakonstantinou V, 'Framing Big Data in the Council of Europe and the EU Data Protection Law Systems: Adding "Should" to "Must" via Soft Law to Address More than Only Individual Harms' (2021) 40 *Computer Law & Security Review* 105496

Bibliography

- DeCew JW and Allen AL, 'Uneasy Access: Privacy for Women in a Free Society.' (1992) 101 *The Philosophical Review* 709
- Diggelmann O and Cleis MN, 'How the Right to Privacy Became a Human Right' (2014) 14 *Human Rights Law Review* 441
- Duan Y and others, 'Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends', *2015 IEEE 8th International Conference on Cloud Computing* (2015)
- Ducuing C, Schroers J and Kindt E, 'The Wirtschaftsakademie Fan Page Decision: A Landmark on Joint Controllership - A Challenge for Supervisory Authorities Competences Case Notes' (2018) 4 *European Data Protection Law Review* (EDPL) 547
- Dunne N, 'Knowing When to See It: State Activities, Economic Activities, and the Concept of Undertaking' 16 *Columbia Journal of European Law* 427
- Edwards L and others, 'Data Subjects as Data Controllers: A Fashion(Able) Concept?' (*Internet Policy Review*) <<https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400>> accessed 23 March 2024
- Falk R, 'Revisiting Westphalia, Discovering Post-Westphalia' (2002) 6 *The Journal of Ethics* 311
- Finck M, 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law' (2021) 11 *International Data Privacy Law* 333
- Finck M and Pallas F, 'They Who Must Not Be Identified — Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 *International Data Privacy Law* 11
- Freund P, 'Address at the American Law Institute, 52nd Annual Meeting 42-43'
- Fried C, 'Privacy' (1968) 77 *The Yale Law Journal* 475
- Furey E and Blue J, 'Alexa, Emotions, Privacy and GDPR', *Proceedings of the 32nd International BCS Human Computer Interaction Conference* 32 (2018)
- Galič M, Timan T and Koops B-J, 'Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation' (2017) 30 *Philosophy & Technology* 9
- Gavison R, 'Privacy and the Limits of Law' (1980) 89 *The Yale Law Journal* 421
- Geenens R, 'Modernity Gone Awry: Lefort on Totalitarian and Democratic Self-Representation' (2012) 13 *Critical Horizons* 74
- Gerety T, 'Redefining Privacy' (1977) 12 *Harvard Civil Rights and Civil Liberties Law Review*
- Glancy DJ, 'The Invention of the Right to Privacy' (1979) 21 *Arizona Law Review* 1

Globocnik J, 'On Joint Controllorship for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID: Directive 95/46/EC, Arts. 2(d) and (h), 7(a) and (f), 10.' (2019) 50 IIC - International Review of Intellectual Property & Competition Law 1033

Golpayegani D and others, 'Towards a Taxonomy of AI Risks in the Health Domain' (2022) <<https://doi.org/10.5281/zenodo.7311185>>

Gömann M, 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) 54 Common Market Law Review 567

Gross H, 'Privacy and Autonomy' (1971) 13 Nomos: Yearbook of the American Society for Political and Legal Philosophy 169

Gutermuth A, Italianer A and Thiry L, 'Europe's Digital Markets Act: New Regulation of Gatekeepers in the Digital Platform Economy.' (2022) 34 Intellectual Property & Technology Law Journal 15

Hartzog W 'The Case Against Idealising Control' (2018) 4 European Data Protection Law Review

— —, 'What Is Privacy? That's the Wrong Question' (2021) 88 University of Chicago Law Review 1677

Hehir A, 'The Responsibility to Protect in International Political Discourse: Encouraging Statement of Intent or Illusory Platitudes?' (2011) 15 The International Journal of Human Rights,

Helberger N and Hoboken J van, 'Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers' (2010) 11 Computer Law Review International 101

Hintze M, 'Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR' (2018) 22 Journal of Internet Law 17

Hirsch D, 'From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics' (2020) 79 Maryland Law Review 439

Hon WK, Millard C and Walden I, 'Who Is Responsible for "personal Data" in Cloud Computing?--The Cloud of Unknowing, Part 2' (2012) 2 International Data Privacy Law 3

Hondius FW, 'Data Law in Europe' (1980) 16 Stanford Journal of International Law 87

Hornung G and Schnabel C, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 Computer Law & Security Review 84

Bibliography

- Hovsha J and Brian DO, 'Drone Use Cases and Their Privacy Impacts: A Taxonomy' (2023) 27 *Tilburg Law Review* 60
- Ian Goldberg, Austin Hill, and Adam Shostack, 'Trust, Ethics and Privacy. 81(2): .' (2001) 81 *Boston University Law Review* 407
- Irwin Altman, 'Privacy: A Conceptual Analysis' (1976) 8 *Environment and Behavior* 141
- Jain S and Purohit HC, 'Consumer Acceptance of Online Behavioural Advertising: Role of Persuasion Knowledge and Protection Motivation.' (2022) 18 48
- Janžekovič I, 'The Balance of Power from the Thirty Years' War and the Peace of Westphalia (1648) to the War of the Spanish Succession and the Peace of Utrecht (1713)' (2023) 49 *History of European Ideas* 561
- Javadi SA and others, 'Monitoring Misuse for Accountable "Artificial Intelligence as a Service"', *Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society* (arXiv 2020) <<http://arxiv.org/abs/2001.09723>> accessed 1 June 2023
- Jenkins RV, 'Technology and the Market: George Eastman and the Origins of Mass Amateur Photography' (1975) 16 *Technology and Culture* 1
- Kelly KA, 'The Ring Video Doorbell and the Entry of Amazon into the Smart Home: Implications for Consumer-Initiated Surveillance.' (2023) 46 *Journal of Consumer Policy* 95
- Kidd CD and others, 'The Aware Home: A Living Laboratory for Ubiquitous Computing Research', *Proceedings of the Second International Workshop on Cooperative Buildings, Integrating Information, Organization, and Architecture* (Springer-Verlag 1999)
- Koops B-J, 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 250
- Kramer IR, 'The Birth of Privacy Law: A Century since Warren and Brandeis' (1989) 39 *Catholic University Law Review* 703
- Kuan Hon W, Millard C and Singh J, 'Cloud Technologies and Services' in Christopher Millard (ed), *Cloud Computing Law* (Oxford University Press 2021) <<https://doi.org/10.1093/oso/9780198716662.003.0001>> accessed 22 March 2023
- Kuner C, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18 *German Law Journal* 881
- Kuru T and Beriain IDM, 'Your Genetic Data Is My Genetic Data: Unveiling Another Enforcement Issue of the GDPR' (2022) 47 *Computer Law & Security Review* 105752

- Lau J, Zimmerman B and Schaub F, 'Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers' (2018) 2 *Proceedings of the ACM on human-computer interaction* 1
- Lawson G, 'The Rise and Rise of the Administrative State' (1994) 107 *Harvard Law Review* 1231
- LeCun Y, Bengio Y and Hinton G, 'Deep Learning' (2015) 521 *Nature* 436
- Lee EW, 'Political Science, Public Administration, and the Rise of the American Administrative State' [1995] *Public Administration Review* 538
- Lenaerts K, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 *German Law Journal* 779
- Lewicki K and others, 'Out of Context: Investigating the Bias and Fairness Concerns of "Artificial Intelligence as a Service"', *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2023) <<https://doi.org/10.1145/3544548.3581463>> accessed 24 March 2024
- Lindroos-Hovinheimo S, 'Who Controls Our Data? The Legal Reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojaalvauttettu v Jehovan Todistajat*' 28 *Information & Communications Technology Law* 225
- Louisa Specht-Riemenschneider and Ruben Schneider, 'Stuck Half Way: The Limitation of Joint Control after *Fashion ID* (C-40/17) : Case Note – *Fashion ID* (C-40/17)' (*GRUR international*, 2020)
- Lubar S, "'Do Not Fold, Spindle or Mutilate": A Cultural History of the Punch Card' (1992) 15 *Journal of American Culture* 43
- Lundgren B, 'A Dilemma for Privacy as Control' (2020) 24 *The Journal of Ethics* 165
- Lynskey O, 'Deconstructing Data Protection: The "Added-Value" of a Right To Data Protection in the EU Legal Order' (2014) 63 *International and Comparative Law Quarterly* 569
- , 'Another Turn of the Screw? The "Facebook Fanpages" Judgment' (*European Law Blog*, 25 June 2018) <<https://europeanlawblog.eu/2018/06/25/another-turn-of-the-screw-the-facebook-fanpages-judgment/>> accessed 23 March 2024
- , 'Complete and Effective Data Protection' (2023) 76 *Current Legal Problems* 297
- Macnish K, 'Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World' (2018) 35 *Journal of Applied Philosophy* 417
- Mahieu R, 'The Right of Access to Personal Data: A Genealogy' (2021) 2021 *Technology and Regulation* 62

Bibliography

- Mahieu R and van Hoboken J, 'Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?' (*European Law Blog*, 30 September 2019) <<https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/>> accessed 23 March 2024
- Mahieu R, van Hoboken J and Asghari H, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and Its Application to Data Access Rights in Europe, 10 (2019) Para 1.' (2019) 10 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 85
- Margulis ST, 'Conceptions of Privacy: Current Status and Next Steps' (1977) 33 *Journal of Social Issues* 5
- Meurisch C and Mühlhäuser M, 'Data Protection in AI Services: A Survey' (2022) 54 *ACM Computing Surveys* 1
- Millard C, 'At This Rate, Everyone Will Be a [Joint] Controller of Personal Data!' (2019) 9 *International Data Privacy Law* 217
- Minorini K, 'A Vendetta against Alexa: Privacy Concerns in the Age of the Smart Home' (2021) *Boston College Intellectual Property and Technology Forum* 1
- Mou Y and Meng X, 'Alexa, It Is Creeping over Me - Exploring the Impact of Privacy Concerns on Consumer Resistance to Intelligent Voice Assistants' (2024) 36 *Asia Pacific Journal of Marketing and Logistics* 261
- Murphy MH, 'Assessing the Implications of Schrems II for EU-US Data Flow' (2022) 71 *International and Comparative Law Quarterly* 245
- Murphy C, 'Anyone Who Thinks We've Now Grasped What the Internet Has in Store for Us Should Revisit What the Printing Press Unleashed.' (2020) January, *The Atlantic* 4
- Nissenbaum H, 'Accountability in a Computerized Society' (1996) 2 *Science and Engineering Ethics* 25
- Papakonstantinou V and De Hert P, 'Post GDPR EU Laws and Their GDPR Mimesis. DGA, DSA, DMA and the EU Regulation of AI' (*European Law Blog*, 1 April 2021) <<https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/>> accessed 7 March 2024
- Parent WA, 'Privacy, Morality, and the Law' (1983) 12 *Philosophy and Public Affairs* 269
- Parker R, 'A Definition of Privacy' (1974) 27 *Rutgers Law Review* 275
- Pfeifle A, 'Alexa, What Should We Do about Privacy: Protecting Privacy for Users of Voice-Activated Devices Comments' (2018) 93 *Washington Law Review* 421

Podlech A, 'Die Begrenzung Staatlicher Informationsverarbeitung Durch Die Verfassung Angesichts Der Möglichkeit Unbegrenzter Informationsverarbeitung Mittels Der Technik: Zur Entscheidung Des Bundesverfassungsgerichts Über Das Volkszählungsgesetz 1983' (1984) 12 *Leviathan* 85

Post RC, 'Three Concepts of Privacy' (2001) 89 *The Georgetown Law Journal* 2087

Purtova N, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table ... and Back on Again?' (2014) 30 *Computer Law & Security Review* 6

— —, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 *Law, Innovation and Technology* 40

Qiu J and others, 'A Survey of Machine Learning for Big Data Processing' (2016) 2016 *EURASIP Journal on Advances in Signal Processing* 67

Quelle C, 'GC and Others v CNIL on the Responsibility of Search Engine Operators for Referring to Sensitive Data: The End of "Right to Be Forgotten" Balancing?' (2019) 5 *European Data Protection Law Review* 438

Quintais JP and Schwemer SF, 'The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?' (2022) 13 *European Journal of Risk Regulation (EJRR)* 191

Rebecca Wong, 'Social Networking: A Conceptual Analysis of a Data Controller' (2009) 14 *Communications Law* 142

Reidenberg JR, 'Privacy Wrongs in Search of Remedies' 54 *Hastings Law Journal* 877

Revathi R, 'Evolution of Privacy Jurisprudence – A Critique' (2018) 60 *Journal of the Indian Law Institute* 189

Richards NM and Hartzog W, 'Privacy's Constitutional Moment' (2020) 61 *Boston College Law Review* 1687

Risse M, 'What to Say About the State' (2006) 32 *Social Theory and Practice* 671

Rothkegel T and Strassemeyer L, 'Joint Control in European Data Protection Law – How to Make Sense of the CJEU's Holy Trinity - A Case Study on the Recent CJEU Rulings (Facebook Fanpages; Jehovah's Witnesses; Fashion ID).' (2019) 20 *Computer Law Review International* 161

Scanlon T, 'Thomson on Privacy' (1975) 4 *Philosophy and Public Affairs* 315

Scheuerman MK, Paul JM and Brubaker JR, 'How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis Services' (2019) 3 *Proc. ACM Hum.-Comput. Interact.* <<https://doi.org/10.1145/3359246>>

Bibliography

Schneier B, 'A Taxonomy of Social Networking Data' (2010) 8 IEEE Security & Privacy 88

Schwartz P, 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination' (1989) 37 The American Journal of Comparative Law 675

Schwartz PM, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review 1607

Schwartz PM and Solove DJ, 'Reconciling Personal Information in the United States and European Union' (2014) 102 California Law Review 877

Simitis S, 'Reviewing Privacy In an Information Society' (1987) 135 University of Pennsylvania Law Review 707

Singh J, Cobbe J and Norval C, 'Decision Provenance: Harnessing Data Flow for Accountable Systems' (2019) 7 IEEE Access 6562

Sioli L, 'A European Strategy for Artificial Intelligence' (CEPS webinar -European approach to the regulation of artificial intelligence, 23 April 2021)

Sloot B van der, 'Truth from the Sewage: Are We Flushing Privacy down the Drain?' (2021a) 12 European Journal of Law and Technology

Smuha NA, 'Beyond the Individual: Governing AI's Societal Harm' 10 Internet Policy Review

—, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' <<https://ssrn.com/abstract=3899991>> accessed 24 March 2024

Solove DJ, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087

—, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477

—, 'Privacy Self-Management and the Consent Dilemma', (2013) 126 Harvard Law Review 1880

—, 'The Limitations of Privacy Rights' (2023) 98 Notre Dame Law Review 975

—, 'Against Privacy Essentialism' [2024] SSRN Electronic Journal <<https://www.ssrn.com/abstract=4826385>> accessed 25 July 2024

—, 'Artificial Intelligence and Privacy' (1 February 2024)

Solove DJ and Hartzog W, 'Kafka in the Age of AI and the Futility of Privacy as Control' (2024) 104 Boston University Law Review 1024

Stauffer DJ, 'Tocqueville on the Modern Moral Situation: Democracy and the Decline of Devotion' (2014) 108 *The American Political Science Review* 772

Strawn G, 'Masterminds of Punched Card Data Processing: Herman Hollerith and John Billings' (2023) 25 *IT Professional* 90

Strugala R, 'Art. 82 GDPR: Strict Liability Or Liability Based on Fault?' (2020) 2020 *European Journal of Privacy Law & Technologies (EJPLT)* 71

Stuchebrukhov O, "'Ridiculous" Dream versus Social Contract: Dostoevskij, Rousseau, and the Problem of Ideal Society' (2007) 59 *Studies in East European Thought* 101

Tedlow RS, 'The Beginning of Mass Marketing in America: George Eastman and Photography as a Case Study' (1997) 17 *Journal of Macromarketing* 67

Thomson JJ, 'The Right to Privacy' (1975) 4 *Philosophy and Public Affairs* 295

Thouvenin F, 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?' (2021) 12 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 246

Tosi E, 'Unlawful Data Processing Prevention and Strict Liability Regime under EU GDPR' (2021) 7 *Italian Law Journal* 873

Van Alsenoy B, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 271

Van Alsenoy B and others, 'Social Networks and Web 2.0: Are Users Also Bound by Data Protection Regulations?' (2009) 2 *Identity in the Information Society* 65

Van Cleynenbreuge P, 'Digital Markets Act: Beware of Procedural Fairness and Judicial Review Booby-Traps!' (*European Law Blog*, 24 June 2021)
<<https://europeanlawblog.eu/2021/06/24/digital-markets-act-beware-of-procedural-fairness-and-judicial-review-booby-traps/>> accessed 23 March 2024

van den Haag E, 'On Privacy' (1971) 13 *Nomos: Yearbook of the American Society for Political and Legal Philosophy* 149

Van Der Sloot B, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"' (2015) 31 *Utrecht Journal of International and European Law* 25

Van Eecke P and Truyens M, 'Privacy and Social Networks' (2010) 26 *Computer, Law & Security Review* 535

Van Ooijen I and Vrabec HU, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 *Journal of Consumer Policy* 91

Veale M and Zuiderveen Borgesius F, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 4 Computer Law Review International 97

Warren S and Brandeis L, 'The Right to Privacy' (1890) 4 Harvard Law Review

Whitman JQ, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2003) 113 Yale Law Journal 1151

Wong B, 'Problems with Controller-Based Responsibility in EU Data Protection Law' (2021) 11 International Data Privacy Law 375

Woods L, 'EU Law Analysis: Facebook Fan Pages and EU Data Protection Law: The Implications of Unabhängiges Landeszentrum Für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH' (*EU Law Analysis*, 3 July 2018) <<https://eulawanalysis.blogspot.com/2018/07/facebook-fan-pages-and-eu-data.html>> accessed 23 March 2024

Yeung K and Bygrave LA, 'Demystifying the Modernized European Data Protection Regime: Cross-disciplinary Insights from Legal and Regulatory Governance Scholarship' (2022) 16 Regulation & Governance 137

Zalnieriute M and Churches G, 'When a "Like" Is Not a "Like": A New Fragmented Approach to Data Controllorship' (2020) 83 Modern Law Review 861

Government and Regulatory Body Reports, Press Releases, and Guidance

Article 29 Working Party ('WP29'), 'Guidelines on Data Protection Impact Assessment (DPIA) WP248. Endorsed by the European Data Protection Board on 25 May 2018' (2018)

— — 'Opinion 1/2008 on Data Protection Issues Related to Search Engines. Adopted 4 April 2008' (2008) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf> accessed 13 March 2024

— —, 'Opinion 5/2009 on Online Social Networking Adopted on 12 June 2009 01189/09/EN WP 163'

— —, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"'

— —, 'Opinion 05/2012 on Cloud Computing 01037/12/EN WP 196'

— —, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks, Adopted on 30 May 2014 (WP218)'

Belgian Data Protection Authority ('Autorité de protection des données Gevevensbeschermingsautoriteit', 'General Secretariat Decision N° 05/2021 of 20 May 2021'

Commission nationale de l'informatique et des libertés (CNIL), 'Cloud Computing : CNIL's Recommendations for Companies Using These New Services' (2012) <<https://www.cnil.fr/en/cloud-computing-cnils-recommendations-companies-using-these-new-services>> accessed 19 July 2023

— —, 'Law Enforcement Directive: What Are We Talking About? | CNIL' <<https://www.cnil.fr/en/law-enforcement-directive-what-are-we-talking-about>> accessed 13 March 2024

— —, 'Délibération N° 2018-326 Du 11 Octobre 2018 Portant Adoption de Lignes Directrices Sur Les Analyses d'impact Relatives à La Protection Des Données (AIPD) Prévues Par Le Règlement Général Sur La Protection Des Données (RGPD)' (2018) 81 Légifrance - Publications officielles - Journal officiel

Commission of the European Communities, 'Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM(92) 422 Final – SYN 287, 15 October 1992, OJ 27 November 1992, C 311/30-61' (m)

Commission of the European Communities, 'Opinion of the Commission Pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament's Amendments to the Council's Common Position Regarding the Proposal for a European Parliament and Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM(95) 375 Final- COD287, 18 July 1995.'

Council of EU, 'Note from Presidency to JHA Counsellors on the Proposed General Data Protection Regulation – Chapter VIII, 9083/15, 27 May 2015',

Data Protection Commission (Ireland), 'Guidance Note on Cookies and Other Tracking Technologies' <<https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf>> accessed 13 March 2024

— —, 'Data Protection Commission Announces Conclusion of Two Inquiries into Meta Ireland' (*Data Protection Commission*) <<https://www.dataprotection.ie/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland>> accessed 14 August 2024

— —, 'Guidance on the Use of Domestic CCTV.' (2021) <<https://www.dataprotection.ie/en/dpc-guidance/guidance-use-domestic-cctv>> accessed 13 March 2024

Bibliography

— —, 'The Data Protection Commission (DPC) Has Today Announced a Conclusion to a GDPR Investigation It Conducted into WhatsApp Ireland Ltd.' (*Data Protection Commission*, 2 September 2021)

— —, 'Annual Report 25 May - 31 December 2018'
<<https://www.dataprotection.ie/sites/default/files/uploads/2019-03/DPC%20Annual%20Report%2025%20May%20-%2031%20December%202018.pdf>>
accessed 7 September 2024

European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union", Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions'

— —, 'Data Act | Shaping Europe's Digital Future' <<https://digital-strategy.ec.europa.eu/en/policies/data-act>> accessed 28 November 2022

— —, 'Data Act: Measures for a Fair and Innovative Data Economy' (*European Commission - European Commission*)
<https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113> accessed 25 November 2022

— —, 'Press Release. Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses. European Commission.' (25 January 2012)
<https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46> accessed 7 March 2024

— —, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 Final, (Apr. 21, 2021)'

— —, 'Artificial Intelligence – Questions and Answers' (*European Commission - European Commission*, 12 December 2023)
<https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683> accessed 20 January 2024

— —, 'The Future of European Competitiveness. Part A | A Competitiveness Strategy for Europe'

— —, 'Commission Sends Preliminary Findings to Meta over Its "Pay or Consent" Model for Breach of the Digital Markets Act.' (*European Commission - European Commission*, 1 July 2024)
<https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582> accessed 14 August 2024

— —, 'Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by

the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce.'

— —, '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, 19.2.2020 COM (2020) 66' <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>> accessed 18 November 2022

— —, 'EU Digital Strategy' <<https://eufordigital.eu/discover-eu/eu-digital-strategy/>> accessed 7 March 2024

— —, 'European Data Governance Act | Shaping Europe's Digital Future' <<https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>> accessed 18 November 2022

— —, 'Press Release. Commission Opens Formal Proceedings against X under the DSA. 18 December 2023. Brussels' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709> accessed 26 January 2024

— —, 'Press Release. Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines. 25 April 2023, Brussels.' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413> accessed 26 January 2024

— —, 'Press Release. The Commission Sends Request for Information to X under DSA. 12 October 2023, Brussels.' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953> accessed 26 January 2024

— —, 'Recommendation of 29 July 1981 Relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [1981] OJ L246/31.'

— —, 'Stronger Enforcement of the GDPR in Cross-Border Cases' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3610> accessed 28 March 2024

— —, 'Supervision of the Designated Very Large Online Platforms and Search Engines under DSA' <<https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>> accessed 26 January 2024

— —, 'The Digital Services Act: Ensuring a Safe and Accountable Online Environment' (*European Commission - European Commission*) <<https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital->

services-act-ensuring-safe-and-accountable-online-environment_en> accessed 23 March 2024

European Data Protection Board (EDPB), 'Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)' (2018)

— —, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices Version 2.0 Adopted on 29 January 2020' (2020)

— —, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (2020)

— —, 'Guidelines 05/2020 on Consent under Regulation 2016/679 Version 1.0 Adopted on 4 May 2020' (2020)

— —, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0 Adopted on 07 July 2021' (2021)

— —, 'Guidelines 08/2020 on the Targeting of Social Media Users' (2021)

— —, 'Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data.' (2021)

— —, 'Facial Recognition: The French SA Imposes a Penalty Payment on CLEARVIEW AI | European Data Protection Board' (11 May 2023)
<https://edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en> accessed 4 February 2024

— —, 'Opinion 16/2021 on the Draft Decision of the Belgian Supervisory Authority Regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" Submitted by Scope Europe Adopted 19 May 2021'

— —, 'Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities'
<https://www.edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf>

— —, 'Report of the Work Undertaken by the Supervisory Authorities within the 101 Task Force. 28 March 2023' <https://www.edpb.europa.eu/system/files/2023-04/edpb_20230328_report_101task_force_en.pdf> accessed 7 September 2024

'First Report on the Implementation of the Data Protection Directive (95/46/EC)',
<<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=EN>> accessed 27 September 2021

European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the Potential of Cloud Computing in Europe"' <https://edps.europa.eu/sites/edp/files/publication/12-11-16_cloud_computing_en.pdf> accessed 19 July 2023

European Group on Tort Law, 'Principles of European Tort Law (PETL)' (2005)

Information Commissioner (Slovenia), 'Decision No. 0612-23/2019/19' <https://gdprhub.eu/images/8/89/IP_%28Slovenia%29_-_0612-23-2019-19.pdf> accessed 19 July 2023

Information Commissioner's Office (UK) 'Information Commissioner's Annual Report and Financial Statements 2021-22 July 2022 HC 392' <<https://ico.org.uk/media/about-the-ico/documents/4021039/ico-annual-report-2021-22.pdf>> accessed 28 September 2024

United States House of Representatives, 'The Computer and Invasion of Privacy: Hearings before a Subcommittee on Government Operations, House of Representatives, Eighty-Ninth Congress, First Session, July 2, 3, 4, 7, 23 and September 23. Part 1 and Part 2, 1965.' <<https://babel.hathitrust.org/cgi/pt?id=uc1.a0000162578&seq=5>> accessed 29 July 2023

United States Senate, 'Computer Privacy. Hearings, Ninetieth Congress, First Session, Pursuant to S. Res. 25. March 14 and 15, 1967.' <<https://babel.hathitrust.org/cgi/pt?id=osu.32437121556241&seq=7>> accessed 29 July 2023

— —, 'Federal Data Banks, Computers, and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-Second Congress, February 23-25, and March 2-15 and 17, 1971.' <<https://babel.hathitrust.org/cgi/pt?id=uc1.c051765460&seq=11>> accessed 29 July 2023

Newspapers, Magazines, and Blogs

Clearview AI, 'Clearview AI Product Overview' <<https://app.hubspot.com/documents/6595819/view/454213073?accessId=c85a92>> accessed 31 May 2023

'Clearview AI Data Use Deemed Illegal in Austria, However No Fine Issued' <<https://noyb.eu/en/clearview-ai-data-use-deemed-illegal-austria-however-no-fine-issued>> accessed 4 February 2024

'FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests' (*Federal Trade Commission*, 31 May 2023) <<https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>> accessed 5 July 2023

'FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras' (*Federal Trade Commission*, 31 May 2023) <<https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring>>

Bibliography

employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users>
accessed 5 July 2023

Gates B, 'Bill Gates: Trustworthy Computing' [2002] *Wired*
<<https://www.wired.com/2002/01/bill-gates-trustworthy-computing/>> accessed 7 July 2023

Gibbs S, 'Amazon Buys Video Doorbell Firm Ring for over \$1bn' *The Guardian* (28 February 2018) <<https://www.theguardian.com/technology/2018/feb/28/amazon-buys-video-doorbell-ring-smart-home-delivery>> accessed 5 July 2023

Godkin EL, 'Libel and Its Legal Remedy' [1880] *The Atlantic*
<<https://www.theatlantic.com/magazine/archive/1880/12/libel-and-its-legal-remedy/632214/>> accessed 8 July 2023

'Global Smart Home Market Research Report (2021 to 2026) - by Product, Technologies, Service, Deployment and Region - ResearchAndMarkets.Com' (7 December 2021)
<<https://www.businesswire.com/news/home/20211207005627/en/Global-Smart-Home-Market-Research-Report-2021-to-2026---by-Product-Technologies-Service-Deployment-and-Region---ResearchAndMarkets.com>> accessed 31 January 2022

Grand View Research, 'Artificial Intelligence as a Service: Market Research Report.'
<<https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-as-a-service-market-report.>>

Greenwald G, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily (The Guardian, 6 June 2013)' <<https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>> accessed 1 September 2024

Guariglia M, 'Amazon's Ring Is a Perfect Storm of Privacy Threats' (*Electronic Frontier Foundation*, 8 August 2019) <<https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats>> accessed 19 January 2022

Hill K, 'Clearview AI Successfully Appeals \$9 Million Fine in the U.K.' *The New York Times* (18 October 2023) <<https://www.nytimes.com/2023/10/18/technology/clearview-ai-privacy-fine-britain.html>> accessed 4 February 2024

iRobot, 'Amazon and iRobot Sign an Agreement for Amazon to Acquire iRobot' (*iRobot MediaKit*) <<https://media.irobot.com/2022-08-05-Amazon-and-iRobot-sign-an-agreement-for-Amazon-to-acquire-iRobot>> accessed 5 July 2023

Ivanišević B and Stojanovic M, 'Cloud Provider a Joint Controller? Slovenian Regulator Joins CNIL in Saying Yes' (*Lexology*, 15 August 2022)
<<https://www.lexology.com/library/detail.aspx?g=243478c5-13c2-435c-a1c3-cecc51d1204c>> accessed 13 March 2024

Lily Rothman, 'In Soviet Russia, the Oscars Host You' (*Time*, 23 February 2015)
<<https://time.com/3715747/bob-hope-russian-reversal/>> accessed 5 July 2023

Bibliography

Mehdi Y, 'Reinventing Search with a New AI-Powered Microsoft Bing and Edge, Your Copilot for the Web' (*The Official Microsoft Blog*, 7 February 2023) <<https://blogs.microsoft.com/blog/2023/02/07/reinventing-search-with-a-new-ai-powered-microsoft-bing-and-edge-your-copilot-for-the-web/>> accessed 31 May 2023

Microsoft,, 'Microsoft and OpenAI Extend Partnership' (*The Official Microsoft Blog*, 23 January 2023) <<https://blogs.microsoft.com/blog/2023/01/23/microsoftandopenaiextendpartnership/>> accessed 31 May 2023

Molla R, 'How Amazon's Ring Is Creating a Surveillance Network with Video Doorbells' (*Vox*, 5 September 2019) <<https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell-hacks>> accessed 10 March 2024

Neighbors EK Head of, 'Ring Announces New Neighbors App Features, Sunsets Request for Assistance Post' (*The Ring Blog*, 24 January 2024) <<https://blog.ring.com/about-ring/ring-announces-new-neighbors-app-features-sunsets-request-for-assistance-post/>> accessed 28 February 2024

NOYB, 'EU-US Transfers Complaint Overview' <<https://noyb.eu/en/eu-us-transfers-complaint-overview>> accessed 7 September 2024

'Noyb Files GDPR Complaint against Meta over "Pay or Okay"' <<https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay>> accessed 14 August 2024

Pohle J, 'Datenschutz und Technikgestaltung' <<https://edoc.hu-berlin.de/handle/18452/19886>> accessed 3 February 2024

'Ring Neighbors Is the Best and Worst Neighborhood Watch App' (*Wirecutter: Reviews for the Real World*, 3 June 2021) <<https://www.nytimes.com/wirecutter/blog/ring-neighbors-app-review/>> accessed 19 January 2022

'Six Months of Revelations on NSA' (*Washington Post*) <<http://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/>> accessed 15 February 2022

Southern MG, 'Google Updates Privacy Policy To Collect Public Data For AI Training' (*Search Engine Journal*, 3 July 2023) <<https://www.searchenginejournal.com/google-updates-privacy-policy-to-collect-public-data-for-ai-training/490715/>> accessed 5 February 2024

The Avalon Project, 'Blackstone's Commentaries on the Laws of England Book the Fourth - Chapter the Sixteenth : Of Offences Against the Habitations of Individuals' <https://avalon.law.yale.edu/18th_century/blackstone_bk4ch16.asp> accessed 13 March 2024

'The Privacy Threat From Always-On Microphones Like the Amazon Echo | ACLU' (*American Civil Liberties Union*, 12 January 2017) <<https://www.aclu.org/news/privacy->

technology/privacy-threat-always-microphones-amazon-echo> accessed 28 February 2024

Thompson N, 'Jack Dorsey on Twitter's Role in Free Speech and Filter Bubbles' *Wired* <<https://www.wired.com/story/jack-dorsey-twitters-role-free-speech-filter-bubbles/>> accessed 7 July 2023

Weatherbed J, 'Google Admits It's Training AI on Scraped Web Data' (*The Verge*, 5 July 2023) <<https://www.theverge.com/2023/7/5/23784257/google-ai-bard-privacy-policy-train-web-scraping>> accessed 5 February 2024

Website Products, Notices, Terms, and Reports

Amazon, 'Privacy New' (Ring) <<https://eu.ring.com/pages/privacy>> accessed 21 January 2024

AWS, 'Artificial Intelligence Services' (Amazon Web Services, Inc.) <<https://aws.amazon.com/machine-learning/ai-services/>> accessed 31 May 2023

'Cloud Data Processing Addendum' (Google Cloud) <<https://cloud.google.com/terms/data-processing-addendum>> accessed 15 June 2023

'GDPR - Amazon Web Services (AWS)' (Amazon Web Services, Inc.) <<https://aws.amazon.com/compliance/gdpr-center/>> accessed 29 March 2023

Google Cloud, 'AI & Machine Learning Products' (Google Cloud) <<https://cloud.google.com/products/ai>> accessed 31 May 2023

HireVue, 'HireVue Hiring Platform: Video Interviews, Assessment, Scheduling, AI, Chatbot | HireVue' (hirevue.com) <<https://www.hirevue.com/>> accessed 1 June 2023

'IAB Europe' (<https://iabeurope.eu/>) <<https://iabeurope.eu/>> accessed 8 March 2024

IBM, 'IBM Watson Products and Solutions' <<https://www.ibm.com/watson>> accessed 31 May 2023

Microsoft, 'Microsoft Products and Services Data Protection Addendum (DPA)' (2023) <<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>> accessed 15 June 2023

—, 'Azure AI Platform — Artificial Intelligence | Microsoft Azure' <<https://azure.microsoft.com/en-us/solutions/ai/>> accessed 31 May 2023

OpenAI, 'ChatGPT' <<https://openai.com/product/chatgpt>> accessed 31 May 2023

—, 'DALL·E 2' <<https://openai.com/product/dall-e-2>> accessed 31 May 2023

'Privacy Notice' (Ring) <<https://eu.ring.com/pages/privacy-notice>> accessed 10 September 2024

Bibliography

Pymetrics, 'Pymetrics' Gamified Skills Assessments Leverage Behavioral Science and AI Technology to Help Companies Build Diverse and Innovative Teams.'
<<https://www.pymetrics.ai/>> accessed 1 June 2023

X, Twitter International Unlimited Company (TIUC), 'DSA Transparency Report. X, Twitter International Unlimited Company (TIUC). 3 November 2023.'
<<https://transparency.twitter.com/dsa-transparency-report.html>> accessed 26 January 2024

Other

Mell P and Grance T, The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology (Computer Security Division Information Technology Laboratory National Institute of Standards and Technology 2011)

Nolan K, 'The Individual in EU Data Protection Law (PhD Thesis; LSE Law School)' (PhD Thesis, LSE Law School 2023) <<https://etheses.lse.ac.uk/4596/>>