

Durham E-Theses

Protecting Private Information Online in the Digital Era: Evaluating and Critiquing the Effectiveness of the UK GDPR Model with Comparative Reference to the Data Protection Position in China

Shuxin Zhang

How to cite:

Zhang, Shuxin (2026) Protecting Private Information Online in the Digital Era: Evaluating and Critiquing the Effectiveness of the UK GDPR Model with Comparative Reference to the Data Protection Position in China. Doctoral thesis, Durham University.

Use policy

The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a <https://etheses.durham.ac.uk/id/eprint/16613/> is made to the metadata record in Durham E-Theses
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Please consult the [full Durham E-Theses policy](#) for further details.

**PROTECTING PRIVATE INFORMATION ONLINE IN THE DIGITAL ERA:
EVALUATING AND CRITIQUING THE EFFECTIVENESS OF THE UK GDPR
MODEL WITH COMPARATIVE REFERENCE TO THE DATA PROTECTION
POSITION IN CHINA**

**A Thesis Submitted to Durham University for the Degree of Doctor of Philosophy in the
Durham Law School**

2025

Shuxin Zhang

Durham Law School

ABSTRACT

The thesis critically examines the United Kingdom General Data Protection Regulation (UK GDPR), assessing its strengths, limitations, and overall effectiveness in protecting personal data in a rapidly evolving digital landscape. The research is grounded in a legal and comparative methodology, offering a rigorous analysis of the UK GDPR both within its domestic context and through comparison with the data protection framework emerging in China. The central argument advanced is that while the GDPR provides a strong foundation for data protection, arguably one of the most advanced in the world in some respects, it is not without challenges. One of the key areas of focus is the effectiveness of the UK GDPR in practice. The study considers to what extent the legislation has achieved its stated objectives, including strengthening individuals' rights. The effectiveness is evaluated through multiple lenses: legislative clarity, judicial decisions, public interests.

A critical dimension of the thesis is the exploration of how personal data misuse is addressed through both statutory and judicial means. The analysis delves into landmark legal cases involving online privacy, shedding light on how courts have interpreted data protection rights and balanced them against competing interests such as freedom of expression and commercial means. This case-based approach provides an insight into how the judiciary has shaped the contours of data protection law and how this process has evolved with the introduction of the GDPR framework. By comparing outcomes and judicial reasoning in cases decided under older legislation with those interpreted under the UK GDPR, the thesis demonstrates both progress and ongoing inconsistencies in the legal protection of personal information online.

The research also brings into focus the broader legal infrastructure supporting data privacy in the UK, including the Data Protection Act 2018 and the tort of misuse of private information. These legal mechanisms interact with the UK GDPR in complex ways, at times reinforcing and at other times overlapping with or diverging from it. This pluralistic framework, comprising statutory provisions and the tort, creates both opportunities and challenges for individuals seeking redress for private data violations. The thesis examines whether this layered approach offers a comprehensive safety net or whether it leads to fragmentation and uncertainty for both litigants and courts.

An essential component of the study is its comparative perspective, particularly the analysis of data protection laws in China. The thesis explores China's recent efforts to regulate personal information through new legislative instruments such as in particular the Personal Information Protection Law (PIPL), which has drawn comparisons with the GDPR for its structure and stated objectives. However, significant differences exist in enforcement philosophy, regulatory culture, and underlying legal principles. This research provides an in-depth comparison between the UK GDPR and China's data protection approach, probing both structural and ideological divergences and considering possible greater alignment between the two; For instance, while the GDPR is rooted in liberal democratic values prioritising individual rights, China's model reflects more state-centric options, emphasising national security and governmental oversight.

TABLE OF CONTENTS

ABSTRACT	2
TABLE OF CONTENTS	4
LIST OF ABBREBIATIONS	8
TABLE OF LEGISLATION	9
TABLE OF CASES.....	12
STATEMENT OF COPYRIGHT	20
ACKNOWLEDGEMENT	21
CHAPTER 1 GENERAL INTRODUCTION AND OVERVIEW.....	22
1.1 INTRODUCTION	22
1.1.1 Threats to privacy online.....	22
1.1.2 The GDPR model	24
1.1.3 The relevant definitions/concepts regarding the research of this thesis	27
1.1.4 Conflicts with freedom of expression	28
1.2 OBJECTIVES OF THE RESEARCH	28
1.3 METHODOLOGY	29
1.3.1 Research design	29
1.3.2 Research data and collection process	30
1.3.3 Methodological issues	31
1.4 THE ROADMAP TO THE THESIS	32
CHAPTER 2 THE CONCEPT OF PRIVACY AND ITS SIGNIFICANCE IN RELATION TO PERSONAL INFORMATION.....	37
2.1 THE CONCEPTIONS OF PRIVACY: PHYSICAL AND INFORMATIONAL DIMENSIONS	40
2.2 PRIVACY AS THE RIGHT TO CONTROL PERSONAL INFORMATION.....	43
2.3 A CLOSER LOOK AT DIGITAL PRIVACY	49
2.4 A FURTHER ANALYSIS OF PRIVACY AND PERSONAL INFORMATION.....	56
2.5 CONCLUSION	59
CHAPTER 3 PUTTING THE GDPR INTO CONTEXT: EXAMINING THE EFFICACY OF THE PREVIOUS DATA PROTECTION REGIME.....	64
3.1 INTRODUCTION	64
3.2 PROCESSING PERSONAL DATA PRIOR TO THE GDPR	68
3.2.1 Analysis of the previous data protection regime in the UK, with the influence of ECHR	70
3.2.2 Impact of the previous data protection regime on individuals	83
3.2.3 Assessment of the strengths and weaknesses of the previous data protection framework.....	86
3.3 CONCLUSION	91
CHAPTER 4 KEY FEATURES OF THE CURRENT DATA PROTECTION MODEL IN THE UNITED KINGDOM.....	94
4.1 INTRODUCTION	94

4.2 THE CURRENT LEGAL PROTECTION OF THE UK, CONSIDERING THE BACKGROUND OF THE EU GDPR AND ITS NATURE	96
4.2.1 Identification of the key changes and improvements brought about by the current data protection model	97
4.2.2 The current data protection model in the UK.....	100
4.3 THE SCOPE OF THE UK GDPR	104
4.3.1 The meaning of personal data processing within GDPR	106
4.3.2 The extra-territorial scope of the UK GDPR.....	108
4.4 THE PRINCIPLES OF THE UK'S DOMESTIC PERSONAL DATA PROTECTION REGIME	114
4.4.1 The principles of the UK GDPR	114
4.4.2 The importance in practice of the principles in the UK GDPR.....	116
4.5 EXPLANATION OF THE GDPR IMPLEMENTATION IN THE UK	118
4.5.1 Remedies, liability and penalties.....	123
4.5.2 Lack of injunctive relief under the UK GDPR.....	130
4.6 CONCLUSION	135
 CHAPTER 5 AN ANALYSIS OF THE EFFECTIVENESS OF THE CURRENT PERSONAL DATA PROTECTION ENFORCEMENT IN THE UK.....	 136
5.1 INTRODUCTION	136
5.2 THE ROLE OF THE ICO, THE UK GDPR COMPARED WITH THAT OF THE TORT OF MISUSE OF PRIVATE INFORMATION (MPI).....	138
5.2.1 Informational security and consent under the UK GDPR/DPA	142
5.2.2 Reform of the UK GDPR under the Data Use (and Access) Act	146
5.3 THE ENFORCEMENT OF THE GDPR IN THE UK AND EU.....	154
5.3.1 Use of fines as an aspect of enforcement	154
5.3.2 Evaluation of the effectiveness of the current data protection model, centred on the impact of the GDPR.....	157
5.3.3 Examination of the challenges and loopholes in the implementation of the current personal data protection model.....	162
5.4 IMPACT OF THE GDPR ON PROTECTING PRIVATE INFORMATION IN THE CONTEXT OF THE CELEBRITY INDUSTRY AND THE PRIVACY OF 'ORDINARY' PEOPLE	164
5.4.1 Impact of the current personal data protection model on search engines, the media, including social media	165
5.4.2 The right to be forgotten and injunctions.....	174
5.4.3 The legal ramifications and ethical considerations surrounding the media exploitation of private information.....	181
5.5 CONCLUSION	191
 CHAPTER 6 THE CURRENT CHINESE LEGAL POSITION ON PERSONAL DATA PROTECTION	 194
6.1 INTRODUCTION	194
6.2 THE DEVELOPMENT OF THE PERSONAL DATA PROTECTION LEGAL FRAMEWORK IN CHINA	197
6.2.1 From the Brussels effect to the Beijing effect.....	199
6.2.2 The cultural approach to the development of Chinese data protection policy	203
6.2.3 The annotation method within legislative responses in China	206
6.2.4 Overview: understanding the Personal Information Protection Law and the Chinese data protection framework.....	209
6.3 DOCTRINAL DEBATES ON LEGAL CONCEPTS AND THE STATUS OF THE PERSONAL INFORMATION PROTECTION LAW	210
6.3.1 The fundamental legal position and protective functions of the PIPL	211

6.3.2 The rights to personal information in China.....	213
6.3.3 Lessons from the UK model: working on the Chinese data protection framework.....	217
6.4 THE RIGHT TO BE FORGOTTEN IN THE EU AND ITS CONTROVERSY IN ITS INTRODUCTION TO THE CHINESE LEGAL SYSTEM	219
6.4.1 Scholarly hypotheses on the right to be forgotten in China.....	220
6.4.2 The quasi-foundational regulations for the right to be forgotten.....	222
6.4.3 Case study (the first case): Ren Jiayu v Baidu	224
6.5 DYNAMIC BALANCE? CHINA'S APPROACHES TO BALANCING PROTECTION OF PERSONAL INFORMATION AND FREEDOM OF EXPRESSION	225
6.5.1 The legal approach to the balancing test.....	226
6.5.2 Creating a flexible balancing mechanism in China?	228
6.6 CONCLUSION	231
CHAPTER 7 CONCLUSIONS AS TO THE EFFICACY OF THE CHINESE PERSONAL DATA PROTECTION FRAMEWORK	234
7.1 INTRODUCTION	234
7.2 THE COMMODIFICATION OF PRIVACY: RETHINKING DATA PROTECTION IN THE CHINESE CONTEXT.....	239
7.2.1 The socio-historical concepts of privacy in China	239
7.2.2 The evolution of data protection in China: Statutory developments and practical challenges	242
7.3 CHINA'S EVOLUTION TOWARD DATA PROTECTION LAW: A COMPARATIVE ANALYSIS OF REGULATORY AND REMEDIAL SCHEMES	245
7.3.1 Disclosing/facilitating online actors; threats to private information and its remedies	245
7.3.2 Contrasts between remedial relief and regulatory aspects of the two schemes: influence on design	260
7.3.3 Enforcement in China, comparing it with the GDPR.....	268
7.3.4 'Personal data' under the GDPR/DPA and the PIPL.....	271
7.4 THE SPEECH/PRIVACY BALANCING ACT: A COMPARISON BETWEEN THE GDPR/DPA FRAMEWORK AND THE CHINESE MODEL	274
7.4.1 The protective framework for freedom of expression and information.....	274
7.4.2 The legislative approach: the 'Rule by Law' system for data protection in China.....	276
7.4.3 A closer focus on free speech and information values.....	278
7.5 CONCLUSION	287
CHAPTER 8 CONCLUSIONS AND POTENTIAL REFORMS.....	289
8.1 REVISITING THE UK FRAMEWORK: FURTHER EVALUATING THE EFFECTIVENESS OF THE TORT AND GDPR/DPA REMEDIES	290
8.1.1 The declining impact of traditional injunctions.....	290
8.1.2 Comparative analysis: injunctions and the right to be forgotten.....	303
8.1.3 Dealing with anonymous or hard-to-locate publishers	309
8.1.4 Are injunctions and erasure rights constrained by speech-friendly standards in courts?	314
8.2 REFORMING CHINA'S DATA PROTECTION FRAMEWORK	320
8.2.1 Is a specific Data Protection Act necessary?.....	321
8.2.2 Toward legal harmonisation: unifying fragmented personal data regulations in China	326
8.2.3 Embracing a GDPR-style, rights-based approach for China	331
8.3 CONCLUSIONS AS TO THE RESEARCH QUESTIONS OF THE THESIS.....	332
8.3.1 The United Kingdom	333
8.3.2 China.....	339
8.3.3 Conclusions.....	341
BIBLIOGRAPHY	345

BOOKS	345
JOURNAL ARTICLES	346
WEBSITES AND BLOGS	359
ONLINE REPORTS AND OFFICIAL PUBLICATIONS	364
CHINESE LANGUAGE SOURCES.....	365

LIST OF ABBREBIATIONS

Artificial Intelligence	AI
Court of Justice of the European Union	CJEU
Data (Use and Access) Act 2025	DUAA
Data Protection Act	DPA
European Convention on Human Rights	ECHR
European Court of Human Rights	ECtHR
European Economic Area	EEA
Federal Trade Commission	FTC
General Data Protection Regulation	GDPR
Human Rights Act 1998	HRA 1998
Information and Communication Technologies	ICTs
Information Commissioner's Office	ICO
Independent Press Standards Organisation	IPSO
Internet of Things	IoT
Online Safety Act	OSA
Personal Information Protection Law	PIPL
Standard Contract Clauses	SCCs
Strategic Communication Laboratories	SCL
The Right to be Forgotten	RTBF
Universal Declaration of Human Rights	UDHR

TABLE OF LEGISLATION

UK LEGISLATION

- *Data (Use and Access) Act 2025*
- *Data Protection Act 1984*
- *Data Protection Act 1998*
- *Data Protection Act 2018*
- *Defamation Act 2013*
- *Human Rights Act 1998*
- *Investigatory Powers Act 2016*
- *Online Safety Act 2023*
- *The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, SI 2019/419*
- *The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020, SI 2020/1586*

EU LEGISLATION AND DIRECTIVES

- *Charter of Fundamental Rights of the European Union* [2000] OJ C364/01 and [2010] OJ C83/389
- *Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended)* (ECHR)
- *Council of Europe Convention No. 108 on data protection Convention for the protection of individuals with regard to automatic processing of personal data* (ETS No. 108, 28.01.1981)
- *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016*
- *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 L281/23
- *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 (United Kingdom General Data Protection Regulation)*

CHINESE LEGISLATION

- *Civil Code of the People's Republic of China* [2020]
- *Criminal Law of the People's Republic of China* (2021 Edition)
- *Cybersecurity Law of the People's Republic of China* [2016]

- *Data Security Law of the People's Republic of China* [2021]
- *General Provisions of the Civil Law* [2017]
- *Personal Information Protection Law* [2021]
- *Provisions of the Supreme People's Court on Certain Issues Concerning the Application of Law in the Hearing of Cases of Civil Disputes over the Use of Information Networks to Infringe upon Personal Rights and Interests* 2014 (SPC Interpretation 11/2014) (Revised)
- *Tort Liability Law* [2009]

INTERNATIONAL INSTRUMENTS

- *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, The Organisation for Economic Co-Operation and Development (1980)
- *United Nations, 'Universal Declaration of Human Rights'* (1948)

TABLE OF CASES

UNITED KINGDOM

- *AAA v Associated Newspapers* [2013] EWCA Civ 554
- *ABC v Telegraph Media Group Ltd* [2018] EWCA Civ 2329
- *A v B plc (Flitcroft v MGN Ltd)* [2002] EWCA Civ 337; [2003] QB 195
- *Ali v Chief Constable of Bedfordshire* [2023] EWHC 938 (KB)
- *AMP v Persons Unknown* [2011] EWHC 3454 (TCC)
- *Bekoe v Islington LBC* [2023] EWHC 1668 (KB)
- *Bloomsbury Publishing Group plc v News Group Newspapers Ltd* [2003] EWHC 1205 (Ch)
- *Campbell v MGN Ltd* [2002] EWCA Civ 1373
- *Campbell v MGN Ltd* [2004] UKHL 22
- *CG v Facebook Ireland Ltd and McCloskey* [2015] NIQB 11
- *Clearview AI Inc v The Information Commissioner* [2023] UKFTT 00819 (GRC)
- *CTB v News Group Newspapers Ltd* [2011] EWHC 1326
- *Doorstep Dispensaree Ltd v the Information Commissioner* [2023] UKUT 132 (AAC)
- *Douglas v Hello! Ltd (No.2)* [2003] EWCA Civ 139
- *Driver v Crown Prosecution Service* [2022] EWHC 2500 (KB)

- *Duke of Sussex and others v MGN Limited, The* [2023] EWHC 3217 (Ch)
- *Durant v Financial Services Authority* [2003] EWCA Civ 1746
- *Farley v Paymaster* [2024] EWCA Civ 781
- *Ferdinand v MGN Ltd* [2011] EWHC 2454 (QB)
- *FGX v Gaunt* [2023] EWHC 419 (KB)
- *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311
- *Gulati v MGN* [2015] EWHC 1482 (CH)
- *Gulati v MGN* [2017] Q.B 149
- *GYH v Persons Unknown* [2017] EWHC 3360 (QB)
- *HH Prince Moulay Hicham Ben Abdallah Al Alaoui of Morocco v Elaph Publishing Ltd*
[2017] EWCA Civ 29
- *Hutcheson v News Group Newspapers Ltd* [2011] EWCA Civ 808
- *J20 v Facebook Ireland Ltd* [2016] NIQB 98
- *JIH v News Group Newspapers Ltd* [2011] 1 WLR 1645
- *JQL v NTP* [2020] EWHC 1349 (QB)
- *JRV & Anor v BRG (Re Injunction)* [2023] EWHC 2238 (KB)
- *Kaye v Robertson* [1991] FSR 62
- *Lachaux v Independent Print Ltd and Evening Standard Ltd* [2019] UKSC 27
- *Lachaux v Independent Print Ltd and another* [2021] EWHC 1797 (QB)
- *Law Society v Kordowski* [2011] EWHC 3185 (QB)

- *LJY v Persons Unknown* [2017] EWHC 3230 (QB)
- *Lloyd v Google LLC* [2020] Q.B. 747
- *Lloyd v Google LLC* [2021] UKSC 50
- *McKennitt v Ash* [2006] E.M.L.R 10
- *MLA v OPO & Anor* [2014] EWCA Civ 1277
- *Mosley v News Group Newspapers Ltd* [2008] E.M.L.R 20
- *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446
- *Murray v Ministry of Defence* [1988] 1 W.L.R. 692
- *NT1 & NT2 v Google* [2018] EWHC 799 (QB)
- *Pacini & Anor v Dow Jones & Company Inc.* [2024] EWHC 2714 (KB)
- *PJS v News Group Newspapers Ltd* [2016] A.C. 1081
- *Prince Albert v Strange* [1849] 47 ER 1302
- *Prismall v Google UK Ltd and DeepMind Technologies Ltd* [2024] EWCA Civ 15
- *R (on the application of AB) v Secretary of State for the Home Department* [2013] EWHC 3453
- *Richard v The British Broadcasting Corporation (BBC) & Anor* [2018] EWHC 1837 (Ch)
- *Sicri v Associated Newspapers Ltd* [2020] EWHC 3541 (QB)
- *Sir Cliff Richard v The BBC & The Chief Constable of South Yorkshire Police* [2018] EWHC 1837

- *Smith v TalkTalk Telecom Group Plc* [2022] EWHC 1311
- *Soriano v Forensic News LLC* [2021] EWHC 56 (QB)
- *Spelman v Express Newspapers* [2012] EWHC 355 (QB)
- *Stunt v Associated Newspapers Ltd* [2017] EWHC 695 (QB)
- *Terry (previously referred to as 'LNS') v Persons Unknown* [2010] EWHC 119 (QB)
- *Vidal-Hall v Google Inc (CA)* [2015] EWCA Civ 311
- *Wainwright v Home Office* [2003] UKHL 53
- *Weller v Associated Newspapers Limited* [2014] EWHC 1163 (QB)
- *WFZ v BBC* [2023] EWHC 1618 (KB)
- *Wikimedia Foundation and Another v Secretary of State for Science, Innovation and Technology* [2025] EWHC 2086 (Admin)
- *ZAM v CFW* [2011] EWHC 476 (QB)
- *ZXC v Bloomberg LP* [2021] Q.B. 28
- *ZXC v Bloomberg LP* [2022] UKSC 5

EUROPE

- *A.P., Garçon et Nicot v France* [2017] App. No(s) 79885/12, 52471/13, 52596/13
- *Axel Springer AG v Germany* [2012] App. No. 39954/08
- *Biancardi v Italy* [2021] App. No. 77419/16

- *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] C-101/01, 1 CMLR 20
- *Copland v The United Kingdom* [2007] App. No. 62617/00
- *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] C-311/18
- *Dimitrov-Kazakov v Bulgaria* [2011] App. No. 11379/03
- *Drelon v France* [2022] ECHR 278
- *Dudgeon v The United Kingdom* [1981] App. No. 7525/76
- *Egeland and Hanseid v Norway* [2009] App. No. 34438/04
- *Fuchsmann v Germany* [2017] App. No. 71233/13
- *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* [2019] C-136/17
- *Google Inc v CNIL* [2019] C-507/17
- *Google Spain SL v Agencia Española de protección de Datos (AEPD)* [2014] Q.B. 1022
- *Handyside v The United Kingdom* [1976] App. No. 5493/72
- *Herbecq and the Association 'Ligue des droits de l'homme' v Belgium* [1998] App. No(s). 32200/96 and 32201/96
- *Hurbain v Belgium* [2023] GC App. No. 57292/16
- *Kruslin v France* [1990] App. No. 11801/85
- *Leander v Sweden* [1987] App. No. 9248/81
- *Lithuaniaia, OT v Vyriausioji tarnybinės etikos komisija* [2022] C-184/20

- *Malone v The United Kingdom* [1984] App. No. 8691/79
- *M.L. and W.W. v Germany* [2018] App. No(s). 60798/10 and 65599/10, ECLI: CE: ECHR:2018:0628JUD006079810
- *Mosley v The United Kingdom* [2011] 53 E.H.R.R. 30
- *Peck v The United Kingdom* [2003] EHRR 287 App. No. 00044647/98
- *Radu v Moldova* [2014] App. No. 50073/07
- *Ragnhildur Guðmundsdóttir v The State of Iceland* [2003] No. 151/2003
- *Rechnungshof v Österreichischer Rundfunk* [2003] C-465/00, C138-/01, and C-139/01, ECLI:EU:C:2003:294
- *S. and Marper v The United Kingdom* [2008] GC, App. No(s). 30562/04, 30566/04
- *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] 64 EHRR 8
- *Sunday Times v The United Kingdom* [1979] App. No. 6538/74 EHRR 245
- *Taylor-Sabori v The United Kingdom* [2002] App. No. 47114/99
- *TU and RE v Google LLC* [2022] C-460/20, ECLI:EU:C:2022:962
- *Von Hannover v Germany* [2005] 7 WLUK 866
- *Von Hannover (No 2)* [2012] 55 E.H.R.R. 15
- *Węgrzynowski and Smolczewski v Poland* [2013] App. No. 33846/07
- *Weltimmo sro v Nemzeti Adatvédelmi és Információs Zrt* [2015] C-230/14 EU:C: 2015:639

CHINA

- *Gao v Ju* (2014) Beijing No. 3 Intermediate People's Court, Sanzhong Minzhong No. 04060
- *Gui & Zhang v Xu* (2015) Jiangning District People's Court of Nanjing, Jiangning Shaominchu No. 7
- *Guo, Lu and Others* (2020) *Personal Information Infringement Case*, Gan 0123 Xing Chu 53
- *Jiang v Binzhou Magic Pharmacy Co., Ltd.* (2022) Lu 1602 Minchu No. 976
- *Lin Nianping v Sichuan Airlines Co., Ltd.* (2015) Cheng Minzhong No. 1634
- *Lin Shengbin v Liu Xinda* (2024) Beijing No. 4 Intermediate People's Court, Jing 04 Minzhong No. 328
- *Ma Chunyan v China Southern Airlines Co., Ltd.* (2016) Su 01 Min Zhong 3947
- *Pang v Beijing Qunar Information Technology Co., Ltd. et al.* (2017) Jing 01 Min Zhong No. 509
- *Qi v Beijing [Unnamed] Network Company and Yao* [2024] Beijing Internet Court CLI.CR.501993222
- *Qin Moule and Others* (2021) *Personal Information Infringement Case*, Jing 0105 Xing Chu 2759
- *Ren Jiayu v Baidu* (2015) Beijing Haidian District People's Court, Hai Min Chu Zi No 17417

- *Wang Fei v Zhang Leyi, Daqi.com and Tianya.cn* (2009) Beijing Chaoyang District Court, No. 10930
- *Xie v Ye* (2019) *General Personality Rights Dispute*, Zhe 0192 Min Chu 624
- *Xu Linlin v Bank of China Liaoning Branch* (2023) Liao 03 Min Zhong No.1358
- *Yang Lijuan v Southern Weekly* (2008) Guangdong Guangzhou Intermediary People's Court, Civil Second Instance, No. 3871
- *Yang v Lin* [2024] Beijing Internet Court CLI.C.555521261
- *Ye v Shi et al.* (2014) Chaoyang District People's Court of Beijing, Chaominchu No. 00008
- *Yuhang District People's Procuratorate v R video platform* (2020) Civil Mediation Statement of the Hangzhou Internet Court, Zhe 0192 Minchu No. 10993
- *Zhao Junyan v China Southern Airlines Co., Ltd.* (2017) Yue 71 Min Zhong 11
- *Zhu Ye v Baidu Company* (2014) Ning Min Zhong Zi No 5028
- *Zhu Ye v Beijing Baidu Wangxun Technology Co., Ltd* (2013) Gu Min Xia Chu Zi No 2

UNITED STATES

- *Jane Doe (D.L.) v M. Jackson*, 2022-20061/Court:113

STATEMENT OF COPYRIGHT

The copyright of this thesis rests with the author. No quotation from it should be published without the author's prior written consent and information derived from it should be acknowledged.

ACKNOWLEDGEMENT

To my dear parents, Tianshui Zhang and Xiaomei Lin. I love you both.

To my wonderful supervisor, Professor Helen Fenwick. You are the best.

CHAPTER 1 GENERAL INTRODUCTION AND OVERVIEW

1.1 Introduction

1.1.1 Threats to privacy online

Privacy is a growing concern in homes, businesses and governments around the world. In recent years, as many aspects of life have moved from offline to online, everyone from civilians to officials has learned in particular about the ‘cookies’ left by digital activities. Companies have long used this data to promote and improve advertising and news. Lawmakers have long intervened in the privacy issues arising because of the risks of privacy-invasion created by data collection and the risk that personal data about all Internet users could be compromised in privacy terms in a range of ways, including via collection. This thesis partly focuses on the General Data Protection Regulation (GDPR)¹ as a globally respected model, in terms of creating protection for private information online. An example as to the need for such protection can be given.

In March 2018, the largest data abuse incident in the history of Facebook, a well-known American social networking site, was revealed. The incident stems from allegations that two of its affiliated companies, Strategic Communication Laboratories (SCL)² and Cambridge Analytica, misused personal data and used data analysis in political campaigns.³ The nature of

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) (Text with EEA relevance).

² See details: Peter Grant, ‘Strategic Communication Laboratories and the Mysterious Origins of Cambridge Analytica’ (Medium 12 September 2023) <https://medium.com/@petergrant_14485/strategic-communication-laboratories-and-the-mysterious-origins-of-cambridge-analytica-b9eff53fe71d>.

³ See Greg Rafferty, *Forecasting Time Series Data with Facebook Prophet* (Packt Publishing - eBooks Account, 2021); with a relevant article of Frederik Schade, ‘Dark Sides of Data Transparency: Organized Immaturity after GDPR?’ [2023] *Business Ethics Quarterly* 1, p 2, available at: <https://doi.org/10.1017/beq.2022.30>.

the event is no longer limited to a purely technological event but evolved into a major political issue.

Facebook does not, however, consider this to be a case of data abuse, but simply a breach of contract by a third-party company that did not follow data protocols.⁴ But the real impact of the incident is that the personal data of 87 million Facebook users may have been misused. The Federal Trade Commission (FTC)⁵ has begun an investigation into the matter, and Facebook could in theory face a \$2 trillion fine if it is found to have violated the 2011 settlement order, which requires Facebook to take several steps to make sure it meets its previous promises in the future, including providing consumers with clear notice and obtaining consumers' consent before their information is shared beyond the privacy settings they have established.⁶ The exposure of this incident is expected to arouse respect for citizens' privacy and legal awareness of personal information protection. A range of other examples are given below of misuse of personal data online.

While more and more people are willing to post their personal daily life and even to operate social accounts to attract/acquire public interest (especially celebrities) on social platforms like Instagram or Facebook, they also risk unwanted dissemination of their private information. At times without cautious consideration, they post the pictures or videos on their personal online accounts but actually do not intend to share material publicly. It is a positive phenomenon that individuals tend to set their social accounts as private, which means leaving relevant account

⁴ See Jim Isaak and Mina J Hanna, 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection' (2018) 51 Computer 56 <<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8436400>>; CBI registers FIR against Cambridge Analytica, Global Science Research heads for 2018 Facebook data leak. 2021, Bar & Bench.

⁵ Federal Trade Commission, 'Federal Trade Commission' (Federal Trade Commission2024) <<https://www.ftc.gov/>>.

⁶ See Aleksandr, 'GDPR in the USA: GDPR Compliance in US: GDPR and Pii' (*Cookiebot*) July 7, 2020, <<https://www.cookiebot.com/en/gdpr-usa/>> accessed March 26, 2023.

contents available to some social circles that they are willing to share information with.

1.1.2 The GDPR model

There have been numerous studies to investigate how to protect personal information in the digital world and to evaluate the effectiveness of the UK GDPR under the domestic and transnational context. In the articles of Judith Townend, she evaluated and critically assessed the protection for personal information by exploring the ‘Right to be Forgotten’ (RTBF) (Art.17 of the GDPR) in practice from the UK perspective which is rooted in a social-legal understanding of data protection.⁷

Under the background of constant intrusion of private information personal information should be protected under Article 8 European Convention on Human Rights (ECHR)⁸ via the Human Rights Act 1998 (HRA 1998),⁹ the UK GDPR and Data Protection Act 2018 (DPA 2018).¹⁰ Data privacy has become a serious issue with the emergence of various online social platforms. As Helen Fenwick and Fiona Brimblecombe indicate in their paper, a key intention underlying GDPR is to rein in the power to invade online data privacy by private companies.¹¹

⁷ See Judith Townend, ‘Data Protection and the ‘Right to Be Forgotten’ in Practice: A UK Perspective’ (2017) 45 International Journal of Legal Information 28, p 31.

⁸ European Convention for the Protection of Human Rights and Fundamental Freedoms, Sept. 3, 1953, ETS 5, 213 UNTS 221.

⁹ Human Rights Act 1998 (Legislation.gov.uk1998) <<https://www.legislation.gov.uk/ukpga/1998/42/contents>>.

¹⁰ Data Protection Act 2018 (Legislation.gov.uk2018) <<https://www.legislation.gov.uk/ukpga/2018/12/contents>>.

¹¹ See Fiona Brimblecombe and Helen Fenwick, ‘Protecting Private Information in the Digital Era: Making the Most Effective Use of the Availability of the Actions under the GDPR/DPA and the Tort of Misuse of Private Information’ (2022) 73 Northern Ireland Legal Quarterly 26, p 30.

Tech companies who became the intermediaries¹² and traditional media bodies were impacted by such regulation as well under data protection. Traditional tort claims for misuse of private information can be brought alongside data protection ones. Fenwick and Brimblecombe also propose that in relation to disclosures of private information online, an increasing court-based reliance on both causes of actions (tort and data protection) is arising; they foreshadow the nature of the jurisprudence that is beginning to arise, arguing that it is likely to provide privacy claimants with an enhanced ability to rely on both areas against online intermediaries.¹³ Prior research suggests that there are barriers to data free flow between countries; the forms of that are different data protection policies/regulations and the economic burdens like tariffs on businesses.¹⁴ Therefore, under current legal policies and regulations protecting personal information, individuals also have been inevitably influenced by the effects of those barriers.

Although there remains most of the EU data protection framework in the UK GDPR, its application becomes more complicated when the previous EU cases need to be invoked.¹⁵ The ICO cited the CJEU case from *Lithuaniaia, OT v Vyriausioji tarnybinės etikos komisija*¹⁶ when considering the issue of deducing special categories of personal data. Regarding this case, the ICO had pointed out, this judgment made a confirmation that a high level of protection exists which the GDPR gives to the special categories of data subject.¹⁷ The ICO has sought to cite

¹² Department for Science, Innovation & Technology, 'Data Intermediaries' (GOV.UK 17 March 2025), section B <<https://www.gov.uk/government/calls-for-evidence/data-intermediaries/data-intermediaries>> accessed 13 April 2025; *Data intermediary is used as a general term to describe a range of models of governance, organisation, and structure. They are entities that facilitate data sharing or access between those who wish to make their own data available (or those legally permitted to exercise the rights for this data, e.g. those appointed under a Lasting Power of Attorney) and those who are seeking to find and use data they do not have.*

¹³ See Fiona Brimblecombe and Helen Fenwick (note 11) p 30.

¹⁴ See Francesca Mazzi and others, 'The UK GDPR Reform: Missing Data Privacy, Regulatory Probity, and Harm Prevention' [2021] SSRN Electronic Journal, chapter 2.1.

¹⁵ See David Erdos, 'Assessing UK Data Protection Reform in Transnational Context: What New Direction?' [2021] University of Cambridge Faculty of Law Research Paper No. 28/2021, section one, para 2.

¹⁶ *Lithuaniaia, OT v Vyriausioji tarnybinės etikos komisija* C-184/20, 1 August 2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62020CJ0184&from=EN>.

¹⁷ *Ibid*, pp 118-127.

it, even though it is not bound to follow new CJEU precedent after Brexit.

Some critics have raised concerns about the new reforms under the GDPR. For example, the UK Government's Department for Digital, Culture, Media and Sport¹⁸ published *Data: A New Direction*¹⁹ which forwarded proposals for the purpose of reform of the UK data protection framework.²⁰ It has been argued that it would undermine three main pillars of the data protection legislation with regard to *data privacy*, *regulatory probity* and *harm prevention*.²¹ Francesca Mazzi etc., in their research, argued that data privacy could be compromised, insofar as data subjects' rights would be negatively impacted by various suggested reforms if implemented.²² They indicated that the reform of GDPR could potentially threaten the level of protection that is enjoyed by data subjects in the UK.²³ With the analysis of that reform, they argued that the reform tends to focus on economic growth and innovation more than on public interests and civilians' privacy.

In order to evaluate the effectiveness of the remedies for individuals, it is unavoidable that the 'right to be forgotten' be mentioned in this legal context, as discussed below in Chapter 4. The explanation in Chapter 5²⁴ of the application of the 'right to be forgotten' in practice evaluates its application in the complicated digital world.

¹⁸ Department for Digital, Culture, Media & Sport, 'Department for Digital, Culture, Media & Sport' (GOV.UK18 May 2019) <<https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport>>.

¹⁹ Department for Digital, Culture, Media and Sport, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document_Accessible_.pdf; Information Commissioner's Office, Response to DCMS consultation '*Data: a new direction*' (6 October 2021), <https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response20211006.pdf>.

²⁰ See David Erdos (note 15) para 2.

²¹ See Francesca Mazzi and others, 'The UK GDPR Reform: Missing Data Privacy, Regulatory Probity, and Harm Prevention' [2021] SSRN Electronic Journal, chapter 1, p 3.

²² Ibid, section 2.2, p 10.

²³ Ibid, chapter 1, p 4.

²⁴ *infra* section 5.4.2.

1.1.3 The relevant definitions/concepts regarding the research of this thesis

Privacy: A human need, *'the right to be let alone, or to control how your personal information is used.'*²⁵

*Personal Data:*²⁶ *'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.'*

Personal Information: The 'personal information' and the 'personal data' are not explicitly distinguished under the GDPR, with the regulation primarily using the term 'personal data.' The EU GDPR also does not explicitly differentiate between the concepts of personal data, and personal information.

This thesis limits the definitions of three terms to the online space, leading to the following hierarchy: private information could be considered a subset of personal information, meaning that its scope online is narrower than that of personal information. Although not strictly distinguished, personal data generally needs to be stored in virtual databases, making its scope slightly smaller than that of personal information, which can be published and disseminated on

²⁵ Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

²⁶ Art 4 of 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance)' (*Legislation.gov.uk*2016) <<https://www.legislation.gov.uk/eur/2016/679/article/4>>.

various online social platforms.

1.1.4 Conflicts with freedom of expression

There exists constantly legal argument in relation to litigation concerning conflicts between free expression and privacy, as explored at a number of points in this thesis. Freedom of speech is clearly necessary for individual autonomy and self-government, but it has to give way to other interests, in certain circumstances, such as to protect private information, if the interest in privacy can be found to be more pressing.

But in contrast with such reining in of the tech companies in terms of protecting private information online, freedom of expression also needs to be clarified and protected. David Erdos suggested that the UK-EU legal data protection framework can be viewed as an ecosystem of privacy and freedom of expression.²⁷ Scholars have argued that the conflicts between personal information and freedom of expression become the highlights in evaluating the effectiveness of the legal framework and specific judicial decisions regarding the legal regime of the UK.²⁸

1.2 Objectives of the Research

This thesis seeks to evaluate and critique the effectiveness of current legal protection of private information online in the UK, taking account of both data protection and the tort of misuse of private information, influenced by Article 8 ECHR. In so doing it will compare the protections

²⁷ See David Erdos (note 15) section one, p 5.

²⁸ See Eliza Bechtold, 'Regulating Online Harms: An Examination of Recent Developments in the UK and the US through a Free Speech Lens' (2024) 16 Journal of Media Law 1, pp 361, 374, 388; Communications and Digital Committee, Free for all? freedom of expression in the Digital age (2021) the Authority of the House of Lords, 1st Report of Session 2021–22, p 3, Available at: <https://committees.parliament.uk/publications/6878/documents/72529/default/>.

available for private information online in Europe and recommend reforms, in order to consider effective models for the legal protection of personal information online. It will also take account of the positions in China in order to place these research questions in a wider context. The legal framework in China still needs reform so as to provide better safeguarding procedures to seek to avoid the misuse of personal information online. Therefore, research regarding protecting personal information online in China will be referred to in this thesis in Chapters 6 and 7. Then it will come to conclusions as to whether the GDPR appears to have the capacity to prevent the Cambridge Analytica type of situation, and in general whether and how far the GDPR provides an effective model that other states, possibly including China, could emulate. It will also consider whether there is any realistic prospect of China adopting an instrument on the GDPR/DPA model.

This thesis therefore addresses the key questions: 1) how far is the GDPR effective in regulating the misusing of personal information online? It asks how far it can provide for effective *ex ante* action to shield data subjects from privacy invasion online? 2) Through a comparative analysis of the UK experience, this study seeks to examine whether China can feasibly consolidate its fragmented data regulatory framework and assesses the necessity of enacting a dedicated and unified Data Protection Act to supplement and enhance the existing legal system, possibly relying on aspects of the GDPR as a model.

1.3 Methodology

1.3.1 Research design

This thesis selects the UK and China as two representative examples to compare personal data

protection under a common law system with that under a civil law system. The purpose of this comparison is to assess the contemporary global consensus on privacy violations, or, more precisely, to examine how two fundamentally different governments, shaped by distinct traditions and historical-cultural influences, are addressing the challenge of online personal data protection in the era of emerging digital technologies. Moreover, by analysing the UK's more established data protection framework, this study seeks to explore potential pathways for enhancing China's personal information protection in the modern digital landscape.

Aiming to understand the legal protection of personal information in the EU and the UK, this study principally employs a library-based research methodology, with a particular emphasis on the analysis of decided cases. Through a comparative examination of legal systems in the UK, this research seeks to delineate the scope and effectiveness of current data protection measures. For comparative purposes, the study also investigates the Chinese legal framework of personal data protection, with the objective of identifying disparities and potential areas for reform within personal data protection system in China.

1.3.2 Research data and collection process

This research employs a law-in-context methodology and case study analysis to evaluate data protection frameworks, with the primary objective of assessing and critiquing the effectiveness of the UK GDPR and the application of tort law in the UK through an examination of decided cases. However, the UK data protection regime is not a settled or coherent system, but one in a pronounced state of flux. Since Brexit, the UK has retained the GDPR in domesticated form through the DPA 2018 and the UK GDPR, yet the government's genuine commitment to this

framework remains deeply ambiguous.²⁹ Legislative initiatives such as the Data (Use and Access) Act 2025 (DUAA)³⁰ signal a deliberate regulatory divergence from EU standards,³¹ raising serious questions about whether the UK government substantively endorses the values and obligations underpinning the GDPR regime, or whether it merely tolerates it as a transitional instrument of adequacy politics, preserving data flows with the EU while quietly dismantling the architecture that makes those flows legitimate. This ideological ambivalence is not a peripheral concern; it directly conditions the effectiveness of the protections this thesis seeks to evaluate.

Accordingly, this research does not treat the UK GDPR as a stable regulatory baseline, but interrogates it as a contested and potentially unstable framework, one whose future trajectory is as legally significant as its present application. The implications of this instability for both statutory data protection and tort-based remedies will be examined in detail in Chapters 5 and 8. Additionally, the study considers the level of protection for personal data online in other relevant jurisdictions, with a particular focus on China. For the purposes of this thesis, three types of data have been collected: legislation, codes of practice, case-law that have established judicial precedents. The foundational data for this research is derived from the specific articles of the GDPR, which serve as the benchmark for analysis and comparison.

1.3.3 Methodological issues

The primary consideration in conducting a comparative analysis between different legal systems is how to ensure the trustworthiness and reliability of personal data. As data protection

²⁹ See Lords Hansard, 'House of Lords - Hansard - UK Parliament' Vol. 854

No. 288 (Parliament.uk2026), pp 1005-1007, <<https://hansard.parliament.uk/lords/2026-03-19>>.

³⁰ 'Data (Use and Access) Act 2025' (Legislation.gov.uk2025) <<https://www.legislation.gov.uk/ukpga/2025/18>>.

³¹ Ibid.

laws and policies vary across jurisdictions, examining how different legal frameworks operate in practice can provide valuable insights into their effectiveness and implementation.

A comparative approach involves analysing legal data protection policies and regulations in various countries while systematically collecting and examining case precedents related to digital privacy. By gathering relevant judicial decisions and statistical data from online legal databases, it could identify patterns in how courts interpret and enforce data protection laws.

Through such comparisons, it becomes possible to assess how different legal systems balance competing interests, such as individual privacy, public interest, and press freedom, within their respective regulatory environments. Examining decided cases allows for a deeper understanding of how rights of data subjects, such as the right to be forgotten, are applied in real-world contexts. Furthermore, comparative legal research can reveal divergences in judicial review, the role of regulatory authorities, and the extent to which data protection frameworks are shaped by cultural, political, and economic factors. By identifying judicial practices and potential weaknesses in different systems, this analysis can contribute to refining data protection regulations and enhancing their practical enforcement across jurisdictions.

1.4 The Roadmap to the Thesis

This thesis will evaluate and critique the UK GDPR and will argue that it currently provides a model which in certain respects could provide more effective data protection than was achieved under the previous regime.

Chapter 2 establishes the foundation for a detailed examination of the evolving concept of

privacy, and the strategies individuals employ to navigate the increasing complexity of exercising control over both their physical and digital lives. It concludes by underscoring the rising importance of privacy and personal information in light of contemporary technological and societal transformations, and by examining the intricate interconnections between privacy, data protection, and the digital infrastructures that shape modern life.

Chapter 3 situates the UK GDPR within its historical and legislative context. It outlines the development of data protection laws in the UK, beginning with the DPA 1984,³² and traces their evolution through the DPA 1998³³ up to the present framework established by the DPA 2018 and the retained EU GDPR following Brexit. It also examines the genesis of the EU GDPR itself, highlighting the socio-political pressures and technological transformations that made such a regulation both necessary and urgent. This chapter aims to lay the foundational understanding of how the GDPR came into being, its principal features, and the role it has played in shaping the UK's post-Brexit data protection strategy.

Chapter 4 offers a critical assessment of the UK GDPR model's effectiveness. It begins by evaluating the regulation's major principles, including lawfulness, fairness, transparency, purpose limitation, and data minimisation, and assesses how these principles are implemented and enforced in practice. Special attention is paid to the transition from the pre-GDPR era and how organisations, regulators, and individuals have responded to the new framework. The chapter explores both qualitative and quantitative indicators of effectiveness, such as the volume of data breach reports, the number and nature of enforcement actions by the Information Commissioner's Office (ICO),³⁴ and compliance behaviours among data

³² Data Protection Act 1984 (Legislation.gov.uk2022) <<https://www.legislation.gov.uk/ukpga/1984/35/enacted>>.

³³ Data Protection Act 1998 (Legislation.gov.uk1998)
<<https://www.legislation.gov.uk/ukpga/1998/29/contents>>.

³⁴ ICO, 'Information Commissioner's Office' (Ico.org.uk21 March 2024) <<https://ico.org.uk/>>.

controllers. The chapter argues that while the UK GDPR strengthens data subjects' rights, challenges remain in areas such as public awareness, enforcement consistency, and clarity in interpretation.

In Chapter 5, the focus shifts to judicial interpretation and enforcement, specifically examining how UK courts have addressed the misuse of personal data before and after the GDPR's implementation. Drawing on decided cases, the chapter analyses how courts have adjudicated on conflicts involving data protection claims, especially in the context of online platforms, social media, and journalism. The chapter contrasts judicial approaches under the DPA 1998 and the UK GDPR, identifying trends in the courts' willingness to uphold privacy claims and their reliance on ancillary legal doctrines such as the tort of misuse of private information. Through this analysis, the chapter highlights the growing judicial recognition of the digital dimensions of privacy and the increasing use of the GDPR in litigation strategies.

Chapter 5 further broadens the analytical scope by examining the legal framework governing online privacy protection in the UK beyond the GDPR. This includes a detailed consideration of the DPA 2018, which complements the UK GDPR and contains specific provisions such as exemptions for journalistic activities, national security, and academic research. The chapter also explores the role of the tort of misuse of private information, which continues to provide a common law remedy for privacy violations and has been instrumental in landmark decisions such as *Campbell v MGN Ltd*³⁵ and *NT1 & NT2 v Google*.³⁶ The interplay between statutory and common law remedies is critically evaluated to determine whether the current legal framework offers a coherent and robust protection mechanism for personal information online.

³⁵ *Campbell v MGN Ltd* [2004] UKHL 22; [2004] 2 AC 457; [2004] 2 WLR 1232; [2004] EMLR 247.

³⁶ *NT1 & NT2 v Google* [2018] EWHC 799 (QB); [2018] EMLR 18; [2018] HRLR 13.

Chapter 6 introduces a comparative element by examining China's current legal framework regarding the misuse of personal data online. This chapter provides a detailed analysis of China's Personal Information Protection Law (PIPL),³⁷ Cybersecurity Law,³⁸ and related regulatory measures. It evaluates how Chinese courts, and administrative bodies have dealt with personal information disputes, and how the regulatory environment differs structurally and philosophically from that of the UK. Through selected case studies, the chapter illustrates the practical challenges and advancements in China's effort to establish a functional data protection regime. This comparative inquiry is not only useful for understanding China's domestic approach, but also provides alternative models of data governance that contrast with Western legal and political traditions.

Building on the comparative approach, Chapter 7 deepens the analysis of China's legal system by evaluating its foundational principles, enforcement mechanisms, and institutional capacity in protecting personal information online. It considers the roles of various actors including the Cyberspace Administration of China (CAC),³⁹ courts, and private litigants. The chapter examines the effectiveness of these institutions in responding to the rapid digitalisation of personal data usage in China and the increasing international scrutiny of its data protection standards. It also investigates how China's regulatory focus on national security, surveillance, and data sovereignty influences its broader data protection policies. This chapter provides a

³⁷ Personal Information Protection Law (China) (中华人民共和国个人信息保护法) [2021] ('PIPL'), available at https://en.spp.gov.cn/2021-12/29/c_948419.htm; without otherwise explained, all translation from Chinese texts was performed by author herself. The Chinese translation into English texts of direct quotes and titles of primary and secondary legal sources is accompanied by the original Chinese texts online wherever necessary.

³⁸ Cybersecurity Law of the People's Republic of China [Effective] 中华人民共和国网络安全法 (Lawinfochina.com2016) <<https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3>>.

³⁹ Cyberspace Administration of China, 'CyberspaceAdministrationofChinaLaunchestheInitiativeonChina-AfricaJointlyBuildingaCommunitywithaSharedFutureinCyberspace_中央网络安全和信息化委员会办公室' [2021] (www.cac.gov.cn) <https://www.cac.gov.cn/2021-08/25/c_1631480920680924.htm>.

critical context for drawing meaningful comparisons with the UK GDPR, helping to frame the broader implications of different legal and political environments on privacy rights.

Chapter 8 synthesises the findings of the preceding chapters to assess the current and future viability of the UK GDPR model, particularly in the post-Brexit context. It reflects on whether Brexit has undermined or enhanced the UK's capacity to enforce robust data protection standards and explores whether the UK may diverge from the EU GDPR framework in the future. The chapter also revisits the comparison with China, drawing final conclusions about the respective strengths and weaknesses of each legal regime in addressing the misuse of personal information online. It considers whether China might adopt more elements of the GDPR model, or whether its trajectory will remain distinct due to ideological, political, and institutional factors.

By juxtaposing the UK's legal model with China's evolving regulatory framework, the thesis contributes to a richer understanding of how legal systems conceptualise and enforce the right to privacy in the digital age. It also opens up critical dialogue on whether a universal or pluralistic approach to data protection is more desirable in a globalised yet ideologically fragmented world. Ultimately, the thesis evaluates the effectiveness of balancing legal, cultural, and technological considerations in the current data protection frameworks of the UK and China.

CHAPTER 2 THE CONCEPT OF PRIVACY AND ITS SIGNIFICANCE IN RELATION TO PERSONAL INFORMATION

*If we are to have a true knowledge of an object we must look at and examine all its facets, its connections and 'mediacies'.*⁴⁰ In relation to personal information, an understanding requires an initial exploration of the concept of privacy and its various, often contested, definitions. Contemporary legal protections for personal data are underpinned by a particular conception of informational privacy, one which often determines what is safeguarded and delineates the scope and character of that protection. However, this foundational conception warrants critical and theoretical re-examination. The dominant legal conception of privacy, rooted largely in individual autonomy and control over personal information, was constructed in an era that could not anticipate the scale, opacity, and commercial logic of modern data processing. It reflects assumptions about bounded, identifiable data subjects and discrete disclosures that are increasingly fictitious in the age of algorithmic profiling. Accordingly, this thesis contends that it is both necessary and urgent to reconceptualise the modern legal understanding of privacy and, in light of that, to develop bespoke legal remedies aligned with a redefined normative framework.

Privacy, at its essence, remains a fluid, context-contingent construct.⁴¹ It resists meaningful abstraction when divorced from the socio-legal realities within which it operates. This chapter does not attempt to extract a definitive or universalised meaning of privacy from the

⁴⁰ Vladimir Lenin, 'Once Again on the Trade Unions' (Marxists.org2025) <<https://www.marxists.org/archive/lenin/works/1921/jan/25.htm>>; Section: Dialectics and Eclecticism 'School' and 'Apparatus'.

⁴¹ See Florian Schaub, Bastian Konings and Michael Weber, 'Context-Adaptive Privacy: Leveraging Context Awareness to Support Privacy Decision Making' (2015) 14 IEEE Pervasive Computing pp 34-35.

voluminous theoretical discourse. Rather, it aims to contextualise and concretise privacy by offering a distinct perspective, one which recognises the transformative impact of technological advancements⁴² on privacy in contemporary life. Whereas traditional conceptions of privacy were shaped largely by physical and spatial concerns, the proliferation of digital technologies has introduced unprecedented threats to personal autonomy and informational control.⁴³ Article 12 of the Universal Declaration of Human Rights (UDHR)⁴⁴ affirms this, stipulating that: *‘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.’* In view of this principle, modern legal systems are compelled to re-evaluate the conceptual contours of privacy, the emergence of novel forms of its violation, and the adequacy of existing legal and remedial mechanisms.

Chapter 2 is thus structured into four sections, each interrogating a distinct dimension of privacy in both physical and digital contexts. The first section addresses the bifurcation between physical and informational privacy. It aims to delineate the conceptual and practical differences between these forms, elucidating their respective roles in shaping individual experience. Physical privacy pertains to the inviolability of personal space and bodily autonomy, shielding individuals from surveillance and intrusion. Informational privacy, by contrast, concerns the control and protection of personal data and communications in digital environments. This section traces the historical development of these concepts and examines

⁴² See *infra* chapters 4 and 5.

⁴³ See Urs Gasser, ‘Futuring Digital Privacy: Reimagining the Law/Tech Interplay’ (Mira Burri ed, Cambridge University Press 2021) p 198 <<https://www.cambridge.org/core/books/big-data-and-global-trade-law/futuring-digital-privacy/D6F968FA6C40F8EF557BBFB1CD333281>>.

⁴⁴ United Nations, ‘Universal Declaration of Human Rights’ (United Nations 1948) <<https://www.un.org/en/about-us/universal-declaration-of-human-rights>>.

their evolving relevance amidst the proliferation of digital technologies and data-driven systems.

The second section engages with the conception of privacy as a right to informational self-determination, that is, the right of individuals to control access to, and use of, their personal data. It interrogates the dynamics of consent, data ownership, and the structural challenges individuals face in regulating access to their information. In a digital economy driven by surveillance capitalism, individuals often unknowingly relinquish control over their data, with profound ethical and legal consequences. This section examines the legal and normative imperatives for reinforcing individual agency in data governance, particularly in an environment where personal data is commodified and subject to widespread exploitation.

The third section focuses specifically on digital privacy, addressing the unique vulnerabilities and risks associated with online activity. It examines phenomena such as algorithmic tracking, data breaches, cybercrime, and the regulatory responses designed to mitigate such harms. Central to this discussion are legal instruments such as the GDPR, the proliferation of surveillance technologies, and the evolving jurisprudence surrounding digital rights. This section will assess the efficacy of current legal frameworks and explores the enduring tension between innovation, security, and individual privacy.

Through these three analytical lenses, section 2.4 aims to provide an in-depth exploration of the evolving notion of privacy and the ways in which individuals are navigating the increasing complexity of maintaining control over their lives: both physical and digital. The chapter concludes by emphasising the growing significance of privacy and personal information

considering contemporary technological and societal shifts, and it poses the intricate relationship between privacy, data protection, and the digital architecture of modern life.

2.1 The Conceptions of Privacy: Physical and Informational Dimensions

The concept of privacy occupies an increasingly contested and complex position within modern legal discourse. While privacy has longstanding roots in both the UK and European legal traditions, its doctrinal foundations remain unsettled. In the UK context, privacy has evolved not through direct statutory recognition, but rather through a patchwork of legal instruments and judicial interpretation, particularly under the influence of European human rights law. Despite the incorporation of the ECHR into domestic law via the HRA 1998, there is still no autonomous right to privacy explicitly recognised in English law which could be claimed against private as well as public bodies.⁴⁵ Parliament has shown a lack of enthusiasm⁴⁶ to legislate to recognise such a right, and common law, on its own, has historically lacked the conceptual apparatus to protect privacy comprehensively.

In the absence of a general right to privacy, two principal legal mechanisms currently underpin privacy protection in the UK; the equitable doctrine of breach of confidence, reconceptualised as the tort of misuse of private information (chapter 5), and Article 8 of the ECHR, which guarantees the right to respect for private and family life, home, and correspondence to be claimed against public authorities. Since the enactment of the HRA, the judiciary has

⁴⁵ *Wainwright v Home Office* (2003) UKHL 53, § 35.

⁴⁶ See David J Seipp, 'English Judicial Recognition of a Right to Privacy' (1983) 3 Oxford Journal of Legal Studies pp 325-326.

incrementally expanded the scope of confidence to serve as a functional, if limited, substitute for a formal privacy right, creating the tort of misuse of private information.

This doctrinal gap was further illustrated in *Kaye v Robertson*.⁴⁷ The Court of Appeal held that English law did not recognise a general right to privacy, even in circumstances involving egregious invasions of personal dignity. The claimant, a hospitalised actor, had been photographed and interviewed by journalists without his consent while recovering from serious head injuries. Despite the moral intuitiveness of the privacy claim, the court was confined to awarding relief under the tort of malicious falsehood, highlighting the inadequacies of the legal framework in protecting privacy *per se*. By contrast, the jurisprudence of the European Court of Human Rights (ECtHR) has developed a broader conception of privacy. In *Peck v United Kingdom*,⁴⁸ the Court held that the public dissemination of CCTV footage capturing the applicant's attempted suicide constituted a violation of Article 8. The Court distinguished between the mere observation of individuals in public and the processing and publication of recorded data, with the latter engaging the right to private life. This distinction is drawn from *Herbecq and the Association 'Ligue des droits de l'homme' v Belgium*,⁴⁹ in which the Court clarified that observation in itself does not amount to a privacy violation,⁵⁰ unless coupled with systematic recording and dissemination.

In the domestic context, statutory protections for informational privacy in the form of data protection were first established through the DPA 1984, and subsequently reformed under the

⁴⁷ *Kaye v Robertson* [1991] FSR 62.

⁴⁸ *Peck v The United Kingdom* [2003] EHRR 287 (App. No. 00044647/98)

⁴⁹ *Herbecq and the Association 'Ligue des droits de l'homme' v Belgium* 32200/96 and 32201/96 Dec Ision of 14 January 1998 on the admissibility of the applications.

⁵⁰ *Ibid*, § 59.

DPA 1998, and most recently, the DPA 2018, incorporating the GDPR. These instruments operate within the broader framework of Article 8 of the ECHR and attempt to reconcile the right to privacy with competing interests, providing an overarching framework for privacy protection and guiding the development of data protection laws,⁵¹ as discussed in Chapters 3 and 4,⁵² such as freedom of expression, public security, and economic activity.

Nonetheless, the conceptual foundations of privacy remain elusive. Legal and philosophical scholarship frequently references Warren and Brandeis's seminal definition of privacy as 'the right to be let alone.'⁵³ While rhetorically appealing, this formulation lacks precision and does not provide a clear or moral account for the complexities of privacy in the digital age.⁵⁴ In contemporary discourse, privacy has often been described as a 'concept in disarray,'⁵⁵ lacking definitional clarity, coherent theoretical underpinnings, and uniform normative justification. This ambiguity has made it difficult to construct a comprehensive legal framework capable of addressing the multi-faceted nature of privacy.

This definitional uncertainty is not new. In 1972, the Younger Committee on Privacy⁵⁶ advised against the formal recognition of a statutory right to privacy, citing '*lack of any clear and generally agreed definition of what privacy itself is.*'⁵⁷ The Committee's concerns remain salient: if the legal system is to protect privacy meaningfully, it must first determine what

⁵¹ See Charles Raab and Benjamin Goold, 'Protecting Information Privacy' (2011) Equality and Human Rights Commission Research report 69, p 1.

⁵² See *infra* pp 68-72, 97-100.

⁵³ See Samuel D Warren and Louis D Brandeis (note 25).

⁵⁴ Gavin Phillipson and Helen Fenwick, 'Breach of Confidence as a Privacy Remedy in the Human Rights Act Era' (2000) 63 Modern Law Review pp 660-661.

⁵⁵ See Daniel Solove, 'Understanding Privacy (Chapter One)' (2008) Harvard University Press, p 1.

⁵⁶ See *infra* pp 71-72.

⁵⁷ See Report on <https://api.parliament.uk/historic-hansard/commons/1973/jul/13/privacy-younger-report>; see also comments from Gerald Dworkin, 'The Younger Committee Report on Privacy' (1973) 36 The Modern Law Review 399 <<https://www.jstor.org/stable/1093890>>.

interests such protection is intended to secure, autonomy, dignity, control over information, or something else entirely.

Moreover, modern threats to privacy have grown exponentially. The rapid proliferation of digital technologies, mass surveillance practices, and the commodification of personal data by both state and private actors⁵⁸ have created a legal environment in which traditional conceptions of privacy are no longer adequate. The ‘secrecy paradigm,’⁵⁹ which treats privacy as the ability to keep personal information hidden, is increasingly untenable in a world of near-constant data collection and algorithmic profiling.⁶⁰ Against this scene, it is more analytically productive to view privacy as an *umbrella* term,⁶¹ encompassing a plurality of interests including bodily integrity, spatial autonomy, decisional freedom, and informational control. This pluralistic model not only aligns with the practical realities of contemporary life, but also offers a more coherent basis for legal and regulatory development. Importantly, such an approach allows for differential treatment of privacy claims depending on context, interest, and degree of interference.⁶²

2.2 Privacy as the Right to Control Personal Information

⁵⁸ See Charles Raab and Benjamin Goold (note 51) Executive summary.

⁵⁹ See Daniel J. Solove, ‘A Taxonomy of Privacy’ (2006), University of Pennsylvania Law Review pp 477, 497.

⁶⁰ See Scott Skinner-Thompson, *Privacy at the Margins* (Cambridge University Press 2020), p 8.

⁶¹ Daniel J. Solove, ‘A Taxonomy of Privacy’ (2006), University of Pennsylvania Law Review p 485.

<https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1376&context=penn_law_review>.

⁶² Charles Raab and Benjamin Goold (note 51) p 16.

The theoretical foundation of privacy as a legal and normative concept remains elusive. As Arthur Miller once remarked, privacy is ‘difficult to define because it is exasperatingly vague and evanescent.’⁶³ Similarly, Daniel Solove observed, in 2008, that privacy is often poorly theorised and rarely subjected to rigorous conceptual scrutiny.⁶⁴ In this context of definitional ambiguity, one influential approach has emerged: the conceptualisation of privacy as the right to control personal information. This understanding has gained traction particularly through the work of Alan Westin and is echoed in the German doctrine of informational self-determination.⁶⁵

According to Westin, privacy entails the individual’s right ‘to control, edit, manage, and delete information about themselves and to decide when, how, and to what extent such information is communicated to others.’⁶⁶ Rather than being conceived as an absolute condition of secrecy, privacy in this view is understood as a fluid and dynamic process involving the negotiation between disclosure and concealment.⁶⁷ Irwin Altman supports this relational model by describing privacy as the ‘selective control of access to the self,’⁶⁸ suggesting that individuals actively regulate their personal boundaries depending on context and intention. This approach, often linked to the principle of ‘fair information practices,’⁶⁹ has been influential in shaping

⁶³ Arthur R. Miller, *The Assault on Privacy*, (1970) 15 *Law Quadrangle* (formerly *Law Quad Notes*) Available at: <https://repository.law.umich.edu/lqnotes/vol15/iss2/6>.

⁶⁴ Daniel Solove (note 55) p 4.

⁶⁵ Alan Westin, ‘Privacy and Freedom’ (1968) 25 *Washington and Lee Law Review* 166.

⁶⁶ *Ibid*, p 7.

⁶⁷ Monika Taddicken, ‘The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure’ (2013) 19 *Journal of Computer-Mediated Communication* p 249.

⁶⁸ See Irwin Altman, ‘The Environment and Social Behaviour: Privacy, Personal Space, Territory, and Crowding.’ Monterey, California (Ed.gov 1975) p 18 <<https://eric.ed.gov/?id=ED131515>>.

⁶⁹ See Pam Dixon, ‘A Brief Introduction to Fair Information Practices | World Privacy Forum’ (World privacy forum.org September 2012) <<https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/>>; In 1980, the OECD developed a set of eight Fair Information Practices in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, building upon the core principles from the U.S. Department of Health, Education, and Welfare (HEW). It is important to note that while

data protection laws globally and has been central to discussions about balancing individual control over personal data with the state's interest in data processing.

Within the UK legal system, privacy claims are frequently brought under the doctrine of breach of confidence, particularly in the form of the modern tort of misuse of private information.⁷⁰ A paradigmatic illustration is *Prince Albert v Strange*,⁷¹ wherein the Court of Chancery intervened to enjoin the unauthorised publication of intimate etchings belonging to the Royal Family. The defendant who was a publisher was in possession of copies of private etchings of the Royal Family at home. The publisher had attained them from an employee of a printer to whom Prince Albert had entrusted the plates. Despite the absence of an explicit privacy right, Knight Bruce V-C recognised an equitable interest in restraining unauthorised disclosure of private materials, ruling in favour of Queen Victoria and Prince Albert, the court held that:⁷²

'Every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public or commit them only to the sight of his friends.'

This early articulation foreshadowed the recognition that control over personal expression and private materials lies at the heart of privacy, even if expressed indirectly through property or confidentiality doctrines. The court further held that the publication of these etchings invaded

this framework assumes some degree of control over personal information is feasible, it also recognises that the level of control an individual can exercise will vary depending on their circumstances and the type of information involved.

⁷⁰ *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 § 50-51, the court concluded in agreement with the judge that misuse of private information should now be recognised as a tort for the purposes of service out the jurisdiction. This does not create a new cause of action; Rebecca Moosavian, Jigsaws and Curiosities: The Unintended Consequences of Misuse of Private Information Injunctions. (2016) Communications Law, 21 (4). pp 104-105.

⁷¹ *Prince Albert v Strange* (1849) 47 ER 1302.

⁷² See Samuel D Warren and Louis D Brandeis, The Right to Privacy [1890] Harvard Law Review, p 198 fn 2.

the Royal Family's right to privacy, in the sense of a right to control one's possessions and enjoy them. It has been established in many of the UK courts' decisions, that publishing or obtaining information or unauthorised photographs equals to a breach of confidence in situations where it is considered that a relationship of confidence exists. In other words, it is a breach of confidence if the information is damaging to the owner or the subject of such information and used without their consent.

Modern privacy jurisprudence has expanded upon this foundation. The incorporation of the ECHR into UK law via the HRA 1998 has introduced a rights-based framework, particularly through Article 8 ECHR. The Strasbourg Court has recently interpreted Article 8 as encompassing a right to informational self-determination.⁷³ In *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland*,⁷⁴ the Court recognised that control over personal data is integral to one's private life, affirming that the '*protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life.*'⁷⁵

Similarly, Recital 7 of the GDPR echoes this position, stating that '[n]atural persons should have control of their own personal data.' The GDPR, which has shaped data protection across the EU and influenced domestic legislation in the UK post-Brexit, reinforces the principle that individuals must be empowered to manage their digital identities in a context of increasing surveillance and commercial data exploitation.

⁷³ *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] 64 EHRR 8; see Fiona Brimblecombe and Gavin Phillipson, 'Regaining Digital Privacy? The New 'Right to Be Forgotten' and Online Expression' (2018) 4 Canadian journal of comparative and contemporary law. p 10 <<https://durham-repository.worktribe.com/output/1355976>>.

⁷⁴ [2017] 64 EHRR 8.

⁷⁵ *Ibid*, § 137.

However, the practical enforcement of privacy rights in the digital age remains fraught with difficulty. Technological advances and the widespread adoption of online platforms have led to unprecedented levels of data generation, collection, and profiling, for example, it has faced significant challenges in balancing the protection of individuals' privacy with the needs of the state and private entities to acquire and process personal information for legitimate purposes.⁷⁶ Simultaneously, societal attitudes toward privacy are shifting. It is frequently observed, perhaps too simplistically, that younger generations prioritise transparency and self-expression over informational privacy.⁷⁷ Nonetheless, this cultural shift does not negate the importance of legal safeguards; rather, it calls for an approach that reconciles individual autonomy with the realities of digital life.

Indeed, privacy today cannot be adequately protected through secrecy-based models alone. As legal scholars have argued, the traditional 'secrecy paradigm' is no longer viable in a world characterised by ubiquitous data flows and pervasive surveillance.⁷⁸ Instead, privacy must be understood as the capacity to exercise agency over one's personal information, even in circumstances where disclosure is necessary or inevitable. Wragg⁷⁹ contends that informational and intrusion-based privacy claims share a common normative foundation, and that this

⁷⁶ See Charles Raab and Benjamin Goold (note 51) p 25.

⁷⁷ See Geoffrey R. Stone, 'Privacy, the First Amendment, and the Internet' (2010) in Saul Levmore & Martha Nussbaum, eds, *The Offensive Internet: Speech, Privacy, and Reputation* (Cambridge, Mass: Harvard University Press) p 193.

⁷⁸ See Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (2004) NYU Press; GWU Law School Public Law Research Paper 2017-5; GWU Legal Studies Research Paper 2017-5. Available at SSRN: <https://ssrn.com/abstract=2899131>, p 8; Benjamin Gerber, 'Conceptualizing Privacy' (2010) 40 ACM SIGCAS Computers and Society 8; Adam Henschke, 'Surveillance Technologies and Ethical Vacuums' [2017] Cambridge Core 1 <<https://www.cambridge.org/core/books/ethics-in-an-age-of-surveillance/surveillance-technologies-and-ethical-vacuums/620C0E5113B83A910C43E8C0B8ABA28D>>; section 1.2.

⁷⁹ See Paul Wragg, 'Recognising A Privacy-Invasion Tort: The Conceptual Unity of Informational and Intrusion Claims' (2019) 78 *The Cambridge Law Journal* 409, p 413.

conceptual unity justifies their recognition within a single, coherent tort of privacy. His argument operates at the level of mid-level principles, that is, it neither commits to a comprehensive theory of privacy nor attempts to map every conceivable privacy interest.⁸⁰ It can therefore proceed from the relatively uncontroversial premise that privacy is a genuine good to which individuals are entitled as autonomous agents pursuing their own conception of a worthwhile life. Where privacy is violated, the interference with autonomy and dignity may amount to a form of objectification; the victim is effectively reduced to something less than a full person, treated merely as an instrument for the tortfeasor's purposes.⁸¹ Bennett's analysis of intrusion reinforces this critique by adopting a problem-by-problem, triangulated approach to understanding privacy.⁸² This method reveals that the apparent conceptual difficulties standing in the way of recognising broader or novel privacy torts at common law are, on closer examination, illusory.⁸³

In conclusion, the conceptualisation of privacy as a juridical entitlement to informational self-governance constitutes a compelling and increasingly indispensable framework. It reconciles the individual's interest in personal autonomy with the exigencies of contemporary data ecosystems, and it aligns with both European human rights jurisprudence and emergent regulatory architectures. However, as information economies grow ever more opaque and more intrusive, safeguarding these rights demands not merely doctrinal innovation, but a recalibration of the legal system's structural orientation toward data, personal information, and personhood.

⁸⁰ Ibid, p 431.

⁸¹ Ibid.

⁸² See Thomas DC Bennett, 'Triangulating Intrusion in Privacy Law' (2019) 39 Oxford Journal of Legal Studies, pp 31, 32.

⁸³ Ibid.

2.3 A Closer Look at Digital Privacy

Notwithstanding the pervasive discourse surrounding privacy risks in the digital age, empirical studies consistently reveal a behavioural inconsistency among users, a phenomenon widely referred to as the ‘privacy paradox’.⁸⁴ Although users frequently articulate apprehensions regarding the erosion of informational privacy in the face of pervasive surveillance and data commodification, they often neglect to implement even the most elementary or cost-effective protective measures.⁸⁵

Critically, this paradox does not necessarily reflect an abandonment of privacy as a valued norm. Rather, it illustrates the complexity of contemporary privacy as an exercise of selective disclosure and contextual negotiation. Individuals retain the capacity to modulate access to their personal sphere: to determine the scope, audience, and granularity of self-revelation. However, as has been cynically contended by segments of the tabloid media, particularly in relation to public figures, some assert that individuals cannot ‘invade their own privacy,’⁸⁶ a claim often employed to legitimise intrusive reporting on grounds of prior voluntary disclosure. This reasoning is fundamentally flawed. The mere act of sharing information selectively does

⁸⁴ See Daniel Solove, ‘The Myth of the Privacy Paradox the Myth of the Privacy Paradox’ (2021) 89 *George Washington Law Review* 1, p 2.

⁸⁵ *Ibid*, this behavioural dissonance, whereby individuals’ normative commitments fail to translate into protective action, necessitates a deeper interrogation into the psychological, structural, and socio-technical dynamics that condition privacy-related decision-making in digital realm.

⁸⁶ See Fiona Brimblecombe and Gavin Phillipson, ‘Regaining Digital Privacy? The New ‘Right to Be Forgotten’ and Online Expression’ (2018) 4 *Canadian journal of comparative and contemporary law*. p 11 <<https://durham-repository.worktribe.com/output/1355976>>.

not extinguish one's residual privacy interests, nor does it confer *carte blanche* for further dissemination beyond the original context or intent.

What persists, then, is not a diminished valuation of privacy, but a transformation in its expression: people increasingly seek to exercise control over the terms of their exposure, rather than aiming for absolute concealment. In an era marked by ubiquitous connectivity and digital transparency, the right to privacy is less about secrecy *per se* and more about informational autonomy, the right to calibrate, curate, and contextualise the narrative of the self across diverse social and technological interfaces. Thus, even when individuals voluntarily share significant aspects of their lives online, this does not negate the legitimacy of their expectations of privacy within defined relational or situational boundaries.⁸⁷

The genealogy of privacy is intrinsically bound to technological development.⁸⁸ Since ancient times, human societies have exhibited an enduring preoccupation with intrusion, whether in the form of gossip, surveillance, or unsolicited observation.⁸⁹ However, it was the advent of computational technologies in the twentieth century, and particularly the exponential rise of data-processing capabilities, that catalysed a paradigmatic shift in privacy discourse.⁹⁰ The emergence of modern informational privacy law in the early 1970s can be directly traced to the anxieties generated by automated data systems, whose capacity for large-scale surveillance rendered traditional privacy frameworks increasingly obsolete.⁹¹

⁸⁷ Ibid, p 12.

⁸⁸ See Urs Gasser (note 43) p 195.

⁸⁹ Daniel Solove (note 55) p 4.

⁹⁰ Ibid.

⁹¹ See Urs Gasser (note 43) p 196.

Contemporary information and communication technologies (ICTs) have exacerbated these tensions. Innovations such as big data analytics, biometric surveillance, the Internet of Things (IoT), wearable computing, facial recognition systems, and artificial intelligence (AI) have engendered a complex regulatory landscape characterised by data ubiquity, asymmetrical power relations, and attenuated user agency.⁹² In this milieu, personal data has emerged as both a commodity and a locus of vulnerability, its collection, analysis, and circulation giving rise to unprecedented *threats* to privacy about autonomy, dignity, and democratic accountability.⁹³ These concerns have often prompted policymakers to introduce additional privacy protections, while citizens and consumers have increasingly demanded stronger legal and regulatory safeguards to protect their personal information.⁹⁴ Some current developments already indicate or suggest shifts and innovations within privacy and data protection regimes in response to the latest changes in the socio-technological environment. For example, basic ideas of how privacy should be defined have already begun to change.⁹⁵ The notion of what constitutes privacy, once synonymous with seclusion and secrecy, has begun to evolve into a more nuanced understanding grounded in relational autonomy and contextual integrity.

In *Terry v Persons Unknown*,⁹⁶ the claimant sought an anonymised interim injunction to restrain the publication of details pertaining to an extramarital affair. The application was ultimately denied, the court finding that the dominant motivation was not to protect intimate

⁹² Ibid, p 197.

⁹³ See Thorsten Wetzling and Kilian Vieth, 'Legal Safeguards and Oversight Innovations for Bulk Surveillance' [2021] in Lora Anne Viola and Pawel Laidler, *Trust and Transparency in an Age of Surveillance* (Routledge 2021), chapter 8, pp 145-146.

⁹⁴ Ibid.

⁹⁵ See Urs Gasser (note 43), p 198.

⁹⁶ *Terry (previously referred to as 'LNS') v Persons Unknown* [2010] EWHC 119 (QB).

personal life, but to preserve commercial reputation. Terry, as a prominent professional footballer, had actively cultivated a public persona through media appearances and interviews in which aspects of his personal and family life were voluntarily disclosed. This prior engagement was doctrinally significant because it undermined the claim that the information in question retained the necessary quality of confidence or sensitivity. Where a claimant has selectively opened their private life to public scrutiny, deploying personal narrative for reputational or commercial benefit, the courts have been reluctant to permit them to reassert privacy protection when subsequent disclosures become inconvenient.

Wragg's analysis of *Mosley* and *Terry* interrogates whether the public interest in celebrity gossip can legitimately override privacy claims. He argues that such expression carries little weight under Article 10 because it is neither political in nature nor conducive to democratic discourse, the primary justification underpinning Article 10 protection.⁹⁷ In *Mosley*, he concerns a significant feature of the court's approach; its treatment of 'public interest' as a morally neutral concept. The media's characterisation of a claimant's conduct as immoral neither strengthens the case for disclosure nor diminishes the weight of the privacy claim. The mere exposure of immoral behaviour does not, without more, constitute a legitimate public interest.⁹⁸ Turning to *Terry*, Wragg suggests that the court's reasoning extends the principle, accepted by the House of Lords in *Campbell* that the public has a right not to be misled by public figures.⁹⁹ The implication goes further than simply permitting the press to correct inconsistencies between a celebrity's public statements and private conduct; it appears to

⁹⁷ See Paul Wragg, 'A Freedom to Criticise? Evaluating the Public Interest in Celebrity Gossip after *Mosley* and *Terry*' (2010) 2 *Journal of Media Law* 295, pp 308-309.

⁹⁸ *Ibid*, p 302.

⁹⁹ *Ibid*, p 307.

license broader media commentary on what that conduct reveals about the individual's personal standards, or indeed about prevailing moral standards in society more generally.¹⁰⁰

In a related contribution, Wragg argues that *Campbell* held out the promise of a more contextually nuanced approach to the privacy of public figures,¹⁰¹ one sensitive to the specific nature of the information at issue and its genuine public interest value. That promise, however, has gone largely unfulfilled. Courts have since applied broad and inconsistent distinctions between public and private spheres, and their tendency to define 'public interest' expansively has substantially weakened the misuse of private information claim. The failure of the House of Lords in *Campbell* to articulate the public's right not to be misled in precise terms has generated further uncertainty in subsequent case law.¹⁰² Jacob Rowbottom¹⁰³ advances a complementary argument, proposing that the public should be understood as consumers of celebrity, that is, celebrity status is not thrust upon the public but is itself a product of sustained public attention. This framing supports a wider latitude for critical commentary directed at public figures, and remains relevant when determining the boundaries of protected speech and the degree of scrutiny that ought to be tolerated.¹⁰⁴ The decisive question is not simply whether a claimant qualifies as a public figure, but whether the information in question bears on the exercise of public power or the discharge of public trust. That standard would be directly applicable in *Terry*, where the claimant's public role as a professional athlete and purported

¹⁰⁰ Ibid.

¹⁰¹ See Paul Wragg, 'Protecting Private Information of Public Interest: Campbell's Great Promise, Unfulfilled' (2015) 7 Journal of Media Law 225, p 230.

¹⁰² Ibid, p 233.

¹⁰³ See Jacob Rowbottom, "Power and the Public Eye: Why the Limits of Acceptable Criticism Are Wider for Public Figures." (2025) Public Law 1 Sweet & Maxwell, p 11.

¹⁰⁴ Ibid, p 18.

role model was inseparable from the reputational interests he sought to preserve through legal action.

Rebecca Moosavian and Peter Coe¹⁰⁵ contend that the Article 8 rights of the claimants in *Terry* ought to have prevailed, a position that, on examination, amounts to a form of crude ‘zonal’ reasoning,¹⁰⁶ albeit one operating in the claimant’s favour rather than the defendant. A claimant-centred ‘zonal’ approach, under which any information falling within the scope of Article 8 is presumptively unpublishable unless it concerns matters of high political importance, is no more persuasive than the now-discredited pro-defendant version of the same logic. It disregards the claimant’s own agency in creating the circumstances under which the information arose, and it provides no satisfactory explanation for why the law of misuse of private information should operate to protect a false public image that the claimant was not, in any event, entitled to project.¹⁰⁷

The judgment was thus more than a recalibration of the balance between Articles 8 and 10 of the ECHR within the tort of misuse of private information. It reveals the judicial inclination to scrutinise both the nature of the information and the motive for seeking privacy relief, and it exposes the inadequacy of a legal framework that lacks a coherent theory of what public figures can legitimately claim to keep private.¹⁰⁸ *Terry* also illustrates that privacy cannot be retroactively invoked to shield information voluntarily disclosed to the public, nor can one be

¹⁰⁵ See Rebecca Moosavian and Peter Coe, *Balancing Privacy Against Free Speech: In Defence of Exposing Hypocrisy* (2025) in D. Clifford, M. Richardson, and N. Witzleb, *Research Handbook on Privacy and Confidentiality in Media Law* (Edward Elgar, 2026).

¹⁰⁶ *Ibid.*, pp 16-17.

¹⁰⁷ *Ibid.*

¹⁰⁸ See Gemma Horton, ‘Injunctions and Public Figures: The Changing Value in Injunctions for Privacy Protection’ (2021) 13 *Journal of Media Law* 1, pp 81-82.

said to ‘invade their own privacy.’ Such observations must be tempered by the recognition that individuals do not forfeit their entire claim to privacy merely by participating in public discourse. As the courts have increasingly acknowledged, ‘*there are different degrees of privacy*’,¹⁰⁹ that is privacy is not binary but scalar, there exist gradations of personal intimacy, and the threshold for lawful interference must rise in proportion to the sensitivity of the information at stake.

This scalar conception is critical in understanding privacy in the digital context. In an age of pervasive social networking, individuals exercise varying degrees of control over their informational boundaries; they may opt to disclose personal details selectively, strategically curating their online identities.¹¹⁰ As Fried has argued, privacy is essential to the conditions of trust that underpin intimate human relationships. It is only under the presumption of confidentiality that individuals are likely to reveal vulnerable or sensitive information.¹¹¹ In this sense, the guarantee of privacy is not antithetical to self-expression, but rather a precondition for its most authentic forms.

Digital privacy, therefore, should not be misconstrued as the total absence of disclosure. Rather, it concerns the ability to determine the terms of that disclosure: its audience, extent, duration, and purpose. It is, at its core, about informational self-governance; the freedom to delineate one’s personal boundaries in an increasingly porous digital landscape. As this chapter has illustrated, both legal doctrine and normative theory are gradually adapting to reflect this more

¹⁰⁹ *Campbell v MGN* [2004] UKHL 22, § 118.

¹¹⁰ See Fiona Brimblecombe and Gavin Phillipson, ‘Regaining Digital Privacy? The New ‘Right to Be Forgotten’ and Online Expression’ (2018) 4 Canadian journal of comparative and contemporary law. p 15 <<https://durham-repository.worktribe.com/output/1355976>>.

¹¹¹ See Charles Fried, ‘Privacy’ (1968) 77:3 The Yale Law Journal 475.

sophisticated understanding, though much remains to be done in operationalising these principles within an effective and enforceable regulatory framework.

2.4 A Further Analysis of Privacy and Personal Information

In the contemporary digital landscape, the ubiquity of personal information has rendered traditional delineations between public and private increasingly porous.¹¹² Personal Information could be defined as ‘information that relates to a person or group of people in some way’,¹¹³ permeates virtually every aspect of societal and technological infrastructure. It is no longer confined to intimate domains but rather extends to ostensibly innocuous and non-sensitive data points, such as browsing habits, geolocation data, or consumer preferences. Nevertheless, this seemingly banal information can become deeply revealing when aggregated, analysed, or cross-referenced, transforming the informational into the personal, and the personal into the intimate.¹¹⁴

While privacy and personal information are often treated synonymously in both legal and colloquial usage, there are critical conceptual and normative distinctions between the two. Privacy, as a normative value, concerns the ability of individuals to exercise control over access to their personhood, whether physical, decisional, or informational. In contrast, personal information is a category of data, a content-specific concept that refers to identifiable or

¹¹² See Adam Henschke, ‘Surveillance Technologies and Ethical Vacuums’ [2017] Cambridge Core 1 <<https://www.cambridge.org/core/books/ethics-in-an-age-of-surveillance/surveillance-technologies-and-ethical-vacuums/620C0E5113B83A910C43E8C0B8ABA28D>> section 5.1.

¹¹³ Ibid.

¹¹⁴ Ibid, section 2.1.

attributable characteristics, regardless of whether the individual maintains any real or perceived control over its dissemination. In this light, the protection of personal information becomes an instrumental mechanism in safeguarding broader privacy interests.

Philosophical accounts illuminate the nuanced moral dimensions of this distinction. James Griffin posits that privacy is not a luxury but an ‘empirical necessity’ for human rights flourishing.¹¹⁵ Without the protective envelope of privacy, personal autonomy is jeopardised by external social pressures.¹¹⁶ As Griffin notes, the richness of interpersonal relationships relies upon the secure space privacy provides, space that enables self-revelation without fear of exposure or reprisal.¹¹⁷ Reiman similarly distinguishes between informational access and relational care, arguing that the significance of personal information lies not in its mere availability but in the relational context within which it is shared.¹¹⁸ Intimacy, under this view, is not a product of data disclosure *per se*, but of mutual investment, trust, and the voluntary curation of one’s personal narrative. Julie Inness furthers this argument by asserting that privacy comprises not only the protection of information, but also the agent’s decisional authority over intimate matters, framing privacy as the ability to define the parameters of one’s own intimate sphere.¹¹⁹

Where these philosophical positions converge is in the emphasis on control, the agency to determine who accesses which dimensions of the self and under what conditions. It is in this conceptual terrain that data protection law operates. Rather than wade into metaphysical

¹¹⁵ See James Griffin, *On Human Rights* (Oxford University Press 2008), p 226.

¹¹⁶ See Andrew McStay, *Privacy and the Media* (SAGE 2017), pp 14, 20.

¹¹⁷ *Ibid*, pp 226, 227.

¹¹⁸ Jeffrey H Reiman, ‘Privacy, Intimacy, and Personhood’ (1976) 6 *Philosophy & Public Affairs* 26 <<https://www.jstor.org/stable/2265060>>, pp 33-34.

¹¹⁹ See Julie Inness, *Privacy, Intimacy, and Isolation* (Oxford University Press 1992), pp 87-88, 92.

inquiries over the essence of privacy, data protection frameworks, as advocated by van den Hoven and John Weckert, aim to preserve the moral function of privacy, its role in enabling autonomy, maintaining dignity, and fostering the integrity of personal relationships.¹²⁰ The regulatory emphasis therefore shifts from the definitional to the justificatory: What moral or political ends are served by limiting access to personal data? What harms arise from its unregulated use?

This functionally grounded view of privacy as facilitated through data protection aligns with legal developments in both domestic and supranational contexts.¹²¹ English Courts have gradually recognised that personal information, even when not overtly intimate, can warrant protection when its exposure impinges upon an individual's dignity, autonomy, or legitimate expectations of confidentiality.¹²² They are increasingly proactive in minimising privacy intrusions stemming from their own proceedings, while also expanding privacy protections through legal doctrines and procedural safeguards in litigation, such as the tort of misuse of private information and by imposing procedural safeguards in litigation to limit intrusive disclosures.¹²³ Requirements of necessity and proportionality, for example, must be satisfied before compelling parties to submit to medical examinations or invasive inquiries,¹²⁴ a recognition that informational access must be justified by more than mere relevance. Thus, personal information becomes the site at which privacy interests are most acutely negotiated in practice. The legal emphasis on proportionality, balancing individual rights against the

¹²⁰ Van Den and John Weckert, *Information Technology and Moral Philosophy* (Cambridge University Press 2010), pp 317-318.

¹²¹ Adam Henschke, 'Surveillance Technologies and Ethical Vacuums' [2017] Cambridge Core 1 <<https://www.cambridge.org/core/books/ethics-in-an-age-of-surveillance/surveillance-technologies-and-ethical-vacuums/620C0E5113B83A910C43E8C0B8ABA28D>> Figure 2.1.

¹²² See David J Seipp (note 46) p 343.

¹²³ Ibid; see The Privacy Perspective, 'A Brief Introduction to the Concept of Privacy under English Law – Parts I, II & III' (The Privacy Perspective 4 April 2019) <<https://theprivacyperspective.com/2019/04/04/a-brief-introduction-to-the-concept-of-privacy-under-english-law-parts-i-ii-iii/>>.

¹²⁴ See David J Seipp (note 46) p 360.

legitimate interests of the state, media, or commercial entities, reflects an evolving jurisprudence that treats personal data not merely as a commodity, but as a locus of moral concern and potential vulnerability.

In conclusion, while privacy and personal information are interdependent, they are not reducible to one another. Privacy is a normative ideal rooted in autonomy and relational trust, while personal information constitutes the evidentiary and operational terrain through which privacy is protected, or, conversely, undermined. As legal, technological, and ethical discourse continues to evolve, it becomes imperative to maintain analytical clarity between these concepts, while also recognising their mutual entanglement in the pursuit of human dignity in the digital age.

2.5 Conclusion

In light of the increasing complexity of data processing activities driven by technological advancement, the following chapters will centre their analytical focus on the protection of personal information in the digital world. Specifically, they examine the safeguarding of individual rights and the availability of legal remedies in cyberspace. This thesis, in the following chapters, adopts a comparative perspective, examining developments in both the UK (Chapters 3-5) and China (Chapters 6-7) to observe emerging trends and anticipate the future trajectory of privacy and evaluate the effectiveness of the protection of personal information under current regime.

At present, breaches of protection for personal information typically arise through two principal pathways. The first is voluntary disclosure, whereby data subjects intentionally disclose their personal data on digital platforms. These platforms often include social networking services (e.g., Instagram, Facebook), as well as third-party service providers and intermediaries. While such disclosures are ostensibly made with a degree of autonomy, they are undermined by ambiguous data processing agreements and insufficient user awareness. While such disclosures are ostensibly made with a degree of autonomy, they are fundamentally undermined by ambiguous data processing agreements, insufficient user awareness, and critically the structural instability of the contractual frameworks through which consent is purportedly obtained. A particularly acute dimension of this problem concerns the frequency, opacity, and unilateralism with which platforms alter their Terms of Service. Users who ostensibly consent to data processing at the point of registration may find, often without meaningful notice, that the terms governing that processing have been materially revised; expanding the scope of data use, introducing new third-party sharing arrangements, or redefining the purposes for which data may be processed. The practical consequence is that initial consent, already of questionable validity given the length, complexity, and inaccessibility of most platform agreements, is rendered increasingly fictitious over time as the normative basis on which it was given quietly shifts beneath the user.

Peter Coe's¹²⁵ analysis identifies a fundamental tension from a free speech and public sphere perspective; delegating decisions about permissible content to platforms, through their terms of service, and relying on those platforms to apply such terms consistently, effectively transfers

¹²⁵ See Peter Coe, 'Tackling Online False Information in the United Kingdom: The Online Safety Act 2023 and Its Disconnection from Free Speech Law and Theory' (2023) 15 *Journal of Media Law* 1, 213, p 235.

control over freedom of expression to private commercial actors such as Facebook and X.¹²⁶ The degree to which users will meaningfully influence how platforms discharge any resulting duty, and whether that duty will be applied with consistency, remains uncertain. This uncertainty is, arguably, precisely what proponents of removing the ‘legal but harmful’ provisions from the Online Safety Act (OSA) sought to guard against.¹²⁷ That aspect of the statutory framework creates a backdoor through which platforms may remove content that is harmful yet lawful, thereby undermining the social function of free speech and, in particular, the democratic case for open public deliberation.

Fenwick and Coe deepen this critique,¹²⁸ arguing that platform self-regulation has effectively rendered tech companies the de facto arbiters of online expression, without producing a satisfactory balance between suppressing anti-democratic harms and preserving legitimate free speech. Platforms adopt markedly different approaches to content moderation; some remove harmful material more swiftly than others, and individual companies’ policies are themselves subject to rapid and unpredictable change. This inconsistency has produced an uneven landscape in which restraint on harmful content is erratic, occasionally serving democratic ends by preserving expressive freedom, but equally enabling the dissemination of content that actively subverts those ends. The efficacy of self-regulation is therefore, almost inevitably, both structurally questionable and practically unreliable. Paul Bernal sharpens this point further,¹²⁹ observing that platform policy changes appear to be reactive rather than principled,

¹²⁶ Ibid.

¹²⁷ Ibid, Online Safety Act 2023 (Legislation.gov.uk2023) <<https://www.legislation.gov.uk/ukpga/2023/50>>.

¹²⁸ See Helen Fenwick and Peter Coe, ‘The Online Safety Act 2023: Fostering Democratic Participation While Combatting Anti-Democratic Harms?’ (2025) 76 Northern Ireland Legal Quarterly 83, p 103.

¹²⁹ See Paul Bernal, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge University Press 2018), p 127.

driven more by the commercial imperatives of reputational management than by any genuine commitment to free expression or democratic values.

Shoshana Zuboff¹³⁰ situates these concerns within a broader structural critique. She argues that surveillance capitalism does not simply reproduce established capitalist dynamics, such as competitive production, profit maximisation, and growth, but superimposes upon them a new logic of accumulation with its own distinctive operating principles. Zuboff contends that in the nearly two decades since surveillance capitalism's emergence, existing legal frameworks, centred primarily on privacy and antitrust, have proven wholly inadequate to constrain its expansion.¹³¹ What is required, she argues, are laws that fundamentally reject the legitimacy of surveillance capitalism's foundational claims and disrupt its core operations, including the unauthorised conversion of human experience into behavioural data; the appropriation of behavioural surplus as a costless raw material; the extreme concentration of the means of data production; the manufacture and trading of prediction products; the deployment of those products for third-order purposes of behavioural modification, influence, and control; and the accumulation of vast, privately held concentrations of knowledge, what Zuboff terms the 'shadow text' together with the disproportionate power such concentrations confer on those who hold them.¹³² As a result, data subjects, *self-initiated*, would be subjected to substantial intrusions into their privacy, particularly when their data are repurposed or monetised by the platform or downstream data recipients in ways that exceed the original scope of consent.

¹³⁰ See Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019), pp 50, 218.

¹³¹ Ibid.

¹³² Ibid.

The second pathway involves involuntary disclosure, which occurs when personal information is disseminated on digital platforms without the data subject's explicit authorisation, or indeed, their knowledge. This commonly manifests itself in the form of algorithmic profiling, where platforms infer user attributes and establish social connections based on behavioural data, or through the exploitation of AI technologies (such as deepfakes) to manipulate or misuse of personal information. These forms of disclosure, often passive, are inherently more opaque and present heightened risks that are difficult for data subjects to foresee or control.

It is critical to note that the boundary between voluntary and involuntary disclosure is often porous in practice. Information initially provided voluntarily may, under certain conditions, be repurposed in ways that violate the expectations or rights of the data subject. For instance, where personal data is submitted for the purpose of accessing a particular service, but subsequently utilised for commercial gain or targeted advertising beyond the scope of the original transaction, such use may amount to a *de facto* breach of the individual's right to privacy. The following chapters will examine the two categories of personal information processing described above, trace the evolving contours of the privacy concept in the contemporary society, and critically assess whether existing legal frameworks provide sufficient protection and responsive remedies for personal information and individual rights in the digital era.

CHAPTER 3 PUTTING THE GDPR INTO CONTEXT: EXAMINING THE EFFICACY OF THE PREVIOUS DATA PROTECTION REGIME

3.1 Introduction

This chapter will examine the efficacy of the previous data protection regime, including discussion of the basic definitions of data protection, taking account of the concept of privacy. Chapter 2 provides the next Chapters 3-5 with a research basis for analysing current personal data protection regimes. Chapter 3 interrogates the foundational architecture of data protection law by critically examining the efficacy of the pre-GDPR regime, tracing its conceptual origins, structural limitations, and the normative assumptions about privacy upon which it was built. In doing so, Chapter 3 provides the essential research foundation upon which Chapters 4 to 5 are built. The key features to be examined in Chapter 4, including the core principles, enforcement mechanisms, and rights architecture of the current UK GDPR, and the evaluative framework deployed in Chapter 5, including critical analysis of the right to be forgotten as a paradigmatic illustration of the GDPR's ambitions and limitations, will be contextualised by the historical and conceptual groundwork laid here.

Privacy is widely regarded as a fundamental human right in many modern societies, as recognised in Article 12 of the UDHR and Article 8 of the ECHR.¹³³ However, ensuring the effectiveness of privacy protections requires more than just international legal recognition; it necessitates specific and detailed domestic regulations and legal standards. A society that fails to maintain a well-balanced social order is unlikely to protect the privacy of its citizens. Various

¹³³ See *supra* p 38; see European Data Protection Supervisor, 'Data Protection | European Data Protection Supervisor' (www.edps.europa.eu9 February 2024) <https://www.edps.europa.eu/data-protection/data-protection_en>.

factors, such as war, cultural traditions, and religious influences, can directly undermine the levels of privacy protections. For instance, in countries where security concerns disrupt daily life, individuals' privacy is often compromised. Many individuals were, and in some cases still are, unaware of how their personal information is collected, shared, and utilised by various entities. They typically focus on the content and functionality of websites, paying little attention to behind-the-scenes data practices, such as the use of cookies or the implications of accepting terms and conditions.¹³⁴ Likewise, the regulations of private information are diverse under different countries' legal systems. For example, personal information could easily be captured and misused from UAVs (Unmanned Aerial Vehicles) nowadays. In Japan, the state does not allow UAVs to record videos from high above in order to protect privacy.¹³⁵ But in China, the regulation of UAVs is not a high priority under the Chinese legal system, as discussed in Chapter 7.

It is essential, however, to distinguish between privacy and data protection. While often used interchangeably, these notions are conceptually distinct. Privacy is a broad right concerning personal autonomy and the control of personal space, communications, and decisions. Data protection, by contrast, refers more narrowly to the governance of personal data: how it is collected, stored, processed, and shared. The conflation of these terms risks obscuring the unique legal standards and objectives each entail. Lynskey¹³⁶ has argued that the right to data protection in a pre-Charter era¹³⁷ in the EU was of limited value, prior to the digital age, since

¹³⁴ See Monika Taddicken, 'The "Privacy Paradox" in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure' (2013) 19 *Journal of Computer-Mediated Communication* pp 250-251; Nina Gerber, Paul Gerber and Melanie Volkamer, 'Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behaviour' (2018) 77 *Computers & Security* p 227.

¹³⁵ Civil Aviation Bureau, Japan's Safety Rules on Unmanned Aircraft (UA)/Drone - MLIT Ministry of Land, Infrastructure, Transport and Tourism' (Mlit.go.jp2015) <<https://www.mlit.go.jp/en/koku/uas.html>>.

¹³⁶ Orla Lynskey, 'Deconstructing Data Protection: The 'Added-Value' of the Right to Data Protection in the EU Legal Order' (2014) 63 *International and Comparative Law Quarterly*.

¹³⁷ European Union, Charter of Fundamental Rights of the European Union [2000] OJ C364/01 and [2010] OJ C83/389, Article 8 of the EU Charter of Fundamental Rights.

awareness and understanding of the scope and significance of personal data collection and processing was not widespread.¹³⁸ People often had, and may still have, limited awareness of the ways in which their personal information was collected, shared and used by various entities. Users may only be interested about the experiences and contents on websites, but fail to concern themselves with matters such as cookies and agreement terms when they are searching. This cognitive disengagement reflects a structurally engineered information asymmetry in which platforms are incentivised to obscure the nature and extent of data processing behind layers of legal complexity and interface design deliberately calibrated to minimise informed resistance. The regulation appeared to shift public understanding of the relationship between individuals and their data, transforming what had been an abstract and largely invisible process into a matter of everyday awareness, at least at the surface level of consent banners and subject access requests.

However, the critical question here is whether this shift in public consciousness has proved durable, or whether it was always more superficial than transformative. There are compelling reasons to be sceptical. The proliferation of cookie consent banners, widely acknowledged as a paradigmatic example of what has been termed ‘consent fatigue.’ Users click to accept not because they understand or endorse what they are consenting to, but because the architecture of consent is designed to make acceptance the path of least resistance. This thesis therefore treats the question of public awareness as a substantive criterion against which the adequacy of the UK data protection regime must be measured. This point will be developed further in Chapter 5 to explain more about personal experiences online.¹³⁹

¹³⁸ See Orla Lynskey (note 136) II section A, the right to data protection in a pre-charter era.

¹³⁹ *infra* pp 142-146.

Courts in certain states have shown an awareness of the need to comply with reasonably high standards of privacy protection, which will be also considered further in Chapter 4. For example, in *Rundfunk*,¹⁴⁰ which related to EU law, potentially read in the light of Article 8 ECHR, in reaching its conclusion, the Court emphasised that the provisions of the Directive must be interpreted in the light of fundamental rights, in particular to privacy. Therefore, ‘for the purposes of applying the Directive’, the Court systematically examined whether there had been an interference with the right to respect for private life contrary to Art. 8 ECHR and, if so, whether it was justified. In so doing, the Court entirely overlooked the specific rules set out in the Data Protection Directive 95/46.¹⁴¹

The case of *Jane Doe (D.L.) v M. Jackson*¹⁴² from U.S. Texas, provides a further pertinent example of privacy-invasion. The woman in question had shared intimate photos of herself with the defendant during their relationship. After a break-up in 2021, he was accused of having posted the photos on social media platforms and adult websites without her consent. The jury ordered Jackson to pay the claimant \$200 million for past and future mental anguish, and \$1 billion in exemplary damages. This American case provides an example of the judicial tendency in certain states to show a marked determination to protect rights to privacy and data protection.

But obviously court decisions cannot provide the detailed guidance to data controllers/processors and subjects that can be provided by a full data protection framework

¹⁴⁰ *Rechnungshof v Österreichischer Rundfunk* (2003) C-465/00, C138-/01, and C-139/01, ECLI:EU:C:2003:294.

¹⁴¹ European Parliament and Council Directive 95/46/EC 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 L281/23 (Directive 95/46 EC).

¹⁴² See *Jane Doe (D.L.) v M. Jackson*, 2022-20061/Court:113 on <https://www.scribd.com/document/664918883/Jane-Doe-D-L-v-M-Jackson>.

enshrined in legislation. In turning to the UK below, how did the Courts and lawmakers build the previous legal protection framework of private information and solve the potential issues? In doing so, it asks: what challenges did the pre-GDPR framework face, and to what extent did it provide meaningful safeguards for personal data? This chapter will now turn to more systematised methods of providing protection for private information previously in the UK, which is the legal framework of processing personal data prior to the GDPR.

3.2 Processing Personal Data Prior to the GDPR

In relation to the UK, the lawful basis for processing personal data prior to the GDPR should be accorded consideration in order to come to some conclusions as to the weight placed on providing data protection at that time and to provide context for discussion of the GDPR. Data protection ‘promotes the right to personality of individuals through informational self-determination and reduces the information and power asymmetries which can have a negative impact on individual autonomy’.¹⁴³ As individual control can be seen as a ‘reflection of fundamental values such as autonomy, privacy and human dignity’,¹⁴⁴ as previously discussed, research and practice agreed that data subjects should have some control over the use of their personal data.¹⁴⁵

In the context of the impact of high-tech in modern society, which was mentioned in chapter 1, the effective use of legal data protection frameworks in the UK prior to the UK GDPR and DPA 2018 needs to be considered, below. Prior to the GDPR, the legal basis for processing

¹⁴³ See Lyn E Pleger, Katharina Guirguis and Alexander Mertes, ‘Making Public Concerns Tangible: An Empirical Study of German and UK Citizens’ Perception of Data Protection and Data Security’ (2021) 122 *Computers in Human Behavior* 106830, section 2.1; see also Orla Lynskey (note 136) p 569.

¹⁴⁴ See van Ooijen I and Vrabec HU, ‘Does the GDPR Enhance Consumers’ Control over Personal Data? An Analysis from a Behavioural Perspective’ (2018) 42 *Journal of Consumer Policy* p 92.

¹⁴⁵ See *supra* chapter 2, section 2.2.

personal data in the UK relied primarily on the DPA 1998. This was the main data protection regulation before the GDPR came into force.

The rights to data protection are enshrined in Article 8 of the EU Charter,¹⁴⁶ which is complementary to the right to privacy as set out in Article 7 of the Charter. The inclusion of the right to data protection in the EU Charter distinguishes it from other major human rights documents, which tend to view data protection as a subset of the right to privacy.¹⁴⁷ The understanding of the role that data protection norms should play in society varies widely across EU member states.¹⁴⁸ The situation of the UK and Poland (and subsequently the Czech Republic) was slightly different from that of the other Member States.¹⁴⁹ These Member States signed Protocol No. 30 to the Treaty of Lisbon,¹⁵⁰ which clarified the effect of the EU Charter in the domestic legal system.

However, the exact effect of the EU Charter in the domestic system remained controversial.¹⁵¹ In the UK, data protection was viewed as a subset of the right to privacy; the courts have refused to accept the requirements of data protection in cases where the ECHR right to respect for privacy is not implicated.¹⁵² However, with one notable exception, the UK High Court¹⁵³ emphasised the distinction between the two rights in order to limit the justiciability of data

¹⁴⁶ European Union, Charter of Fundamental Rights of the European Union [2000] OJ C364/01 and [2010] OJ C83/389.

¹⁴⁷ Ibid, pp 4-5.

¹⁴⁸ Ibid. p 4.

¹⁴⁹ See Helen Fenwick, Gavin Phillipson and Alexander Williams, Text, Cases and Materials on Public Law and Human Rights (Routledge 2017), p 264, footnote 3.

¹⁵⁰ European Union, 'EUR-Lex - 12008E/PRO/30 - EN - EUR-Lex' (Europa.eu2025) <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12008E%2FPRO%2F30>>.

¹⁵¹ See Orla Lynskey (note 136) fn 25.

¹⁵² Ibid, p 5; see also *Durant v Financial Services Authority* [2003] EWCA Civ 1746, Auld LJ at para 28.

¹⁵³ In *R (on the application of AB) v Secretary of State for the Home Department* [2013] EWHC 3453, Mostyn J considered a claim based on the plaintiff's right to data protection. He pointed out that the right to the protection of personal data was not part of the ECHR and therefore had not been incorporated into domestic law by the Human Rights Act 1998 (para 16).

protection rights, aside from the DPA 1998.¹⁵⁴ In contrast, some jurisdictions in Europe have refused to systematically link the application of data protection rules to the right to privacy. In Germany, for example, the Constitutional Court has held that the right to data protection flows from an individual's 'right to informational self-determination'.¹⁵⁵

Moreover, as the EU Directive 95/46 was adopted at a time when the internet was in its infancy, the explosion of social networks and technologies raised important questions¹⁵⁶ about the compatibility of Article 3(2) of the Directive as it applies to the current Internet-world,¹⁵⁷ a point that will be discussed in the following sections. In light of the increasing influence of the ECHR and technological advancements, the following section will explore how the UK's data protection framework developed over time, leading to the establishment of the GDPR and DPA 2018. This historical context is crucial for understanding the role of data protection laws in modern society and the evolution of the legal protections for personal data.

3.2.1 Analysis of the previous data protection regime in the UK, with the influence of ECHR

After discussion of the lawful basis for processing personal data prior to the GDPR, it will be necessary to analyse the previous data protection regime in the UK, below. It could be divided into two specified periods: before Brexit and after the interim (bridging) regime for personal data protection.¹⁵⁸ The interim regime, it may be noted, was a transitional period during which

¹⁵⁴ See Orla Lynskey (note 136) p 5, fn 21.

¹⁵⁵ Ibid, p 5.

¹⁵⁶ For example, while it is true that the provisions in the Directive are intended to mediate between the right to freedom of expression and the right to privacy, it is not entirely clear that the premise of the scope of Article 3(2) can be adhered to in light of the shift that is taking place.

¹⁵⁷ See Rebecca Wong and Joseph Savirimuthu, 'All or Nothing: This Is the Question? The Application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet', (2007) John Marshall Journal of Computer and Information Law 2007/8, p 2.

¹⁵⁸ Anastasia Choromidou, 'EU Data Protection under the TCA: The UK Adequacy Decision and the Twin GDPRs' (2021) 11 International Data Privacy Law, p 390.

EU law continued to apply in the UK and ended on 31 December 2020. The Trade and Cooperation Agreement provides for an interim regime (so-called ‘bridging clause’, enshrined in Article FINPROV.10A of the TCA) that ensures the full continuity of data flows between the EEA and the UK, with no need for companies and public authorities to put in place any transfer tool under the GDPR or the Law Enforcement Directive (LED).¹⁵⁹

The law on the right to privacy developed in Europe since 1950. All member states of the Council of Europe (CoE) are also signatories to the 1950 ECHR. Article 8 of the ECHR provides for the right to respect for one’s ‘private and family life, home and correspondence’.¹⁶⁰ During the time before Brexit, the evolution of data protection in the UK dates back to the 1970s. Although legislative efforts by private members’ Bills in the 1960s were not successful, (for example, there had been attempts to introduce Bills aimed at strengthening the right to privacy, such as promoting the protection of personal data or introducing regulatory measures on surveillance, but they were ultimately not passed),¹⁶¹ notable milestones included the release of the Younger Report on Privacy¹⁶² in 1972 and the Lindop Report on Data Protection¹⁶³ in 1978.¹⁶⁴ Both reports investigated the privacy risks arising from the increased utilisation of computers for processing personal information. Sir Kenneth Younger played a crucial role in formulating the fundamental principles of Data Protection, setting a foundational standard that influences contemporary Data Protection legislation.

¹⁵⁹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent 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.

¹⁶⁰ See Article 8 of European Convention on Human Rights.

¹⁶¹ See Right of Privacy Bill [H.L.], HL Deb 13 March 1961 vol 229 cc607-61, <https://api.parliament.uk/historic-hansard/lords/1961/mar/13/right-of-privacy-bill-hl>.

¹⁶² See Report on <https://api.parliament.uk/historic-hansard/commons/1973/jul/13/privacy-younger-report>.

¹⁶³ Data Protection Committee: Evidence and Papers.

¹⁶⁴ Adam Warren and James Dearnley, ‘Data Protection Legislation in the United Kingdom’ (2005) 8 Information, Communication & Society 238, pp 240-241.

The momentum for the UK government to enact Data Protection laws gained traction with the release of two international legal frameworks on Data Protection during the early 1980s: the OECD Guidelines in 1980 and the Council of Europe Convention¹⁶⁵ in 1981. In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organisation for Economic Co-operation and Development (OECD)¹⁶⁶ issued its ‘Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data’.¹⁶⁷ The primary objective of the Council of Europe Convention in relation to protection for private information was to strike a balance between facilitating the transfer of personal data, freedom of expression, and safeguarding individual privacy at that time.¹⁶⁸ The drafting process was anchored in the ECHR, specifically drawing on Articles 8~10.

Nevertheless, the Council of Europe recognised the necessity for a dedicated Convention to address the challenges posed by computer processing, supplementing the overarching principles of the ECHR. The Member States of the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108)¹⁶⁹ to supplement Article 8 ECHR.¹⁷⁰ The Convention opened for signature on 28 January 1981 and was the first legally binding international instrument in the data protection field. The Convention 108 wielded significant influence, potentially enabling the

¹⁶⁵ Council of Europe Convention No. 108 on data protection Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981).

¹⁶⁶ OECD, ‘About the OECD’ (OECD2023) <<https://www.oecd.org/en.html>>.

¹⁶⁷ Guidelines on the Protection of Privacy and Transborder Flows of Personal Data The Organization for Economic Co-Operation and Development, last modified 5 January 1999.

¹⁶⁸ Kierkegaard S and others, ‘30 Years on – The Review of the Council of Europe Data Protection Convention 108’ (2011) 27 Computer Law & Security Review 223, p 230.

¹⁶⁹ Council of Europe, ‘Convention 108 and Protocols’ (Data Protection1981) <<https://www.coe.int/en/web/data-protection/convention108-and-protocol>>.

¹⁷⁰ Cécile de Terwangne, ‘Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data’ (2021) 40 Computer Law & Security Review 105497, section 1.

unrestricted flow of personal data among countries that had ratified the Convention.¹⁷¹

Under this Convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data. The legal responses adopted for the protection of individuals, at a time when there was no Internet, social networks, big data, or connected objects, proved insufficient in the web-connected world, where personal data has become coveted by all, and the need for protection became more pressing.¹⁷² For instance, the Convention was silent on the need for a legitimate basis for data processing to be admissible; for this purpose the Directive 95/46 made supplements to the data protection principles of Convention 108 in view of developments in technology and practices, which will be discussed later.¹⁷³ But Art 8 ECHR still had relevance; for example, in the case of *Drelon v France*,¹⁷⁴ the Court held that there had been a violation of Article 8 of the Convention on account of the collection and retention of personal information (which reflected the presumed sexual orientation of the applicant).¹⁷⁵ The court considered whether the interference in question served a legitimate purpose and had relied on appropriate, proportionate and strictly necessary means, while respecting the margin of appreciation enjoyed by States in applying the Convention. In general, the size of this margin of appreciation varies according to different parameters. In *Drelon*,¹⁷⁶ the emergence of a European and

¹⁷¹ See Council of Europe Convention 108 on data protection Art. 3 scope and Chapter III transborder data flows, Convention 108 aims to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001); see also Tobias Naef, 'Restrictions on Data Transfers and Trade Agreements' [2022] European Yearbook of International Economic Law 367, 1.1.2.2.

¹⁷² Ibid, see also in cases: *Malone v the United Kingdom* App. No(s). 8691/79, *Kruslin v France* App. No(s). 11801/85.

¹⁷³ See Cécile de Terwangne (note 170).

¹⁷⁴ Case 3153/16 and 27758/18, *Drelon v France* [2022] ECHR 278, legal summary in <https://hudoc.echr.coe.int/eng?i=002-13776> section V.

¹⁷⁵ Ibid, §§ 103-104.

¹⁷⁶ *Drelon v France* 3153/16 and 27758/18, [2022] ECHR 278.

international trend was accepted as affecting or even limiting this margin of appreciation, bearing in mind that the Court's case law in general has tended to defer to States when dealing with moral issues.¹⁷⁷

The Conservative administration in the UK, primarily concerned with the potential business impact of CETS 108 as administered by the Council of Europe, rather than a strong commitment to safeguarding personal privacy,¹⁷⁸ introduced a Data Protection Bill in 1982. Although the bill did not complete its parliamentary passage before the 1983 general election, it was reintroduced afterwards and became law in July of the same year, as the DPA 1984.¹⁷⁹ The 1984 Act embraced the overarching principles outlined in CETS 108, Art 8 ECHR and the OECD Guidelines,¹⁸⁰ constructing a regulatory framework around them. Central to the legislation was the establishment of a public register encompassing organisations in both the public and private sectors engaged in processing personal data.¹⁸¹ This register was overseen by an official known as the Data Protection Registrar, endowed with enforcement powers. The Act granted new rights to individuals, with key provisions, including the right to be informed if an organisation processed their personal data and the right to obtain a copy of such information (the right of subject access).

The impact of the 1984 Act was constrained in scope. It exclusively applied to computer-stored data, featured a cumbersome enforcement regime closely tied to the register, and did not formally acknowledge 'Data Protection' as a privacy concern. Nonetheless, the Registrar and

¹⁷⁷ *A.P., Garçon et Nicot v France*, App. No(s) 79885/12, 52471/13, 52596/13 §121.

¹⁷⁸ See Robert Walgate, 'Data Protection Laws: UK Lags Behind' (1981) 289 *Nature* 527, p 527.

¹⁷⁹ See Adam Warren and James Dearnley (note 164) p 242.

¹⁸⁰ In 1980, the OECD issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The Guidelines have two main purposes: to reflect privacy standards and to facilitate the free flow of information for law enforcement activities; see also details on, The 1980 OECD Privacy Guidelines, which were the first internationally-agreed privacy principles.

¹⁸¹ See Adam Warren and James Dearnley (note 164) p 249.

the Data Protection Tribunal, established by the Act, gradually developed a legal framework that significantly elevated standards for processing personal data. Notably, they interpreted the general principle of fairness to necessitate transparency from data users and a certain level of control for individuals.

In 1990, the European Commission, driven by the objective of a single market and alarmed by the varying Data Protection standards among EU member states (some lacking relevant legislation entirely), released a draft directive as part of six proposed measures.¹⁸² The negotiation process for the draft was protracted, resulting in numerous modifications before the Directive 95/46¹⁸³ was officially adopted in 1995. Throughout these negotiations, the UK Conservative government displayed hostility, contending that a directive was unnecessary. Consequently, the final text of the directive only minimally reflects the UK influence.¹⁸⁴ The directive, on the whole, established relatively high standards for Data Protection. One of its objectives was to ensure no reduction in the level of protection already afforded by existing national laws. It explicitly established the connection between data protection and personal privacy.

However, it represented a somewhat uneasy combination of broad general principles and detailed prescriptive measures, with many reflecting the specific interests of individual member

¹⁸² Karl Löfgren and C William R Webster, 'Policy Innovation, Convergence and Divergence: Considering the Policy Transfer Regulating Privacy and Data Protection in Three European Countries' (2010) 14 Information Polity 295, pp 301-302.

¹⁸³ 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 Official Journal L 281, 23/11/1995 P. 0031 - 0050, see details on <http://data.europa.eu/eli/dir/1995/45/oj>.

¹⁸⁴ Karl Löfgren and C William R Webster, 'Policy Innovation, Convergence and Divergence: Considering the Policy Transfer Regulating Privacy and Data Protection in Three European Countries' (2010) 14 Information Polity 295, p 303.

states.¹⁸⁵ Formally approved by the European Council in October 1995 (Directive 95/46/EC), the UK chose to abstain from the vote. Member states were granted three years from that date to incorporate the directive into their domestic laws.¹⁸⁶ A pivotal consideration was whether the Directive should be implemented through primary or secondary legislation. Respondents to the consultation, including the Data Protection Registrar, overwhelmingly favoured primary legislation.¹⁸⁷ Their preference stemmed from the desire for a unified Data Protection framework and to avoid the complexities of a dual regime that would arise if the existing Data Protection Act 1984 were not repealed. However, it remains uncertain whether the government was fully convinced.¹⁸⁸

The change in government in 1997 ushered in a new approach. In July 1997, the incoming Labour government released a White Paper emphasising the adoption of primary legislation and positioning Data Protection as a priority within the human rights agenda. Subsequently, in January 1998, the Data Protection Bill was introduced in the House of Lords. Lord Williams of Mostyn stated, ‘Data Protection shares common ground to that extent with the Human Rights Bill.’ The Data Protection Bill also concerned privacy, albeit a specific form of privacy: personal information privacy. The subject matter of the Bill was, therefore, inherently important to general social welfare.’¹⁸⁹

The Data Protection Bill received Royal Assent on July 16, 1998, becoming the DPA 1998. The

¹⁸⁵ Peter Hustinx, ‘EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation’ [2017] Oxford Scholarship Online, pp 9, 11; see also Tobias Naef, ‘Restrictions on Data Transfers and Trade Agreements’ [2022] European Yearbook of International Economic Law 367, 1.1.3.3.

¹⁸⁶ Directive 95/46/EC, Article 32.

¹⁸⁷ Adam Warren and James Dearnley, ‘Data Protection Legislation in the United Kingdom’ (2005) 8 Information, Communication & Society pp 254-255.

¹⁸⁸ Ibid, p 257, which reference to Charles D Raab, ‘Implementing data protection in Britain’, International Review of Administrative Sciences, (1996) vol. 62, no. 4, pp 493–511. Raab argues that at the time of enactment, the Registrar had virtually no allies to support in enforcing privacy of individuals.

¹⁸⁹ Colum 436, <https://publications.parliament.uk/pa/ld199798/ldhansrd/vo980202/text/80202-04.html>.

Act faithfully incorporated the provisions of the Directive 95/46 into UK law but fell short of resolving practical challenges arising from some of the Directive's more incongruous aspects. In limiting the definition of the scope of 'personal data',¹⁹⁰ the judgment of the Court of Appeal in *Durant*¹⁹¹ is difficult to reconcile with *Lindqvist*¹⁹² judgment (in particular in relation to Article 8 of the Directive). In that case, the ECJ interpreted Article 8 broadly: a mere reference to part of another person's body (feet) would be sufficient to constitute 'processing' of personal data and also invited criticism that data protection in the UK is weak compared to the data protection laws of other Member States¹⁹³ implementing the Directive 95/46/EC.¹⁹⁴ The *Durant* judgment significantly narrowed the scope of 'personal data' under the DPA 1998; the Court of Appeal held that data qualifies only if it is 'focused on a particular individual'¹⁹⁵ and carries 'biographical significance.'¹⁹⁶ As a result, many records mentioning Mr. Durant's name were excluded from protection, since they primarily concerned his bank's conduct rather than his biographical details.¹⁹⁷

The DPA 1998 provided a legal framework for the protection of personal data in the UK. It established principles for the fair and lawful processing of personal information. The framework outlined certain rights for individuals, including the right to access personal data held by organisations and the right to request corrections. The DPA 1998 assigned

¹⁹⁰ When processing personal information, the Court of Appeal has favoured considering the exemptions set out in the UK's DPA 1998 (e.g. special purposes (processing for journalistic, artistic and literary purposes) or the provisions of ss. 27-29 of the Personal Information Protection Act), rather than ruling directly on whether the data is 'personal' information.

¹⁹¹ *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

¹⁹² *Bodil Lindqvist* C-101/01 [2004] 1 CMLR 20.

¹⁹³ See, for example, the decisions of the Supreme Court of Iceland in *Ragnhildur Guðmundsdóttir v The State of Iceland* 151/2003 (also available at http://www.epic.org/privacy/genetic/iceland_decision.pdf) and see also Renate Gertz, 'An Analysis of the Icelandic Supreme Court Judgment on the Health Sector Database Act', (2004) 1:2 SCRIPT-ed 241, @: <<http://www.law.ed.ac.uk/ahrc/script-ed/issue2/iceland.asp>>.

¹⁹⁴ See Rebecca Wong and Joseph Savirimuthu (note 157) p 13.

¹⁹⁵ [2003] EWCA Civ 1746, §§ 28, 34.

¹⁹⁶ *Ibid*, § 28.

¹⁹⁷ *Ibid*.

responsibilities to data controllers, requiring them to process personal data in accordance with the law and to implement measures to protect data. The following were some of the legal grounds under the DPA 1998 for lawful data processing:¹⁹⁸

1. *Consent: The processing of personal data is usually based on the consent of the data subject. Consent should be explicit, voluntary, specific and revocable. The data controller needs to obtain the consent of the data subject, clearly stating the purpose of the data processing, and can only process the data within the scope of the consent.*
2. *Contractual Necessity: If the processing of personal data is done in order to fulfil a contract with the data subject, then this is considered legal data processing. For example, when purchasing goods or services, a merchant may need to process some personal data to fulfil the transaction.*
3. *Legal Obligation: The data controller may be required by law to process personal data. In this case, the data processing is considered to be due to a legal obligation and is therefore legal.*
4. *Protection of Vital Interests: When personal data is processed to protect the life of the data subject or another person, this is considered legitimate data processing.*
5. *Public Task or Exercise of Official Authority: Data processing is also considered lawful if it is done for the purpose of a public task or exercise of public authority.*

¹⁹⁸ Schedule 2 of the DPA 1998, Conditions relevant for purposes of the first principle: processing of any personal data.

6. *Legitimate Interests: The data controller may process personal data in accordance with its own legitimate interests or those of third parties, provided that this does not infringe the rights and interests of the data subject.*

These legal grounds still exist in the Art 6 of the GDPR, but the GDPR takes a stricter stance on consent and introduces more provisions on transparency, and data subject rights, as discussed in the next chapter. The DPA 1998 officially came into effect in March 2000. Transitional arrangements restricted its impact on existing processing until October 2001. Similar to the ‘interim regime’ following the end of the Brexit transition period, in January 2021, the personal data protection regime became subject to the agreement between the parties in the Trade and Cooperation Agreement (TCA).¹⁹⁹ The ‘interim regime’ solution applies for a maximum of six months, provided that the UK commits not to change the current data protection regime. Essentially, this meant that the UK must continue to apply the EU law-based data protection rules that operated during the transition period, as discussed previously.²⁰⁰

This section will then analyse the way that the previous Act actually operated in practice, including the relationships or conflicts between data protection and freedom of expression. From the view of Erdos²⁰¹ in his book, the practice in the previous data protection framework could be analysed from the perspective of *Von Hannover (No.1)*.²⁰² The ECtHR found that

¹⁹⁹ The EU-UK Trade and Cooperation Agreement, see also Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent 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.

²⁰⁰ See Brexit, Statement and Information from the UK Data Protection Authority - 29 January 2020.

²⁰¹ See David Erdos, ‘The Development of European Data Protection Law and Regulation’ in David Erdos (ed), *European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope?* (Oxford University Press 2019).

²⁰² *Von Hannover v Germany* [2005] 7 WLUK 866.

Article 8 ECHR obliges Member States to take ‘measures aimed at ensuring respect for private life, even in the sphere of relations between individuals’, which also includes ensuring an appropriate balance between private life and the exercise of freedom of expression by the professional press.²⁰³ In that regard, the Court further considered that ‘the decisive factor in striking a balance between the protection of private life and freedom of expression’ lay in assessing the contribution of any publication to ‘a debate of general interest’.²⁰⁴

The fact that the photographs of Princess Caroline of Monaco had been taken in public but in connection with her private activities, meant that the Court found that no such contribution had been made.²⁰⁵ There had therefore been a violation of the Convention. Although this decision does not directly concern data protection, the Court emphasised that ‘heightened vigilance with regard to the protection of private life’ was considered necessary, one of the key reasons being that ‘new communication technologies make it possible to store and reproduce personal data’.²⁰⁶ Moreover, an obvious (and, arguably, necessary under data protection) way for states to fulfil their newly articulated European Convention responsibilities was through the data protection framework (although not the only means). Thus, *Von Hannover*²⁰⁷ has had a powerful impact on data protection and, in particular, on the interaction between data protection and freedom of expression.²⁰⁸

Rebecca Wong and Joseph Savirimuthu,²⁰⁹ in their article, took the *Lindqvist*²¹⁰ case as an

²⁰³ Ibid, § 57.

²⁰⁴ See David Erdos (note 201) pp 43-44.

²⁰⁵ [2005] 7 WLUK 866, § 76.

²⁰⁶ Ibid, § 70.

²⁰⁷ [2005] 7 WLUK 866.

²⁰⁸ David Erdos (note 201) pp 43-44.

²⁰⁹ See Rebecca Wong and Joseph Savirimuthu (note 157) p 6.

²¹⁰ C-101/01, L uploaded the content of a web page containing details of members of a parish church. The website also contained information about a member who had suffered a foot injury. L did not seek the consent of the person concerned before posting the information on the website. L also failed to notify the Swedish Data

example to evaluate the ECJ and the Directive as a legal framework in the new social spaces for processing and disseminating information. They mainly used Art 3(2)²¹¹ of the Directive to cogitate that it is not enough for an individual to rely on the defence of reasonableness, or on the ‘*de minimis*’ rule as to what constitutes personal data, or whether the processing is wholly or partly the product of an automated process.²¹² Another observation that they made about the approach of the ECJ is that any future attempts by individuals to treat their right to expression as an absolute right will not be permitted.²¹³ Conversely, at the policy level, the approach taken by the ECJ demonstrates that the public interest in protecting privacy should not be ignored in the new era of high-technology.

With regard to the discussion of blogs and webpages, there have been relatively few cases of individuals being prosecuted under the DPA 1998 in the UK for publishing personal information about others on their web pages (whether or not they are accessible to the public via the Internet).²¹⁴ The mere mention of an individual on a web page is not sufficient to constitute ‘personal data’²¹⁵ under the UK DPA 1998. The decisive factor is whether the privacy of the individual has been compromised, and it must be balanced against other factors, such as in particular freedom of expression under Article 10 ECHR.²¹⁶ In an indication that the ECHR also has relevance in the data protection sphere, in a significant case at around the same time

Inspection Board of the publication of sensitive information about the health of members of the parish on the website.

²¹¹ Article 3(2) of the Directive provides that the Directive is deemed not to apply in two circumstances. Firstly, the processing of personal data carried out as part of an activity outside Community law is excluded from the Directive. Secondly, the Directive is also deemed not to apply if the processing of personal data is carried out by a natural person in the course of a purely personal or family activity.

²¹² Rebecca Wong and Joseph Savirimuthu (note 157) p 6.

²¹³ Ibid.

²¹⁴ Ibid, p 11.

²¹⁵ Personal data is defined under s 1 of the DPA. However, the definition of ‘personal data’ has been narrowly restricted in the Court of Appeal’s decision, *Durant v FSA* [2003] EWCA Civ 1746.

²¹⁶ See Rebecca Wong and Joseph Savirimuthu (note 157) p 11.

in 2018 regarding Articles 8 and 10 of the ECHR, *M.L. and W.W. v Germany*,²¹⁷ the German Federal Court of Justice (‘the German Federal Court’) held that the individuals were not entitled to remain anonymous as this violated the public’s right to know about matters of public interest. While the German district and appeal courts upheld the applicant’s request, the German Federal Court rejected the applicant’s request on the grounds that the greater public interest in knowing about past and present offenders outweighed the plaintiff’s request.²¹⁸

The judgment of the ECtHR was based on similar reasoning to that of the German Federal Court; it considered the balance of interests and found no violation of Article 8 of the Convention. It ruled that the public’s right to free access to information prevailed over the right to privacy of the two German applicants, who had sought to anonymise personal information contained in archived media reports relating to their criminal convictions. The Court discussed the role of the media in the dissemination of information and the maintenance of archives, which are clearly a source of research in the field of contemporary history. It also held that articles containing statements of fact relating to the conduct of a criminal trial could not be considered to have misrepresented the applicants.²¹⁹

The Court upheld the decision of the German Federal Court on the basis that there was a continuing public interest in events that had occurred in the past and concluded that the denial of anonymous media coverage did not violate the individual’s right to privacy.²²⁰ However, as stated in the judgment, in relation to Article 8, an attack on a person’s reputation must reach a certain level of seriousness and undermine the individual’s right to respect for private life to

²¹⁷ *M.L. and W.W. v Germany* (2018) Apps. 60798/10 and 65599/10, ECLI: CE: ECHR:2018:0628JUD006079810.

²¹⁸ *Ibid*, section C, §§ 21-23.

²¹⁹ *Ibid*, § 106.

²²⁰ *Ibid*, § 116.

fall within the ambit of the Article. In addition, Article 8 cannot be relied upon to complain about reputational damage of foreseeable consequence resulting from an individual's conduct (e.g. the commission of a criminal offence).²²¹

After the analysis above of the previous data protection regime in the UK, under the ECHR and EU, the DPA 1998 can be criticised on the following grounds in terms of weaknesses. Prior to the implementation of comprehensive data protection legislation such as the DPA 1984 and later the DPA 1998, the legal provisions for data protection were often fragmented and lacked the comprehensive protection found in modern data protection regimes. For instance, with regard to consent policy, data collection does not necessarily need an opt-in and fails to make clear privacy notices so that individuals can make an informed decision on whether they consent to allow their data to be stored and used.²²²

Likewise, the DPA 1998 was unable to provide individuals with more substantial rights, e.g. 'the right to be forgotten' in the GDPR,²²³ and often conflated data protection with broader privacy issues, thereby muddling the conceptual clarity necessary for effective enforcement. These deficiencies, along with enforcement challenges and an inadequate definition of 'personal data,' underscore why the previous regime was ultimately deemed ineffective and required the more rigorous reforms embodied in the GDPR.

3.2.2 Impact of the previous data protection regime on individuals

²²¹ Ibid, § 88.

²²² See Changes to the Data Protection Directive 95/46/EC – 2010. The document contains comments on how to improve the Data Protection Act 1998 and provides several references as to how the legislation can be improved without waiting for agreement on a revised form of Directive 95/46/EC, see also on <https://amberhawk.typepad.com/amberhawk/2010/11/shortfalls-in-the-data-protection-act-1998-identified-1.html>.

²²³ Judith Townend, 'Data Protection and the 'Right to Be Forgotten' in Practice: A UK Perspective' (2017) 45 International Journal of Legal Information, p 31.

Whilst an EU member, the UK, as discussed above, was required to implement the data protection framework of EU.²²⁴ Below the impact of the previous data protection regime on individuals is considered; it will be followed by a consideration of how citizens perceive the ‘real world’ environment in which data processing takes place.²²⁵ Scholars agree that data protection and data security are of great importance to individuals.²²⁶ Previous research finds that data protection focuses on personal data in the sense of informational self-determination and its relationship to legal regulations.²²⁷

One of the earliest judicial interpretations of the Data Protection Directive emerged in *Rundfunk*,²²⁸ a case from the earlier phase of European data protection jurisprudence. The CJEU declared the application admissible, noting that Austrian legislation safeguarded the editorial independence and autonomy of the Österreichischer Rundfunk (ORF), thereby classifying it as a non-governmental organisation. Significantly, *Rundfunk* treated data protection and privacy as interchangeable concepts, thereby reinforcing the view that the right to data protection is a subset of the broader right to privacy. This conflation, while conceptually convenient at the time, also reflected the doctrinal underdevelopment of data protection as an autonomous legal right, positioning it as an extension of privacy rather than recognising its distinct normative and functional dimensions, a stance that subsequent legal developments would increasingly challenge.

²²⁴ David Erdos (note 15) section 1, p 4.

²²⁵ Dara Hallinan, Michael Friedewald and Paul McCarthy, ‘Citizens’ Perceptions of Data Protection and Privacy in Europe’ (2012) 28 Computer Law & Security Review p 263.

²²⁶ Lyn E Pleger, Katharina Guirguis and Alexander Mertes (note 143) p 2; see also Dara Hallinan, Michael Friedewald and Paul McCarthy (note 225) pp 263-272; Joinson AN and others, ‘Watching Me, Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom’ (2006) 32 Journal of Information Science pp 334-343.

²²⁷ Ibid, Lyn E Pleger, Katharina Guirguis and Alexander Mertes (note 143) p 2; see also Orla Lynskey, ‘Deconstructing Data Protection: The ‘Added-Value’ of the Right to Data Protection in the EU Legal Order’ (2014) 63 International and Comparative Law Quarterly p 569.

²²⁸ C-465/00, C138-/01, and C-139/01, ECLI:EU:C:2003:294.

Culture plays a crucial role in the behaviour of individuals in relation to their use of the Internet and their concern for their privacy.²²⁹ Cultural values can be understood as ‘underlying mechanisms’ impacting citizens’ judgments of what is of personal importance and ultimately their social behaviour,²³⁰ and thus how citizens deal with data privacy. Empirical findings regarding the influence of culture on privacy concerns support the effect of culture on privacy attitudes to some extent. Bellman et al.²³¹ investigated the influence of cultural values on individuals’ concerns about different dimensions of privacy. Although they found some impact of cultural values on specific aspects of privacy concerns, they could not identify an overall impact.²³²

Custers et al.²³³ found that only 15% of EU citizens feel in full control of their personal data. In an international comparison of different countries, they found that German citizens were below this average, while UK citizens were above average and therefore perceived to have more control over their own data. Perceived control over one’s own data is closely linked to data privacy issues.²³⁴ It could also be seen from a survey in 2010 conducted by Hallinan,²³⁵ in the UK, on behalf of the Joseph Rowntree Foundation²³⁶ that 65% of people were concerned that the Government held their data, up from 53% in a 2006 study²³⁷ asking the same question.

²²⁹ Lyn E Pleger, Katharina Guirguis and Alexander Mertes (note 143) p 4.

²³⁰ Lindsay H Hoffman and Michael D Slater, ‘Evaluating Public Discourse in Newspaper Opinion Articles: Values-Framing and Integrative Complexity in Substance and Health Policy Issues’ (2007) 84 *Journalism & Mass Communication Quarterly* 58, p 59.

²³¹ Steven Bellman and others, ‘International Differences in Information Privacy Concerns: A Global Survey of Consumers’ (2004) 20 *The Information Society* p 313.

²³² Lyn E Pleger, Katharina Guirguis and Alexander Mertes (note 143) p 4 cultural background.

²³³ See Bart Custers and others, ‘A Comparison of Data Protection Legislation and Policies across the EU’ (2018) 34 *Computer Law & Security Review* p 238.

²³⁴ Lyn E Pleger, Katharina Guirguis and Alexander Mertes (note 143) p 3.

²³⁵ Dara Hallinan, Michael Friedewald and Paul McCarthy, ‘Citizens’ Perceptions of Data Protection and Privacy in Europe’ (2012) 28 *Computer Law & Security Review* p 267.

²³⁶ ICM, ‘State of the Nation Survey 2010’, Joseph Rowntree Foundation, York, 2010.

²³⁷ Backhouse, James, and Ruth Halperin, ‘A Survey on EU Citizen’s Trust in ID Systems and Authorities’, FIDIS Deliverable 4.4, London School of Economics and Political Science, London, 2007.
<http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.4.survey.pdf>.

In addition, Hallinan et al conducted survey²³⁸ found that the public tend to show concern about commercial collection and use of data. They looked at this issue from the perspective of personal impact; they found that people are concerned and annoyed by the end result of data dissemination, i.e. direct mail, spam etc. Relatedly, it was found that the public expressed concern about certain data behaviours associated with this fear (but also of wider significance), fearing that information would be ‘used without their knowledge’, ‘shared with third parties without consent’ and that ‘information would be used in a different context to that in which it was disclosed’.²³⁹

3.2.3 Assessment of the strengths and weaknesses of the previous data protection framework

After discussion of the impact of previous data protection regime on individuals, it is necessary to evaluate the strengths and weakness of the previous data protection framework in order to provide context for the discussion of the GDPR in Chapter 4. The DPA 1998 had to be applied consistently with the ECHR under the HRA. Thus, the exceptions under Arts. 8 and 10(2) are relevant. *Dudgeon*²⁴⁰ clarified that any interference must be ‘necessary in a democratic society’, a condition which does not have the flexibility of such expressions as ‘useful’, ‘reasonable’, or ‘desirable’, but implied the existence of a ‘pressing social need’ for the interference in question.²⁴¹ While it is for the national authorities to make the initial assessment of the pressing social need in each case, ‘their decision remains subject to review by the Court’.²⁴² These points will be returned to in chapter 3 in relation to the GDPR. In order to make an assessment of the

²³⁸ See Dara Hallinan, Michael Friedewald and Paul McCarthy (note 225) p 263.

²³⁹ Ibid, p 268; see also Special Eurobarometer 359, 2011.

²⁴⁰ *Dudgeon v The United Kingdom* (1981) App. No. 7525/76.

²⁴¹ Ibid, § 51.

²⁴² Ibid, § 52.

previous data protection framework, all relevant data protection laws will also need consideration.

In terms of creating an interference with Arts 8 and 10, which data protection potentially does, it must be possible to assess it from four aspects, which are: 1) Existence of an interference; 2) Whether the interference was prescribed by law; 3) Whether the interference pursued a legitimate aim; 4) Whether it was necessary and proportionate to the aim pursued. The following section will use the cases *Google Inc v Vidal-Hall & Ors*²⁴³ etc. to test these aspects. The previous and current framework was also related to human rights law, as discussed above, and in particular with trying to reconcile two fundamental rights: privacy and freedom of expression. The discussion below looks at data protection in relation to its interaction with Arts. 8 and 10, in terms of the tests under Art. 10(2).

In a number of cases, Strasbourg has found a violation of Article 8 solely on the grounds of a lack of legal basis at national level to authorise measures capable of interfering with the relevant rights.²⁴⁴ Under the previous data protection framework of the UK, there were frequent interferences with individuals' right to privacy through the collection, processing and dissemination of personal data by public and private sector entities. These interferences manifested themselves in a variety of ways, including via government surveillance programmes, and via data sharing between organisations and commercial data processing activities. However, obviously the interferences could potentially be justified under the DPA 1998 and Art. 8 ECHR.

²⁴³ *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311.

²⁴⁴ See Guide to the Case-Law of the of the ECtHR, p 24; see also *Taylor-Sabori v the United Kingdom* (2002) App no. 47114/99, §§17-19; *Radu v Moldova* (2014) App no. 50073/07, § 31.

In *Townsend v Google Inc. and Google UK Limited*,²⁴⁵ the Court emphasised that the purpose of the DPD and the DPA 1998 is to safeguard the right to privacy in the context of data management.²⁴⁶ In *Google Inc v Vidal-Hall & Ors*,²⁴⁷ for the purposes of data protection rights, the Court of Appeal held that compensation could be awarded even in the absence of pecuniary loss. In order to achieve this result, the Court, in a bold move, *disapplied* the relevant provisions of the DPA 1998 in order to resolve what the Court considered to be a legal incompatibility between the UK and EU law, thereby give full application to EU law.²⁴⁸

After identifying an interference, it must be asked under Art. 10(2) whether the interference is regulated by law. In many cases, interferences with an individual's right to privacy are prescribed by law, either explicitly through legislation on data protection, or implicitly through the broader legal framework governing activities such as law enforcement, national security, or commercial transactions. *Handyside v the United Kingdom*²⁴⁹ provided a basic test for freedom of expression, which is subject to Art 10(2), taking account of the definition of 'formality', 'condition', 'restriction' or 'penalty' within 'democratic society'.²⁵⁰

In *S. and Marper v the United Kingdom*,²⁵¹ with regard to personal data collected and stored in databases by the authorities for the purpose of preventing or punishing offences, the Court stated that it was important to establish clear and detailed rules regulating the scope and application of such measures, together with minimum safeguards, in particular with regard to duration, storage, use, access by third parties, procedures for maintaining the integrity and

²⁴⁵ [2017] NIQB 81.

²⁴⁶ Ibid, see §§36-38.

²⁴⁷ *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311.

²⁴⁸ Ibid, §§ 76,77.

²⁴⁹ *Handyside v the United Kingdom* (1976) App. No(s). 5493/72.

²⁵⁰ Ibid, § 49.

²⁵¹ *S. and Marper v the United Kingdom* [GC] 2008, App. No(s). 30562/04, 30566/04.

confidentiality of the data, and procedures for destroying the data, so as to provide sufficient guarantees against the risk of misuse and arbitrariness.²⁵² The Court found a violation of Article 8 if the domestic law was not sufficiently clear as to the scope and manner of exercise of the discretionary powers conferred on the domestic authorities in *Dimitrov-Kazakov v Bulgaria*.²⁵³

It must be considered whether the interference is for a legitimate purpose. Interference with an individual's right to privacy is often motivated by a legitimate purpose, such as to preserve national security, public safety, law enforcement, or the facilitation of commercial transactions. In some cases, the ECtHR has examined whether the requirement, as also stated in Article 5 of Convention 108, that the personal data undergoing automatic processing must have been collected for explicit, specific and legitimate purposes, has or has not been met.²⁵⁴ For example, the Court held in *Leander v Sweden*²⁵⁵ that the storage of data relating to the private lives of individuals in secret police registers, and their subsequent use in vetting candidates for posts of national security importance, served a legitimate purpose of Article 8(2), namely the protection of national security.²⁵⁶

Finally, it must be considered whether an interference under Arts 8 or 10 was necessary and proportionate to the aim pursued. The necessity of interfering with an individual's right to privacy varies depending on the specific context and purpose of the data processing activity. In some cases, such as national security or law enforcement investigations, the collection and processing of personal data may be considered necessary to fulfil a legitimate purpose, including to further free expression of provision of personal information.

²⁵² Ibid, §§ 99, 103.

²⁵³ *Dimitrov-Kazakov v Bulgaria*, 2011, App. No(s). 11379/03, § 33.

²⁵⁴ Article 5 of Convention 108.

²⁵⁵ *Leander v Sweden*, 1987 App. No(s). 9248/81.

²⁵⁶ Ibid, § 49.

However, in other cases, such as relying on commercial data processing for marketing purposes, the need for intervention may be more questionable, especially if the intervention results in a disproportionate invasion of an individual's privacy. In *Axel Springer AG v Germany*,²⁵⁷ the court held that the fact that X had previously disclosed details of his private life in the media meant that he could not expect the same level of protection of his privacy, by citing Princess Caroline's argument that she had never sought to publicise details of her private life in *Von Hannover (No. 2)*.²⁵⁸ Where *Von Hannover (No. 2)* established that even public figures retain a meaningful privacy sphere in respect of information they have not voluntarily placed in the public domain, *Axel Springer* refined this by making the claimant's own prior conduct a material factor in calibrating the weight to be accorded to Article 8. The practical effect is a sliding scale of privacy entitlement in which voluntary prior disclosure operates as a form of partial waiver, not absolute, but sufficient to tip the balance in favour of Article 10 where the subsequent publication relates to matters the claimant has themselves made a subject of public narrative.

Through survey and social research as above, academics and others have voiced concerns about the previous data protection in the UK, which included the matter of compensation in relation to protecting private information.²⁵⁹ The judges have found that compensation does not provide an adequate remedy for the misuse of private information. Post facto monetary compensation clearly fails to address the harm caused by the form of misuse of personal information at issue.²⁶⁰ Punitive damages were not available in *Moseley*,²⁶¹ and Eady J. acknowledged that

²⁵⁷ *Axel Springer AG v Germany* (2012) App. No. 39954/08.

²⁵⁸ *Von Hannover (No 2)* (2012) 55 E.H.R.R. 15.

²⁵⁹ See Helen Fenwick, Reflections on balancing Articles 8 and 10 in the context of MPI - past, present and future. (2024) *Journal of Communications and Law*, 29(4), pp 153-157.

²⁶⁰ Fiona Brimblecombe and Helen Fenwick (note 11) p 27.

²⁶¹ *Mosley v News Group Newspapers Ltd* [2008] E.M.L.R 20.

they still failed to compensate for the invasion of privacy in comparison to reputational damage.²⁶²

3.3 Conclusion

To sum up, there were disadvantages in the previous data protection regime in the UK. The ICO served as the regulatory body overseeing data protection in the UK (as it does now). It had the authority to investigate breaches and enforce compliance.²⁶³ However, in the face of technological advances and evolving data protection challenges, the DPA 1998 came to be considered outdated.²⁶⁴ The digital landscape has changed dramatically since the Act was enacted. Penalties for non-compliance were relatively light compared to those now available under the GDPR. For example, under the DPA 1998, fines for breach of its eight data protection principles could be imposed, with a maximum £500,000. A key condition was that the personal data breach must have caused harm or financial loss to the Data Subject. The Supervisory Authority now has new powers to impose fines on data controllers and processors for failing to observe the principles of the GDPR and the Supervisory Authority simply needs to show that administrative procedures have not been adhered to in order to punish the organisation.²⁶⁵

The lack of large fines may not have provided a sufficient deterrent for controllers and processors to prioritise data protection. The framework did not give individuals as much control over their personal data as did the later GDPR, discussed in Chapter 4. Consent requirements were less stringent; individuals had less voice in how their data was used. Under the DPA 1998, marketers rely on a negative ‘opt-in’ when obtaining consent (e.g. tick here if you do not wish

²⁶² Ibid, § 231.

²⁶³ Part I, Section 6 of the Data Protection Act 1998.

²⁶⁴ Fiona Brimblecombe and Helen Fenwick (note 11) p 27.

²⁶⁵ Article 51 of the UK GDPR.

to receive offers).²⁶⁶ Under the previous regime, the data subject had the right to request a copy of their data (Subject Access Request) on payment of a nominal fee. But under the GDPR, these rights are explicit and no longer require a fee.²⁶⁷ The previous framework also had limitations in dealing with data processing activities carried out by entities outside the UK.²⁶⁸ To give an example, the DPA 1998 does recognise that the processing of personal data constitutes an interference with an individual's right to privacy. However, the scope of application of the Act is limited to data processing activities within the UK, or by entities that have an organisation in the UK. As a result, it may not adequately address data processing activities carried out by entities outside the UK, which subsequently may not be subject to the UK jurisdiction.²⁶⁹

The cases discussed, such as *Google Inc v Vidal-Hall & Ors* and *S. and Marper v the United Kingdom*, highlight the challenges faced in reconciling privacy rights with the need for data processing in a modern society. The legal framework struggled to provide a sufficient remedy for breaches of privacy, and its reliance on the discretion of national authorities often led to ambiguities in application. Moreover, the perceived lack of control over personal data among UK citizens, as reflected in various surveys, indicates a broader societal concern about the adequacy of protections under the DPA 1998.

The interaction between privacy rights and freedom of expression further complicated the picture, with cases like *Axel Springer AG v Germany* showing the delicate balance that courts had to strike. While the DPA 1998 provided a foundation for data protection, it did not go far enough in addressing the evolving challenges of data processing and privacy in the digital era.

²⁶⁶ See ICO, Consent-Lawful basis for processing, 22 March 2018.

²⁶⁷ Ibid.

²⁶⁸ Francesca Mazzi and others (note 14) chapter 3.

²⁶⁹ See Judith Townend, 'Data Protection and the 'Right to Be Forgotten' in Practice: A UK Perspective' (2017) 45 International Journal of Legal Information pp 29-30.

With the increasing globalisation of data processing, there was a need for a more comprehensive extraterritorial approach. Enforcement of data protection rules was sometimes inconsistent and penalties for breaches were not always commensurate with the severity of the breach. For example, in 2011, Sony PlayStation Network suffered a massive data breach that compromised the personal information of millions of users, including names, addresses, email addresses and credit card details.

Sony was criticised for its handling of the breach and required to take steps to improve its data security practices.²⁷⁰ The ICO fined Sony £250,000 in 2013 for security failings related to the incident.²⁷¹ However, the framework did not emphasise accountability and transparency as much as the GDPR now does, as the discussion in Chapter 4 below. This regime also placed less emphasis on organisations demonstrating compliance and providing clear, accessible information to individuals about their data processing practices. Therefore, the question now arises: how does the current data protection model in the UK regulate high-tech invasions of privacy? The next chapter will further explore the key features of the current data protection model in the UK, taking account of its origins as discussed here.

²⁷⁰ Mark Prinsley and Oliver Yaros, 'UK ICO Imposes a £250,000 Penalty for a Security Breach Which Exposed the Personal Data of Millions of Consumers' (2013) <<https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2013/01/uk-ico-imposes-a-250000-penalty-for-a-security-bre/files/130129-ip-sony/fileattachment/130129-ip-sony.pdf>> accessed 16 September 2025.

²⁷¹ Ibid.

CHAPTER 4 KEY FEATURES OF THE CURRENT DATA PROTECTION MODEL IN THE UNITED KINGDOM

4.1 Introduction

Over the past two decades, studies have provided important information on data protection online in the UK.²⁷² Prior to Brexit, the UK was a member state of the European Union and was subject to its laws. The UK has a similar history of protecting personal information and freedom of expression as had the EU.²⁷³ Due to the Directive²⁷⁴ prior to the GDPR which influenced the previous DPA in the UK. It will be fair to say that the UK and EU developed the framework of protecting personal information online synchronously since the UK was responding to EU provisions. Based on the similar legal structure in the field of privacy law, although there existed some different definitions of privacy and personal information etc legitimately, the regulations of personal data were in common to some extent before Brexit.²⁷⁵ Obviously, the previous data protection Directive was designed to seek to ensure that member states developed data protection legislation in accordance with a common data protection policy.

Although now embedded as domestic law, the UK GDPR is not an original creation of the UK

²⁷² For example, the research archive on UCL's website <https://www.ucl.ac.uk/constitution-unit/research/research-archive/foi-archive/what-freedom-information-data-protection> provides the historical development of Freedom of information and Data Protection; also the research work of various companies and corporate entities like Deloitte etc., which discussed on <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf>.

²⁷³ See Adam D Moore, 'Free Speech, Privacy, and Autonomy' (2020) 37 Social Philosophy and Policy 31, Available at: <https://doi.org/10.1017/s0265052521000030>, page 39-40.

²⁷⁴ 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 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>.

²⁷⁵ See David Erdos, 'The UK and the EU Personal Data Framework after Brexit: A New Trade and Cooperation Partnership Grounded in Council of Europe Convention 108+?' (2022) 44 Computer Law & Security Review 105639, chapter 3, available at <https://doi.org/10.1016/j.clsr.2021.105639>.

Parliament but the ‘on-shored’ successor to the EU GDPR. Post-Brexit reforms have been incremental rather than transformative: the DUAA amends, but does not replace, the UK GDPR, the DPA 2018 and the PECR. It introduces calibrated flexibilities (e.g., recognised legitimate interests, streamlined subject-access procedures, staged relaxations for low-risk technologies)²⁷⁶ while maintaining the GDPR’s principles and rights framework. This approach reflects a regulatory philosophy of pragmatic simplification without deregulatory rupture, yet it raises questions about safeguards, interpretive coherence, and potential divergence from EU standards, a concern given the pending renewal of the EU’s adequacy decision for the UK.²⁷⁷ It is precisely on the broader criteria that the DUAA’s reforms invite the most critical scrutiny. The introduction of recognised legitimate interests as a lawful basis for processing, effectively pre-approving certain categories of processing without requiring the balancing exercise that legitimate interests ordinarily demands, represents a substantive departure from the interpretive culture of the EU GDPR, even if it does not formally contradict its text. From the perspective of EU regulators, such a provision risks lowering the threshold for lawful processing in ways that are difficult to reconcile with the accountability and necessity principles that lie at the heart of the GDPR framework.

The adequacy risk is further compounded by structural and institutional considerations. The DUAA introduces greater ministerial flexibility in amending data protection requirements through secondary legislation, reducing the role of parliamentary scrutiny in future regulatory changes. This concentration of executive discretion over data protection standards sits uneasily with the EU’s insistence on the independence and stability of the supervisory framework as a

²⁷⁶ See ‘Data (Use and Access) Act 2025: Data Protection and Privacy Changes’ (GOV.UK 27 June 2025) <<https://www.gov.uk/guidance/data-use-and-access-act-2025-data-protection-and-privacy-changes>>.

²⁷⁷ Its renewal is not automatic, and the criteria against which the European Commission evaluates adequacy are not confined to formal legislative alignment but extend to the practical effectiveness of enforcement, the independence of supervisory authorities, and the existence of meaningful redress mechanisms for data subjects.

condition of adequacy. This is not a hypothetical concern; the political signals emanating from successive UK governments have consistently prioritised regulatory flexibility and economic competitiveness over alignment with EU standards, and there is little reason to assume that this disposition will not manifest in further divergence over the adequacy renewal period.

To understand the content of the UK GDPR, it is necessary to start with the EU GDPR which then became the UK GDPR. Therefore, this chapter will discuss the data protection framework in the UK from four aspects and then conclude. From the beginning, the first section will state the current UK's data protection policy and its intention in the first place. The second section will evaluate the scope of the UK GDPR. The third section will discuss the data protection principles. The fourth section will discuss the existing remedies under the GDPR in the UK and then come to conclusions which will lead to Chapter 5, which will discuss the efficacy of the GDPR.

4.2 The Current Legal Protection of the UK, Considering the Background of the EU GDPR and Its Nature

A lot of uncertainty arises in the collection of personal information on the network, such as hacking into mobile phone systems and third parties obtaining information illegally. In the case of *The Duke of Sussex and others v MGN Limited*,²⁷⁸ the court's assessment provided that the wrongdoing alleged by all four claimants was basically the hacking of their mobile phones and those of their associates, the use of private investigators to fraudulently or otherwise obtain private information from third parties, and the conduct of unlawful searches and investigations of their private data, information or whereabouts, which were then used by newspapers to

²⁷⁸ *The Duke of Sussex and others v MGN Limited* [2023] EWHC 3217 (Ch).

publish stories or photographs about them.²⁷⁹

4.2.1 Identification of the key changes and improvements brought about by the current data protection model

The current data protection model, primarily embodied in the GDPR, has introduced several key changes and improvements compared to the previous data protection framework. Articles 47, 48 and 49 of the GDPR make it clear in the implementing legislation that processing necessary for legitimate interests may include processing necessary for direct marketing which is defined as the dissemination (by any means) of advertising or marketing material aimed at a specific individual; intra-group transmissions necessary for internal administration; or processing necessary for the security of network and information systems.²⁸⁰ In addition, there is a new ‘recognised legitimate interest’ legal basis for certain important public interests e.g. protection of vulnerable individuals, in which case there will be no need for a balancing test of the rights of the individual, i.e. where certain processing is deemed to be in the legitimate interests of the controller.²⁸¹

In the aspects of the transfer of personal data, the UK makes adequacy decisions on a risk-based basis based on a ‘data protection test’,²⁸² i.e. that the standard of protection in the

²⁷⁹ Ibid, press summary § 2.

²⁸⁰ David Erdos, ‘The UK and the EU Personal Data Framework After Brexit: Another Switzerland?’ [2021] University of Cambridge Faculty of Law Research Paper No. 15/2021, section 2.

²⁸¹ Article 6(1), legal basis of legitimate interests, see further on <https://www.mondaq.com/uk/data-protection/1391470/new-requirements-under-the-uk-data-protection-and-digital-information-bill>.

²⁸² See Jade Kowalski, Data (Use and Access) Bill: Third time lucky for UK data protection reform? (2024) DAC Beachcroft LLP. [https://www.traverssmith.com/knowledge/knowledge-container/the-data-use-and-access-bill-limited-data-protection-reforms-in-the-pipeline/](https://www.dacbeachcroft.com/en/What-we-think/Data-use-and-access-bill-third-time-lucky-for-UK-data-protection-reform#:~:text=Data%20transfers,the%20relevant%20controller%20or%20processor; Travers Smith, ‘The Data (Use and Access) Bill – Limited Data Protection Reforms in the Pipeline | Travers Smith’ (Travers Smith 7 November 2024) <.

receiving country is ‘not materially lower’, called ‘authorised’ transfers. The GDPR introduced a comprehensive and forward-thinking data protection model that strengthens individuals’ rights, enhances accountability for organisations, and promotes a culture of privacy and data protection across the UK, EU and beyond. However, it still exhibits certain flaws and inadequacies, which will be discussed further in the following chapters. Most recently the UK enacted the DUAA 2025, withdrawing the *Data Protection and Digital Information Bill (No.2)*,²⁸³ which was introduced in June 2022 but suspended. The new Act will be discussed in Section 5.2.2.

Personal data is able to flow freely from the EU to the UK, where it enjoys a level of protection that is substantially equivalent to that guaranteed under EU law. The adequacy decisions also facilitate the correct implementation of the EU-UK Trade and Cooperation Agreement,²⁸⁴ which foresees the exchange of personal data, for example for cooperation on judicial matters. Both adequacy decisions include strong safeguards against future disagreements, such as ‘sunset clauses’ that limit the duration of adequacy to four years.²⁸⁵ These safeguards ensure adequacy by addressing individual complaints and monitoring developments in third countries.²⁸⁶

The Commission’s assessment drew upon recent ECtHR jurisprudence when examining the adequacy of certain aspects of the UK regime,²⁸⁷ a methodological choice that itself signals the extent to which adequacy determinations are not purely technical exercises in legislative

²⁸³ UK parliament, ‘Data Protection and Digital Information Bill - Parliamentary Bills - UK Parliament’ (Parliament.uk2024) <<https://bills.parliament.uk/bills/3430>>.

²⁸⁴ See official document on https://commission.europa.eu/strategy-and-policy/relations-non-eu-countries/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en.

²⁸⁵ See EU press corner on https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183.

²⁸⁶ Anastasia Choromidou (note 158) pp 393-394; and also see European Union Agency for Fundamental Rights., *Your Rights Matter: Data Protection and Privacy: Fundamental Rights Survey*. (Publications Office 2020) <<https://data.europa.eu/doi/10.2811/292617>> accessed 21 May 2023.

²⁸⁷ Ibid, p 395.

comparison but normative evaluations of whether a third country's legal order affords rights-compatible protection in substance as well as in form. The significance of this approach is sharpened considerably when read against the backdrop of *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II)*,²⁸⁸ in which the CJEU, acting on a preliminary reference, invalidated the EU-US Privacy Shield arrangement that had served as the primary legal basis for transatlantic personal data transfers.²⁸⁹ The Court's reasoning was not confined to the technical inadequacies of the Privacy Shield's self-certification mechanism; it went to the root of whether US surveillance law, and the absence of effective judicial redress for EU data subjects against US intelligence agencies,²⁹⁰ was compatible with the essential equivalence standard that adequacy requires. In doing so, the CJEU made clear that adequacy is not satisfied by formal legislative alignment alone; a third country's framework must afford effective, enforceable, and judicially accessible protection that is substantively equivalent to that guaranteed within the EU legal order, including under the Charter of Fundamental Rights. The relevance of this reasoning to the UK's adequacy position is both direct and pressing. *Schrems II* established that the Commission cannot grant or maintain adequacy where structural features of a third country's legal order, whether in the form of disproportionate surveillance powers, insufficient supervisory independence, or the absence of meaningful redress, undermine the substantive protection afforded to EU data subjects.

Applied to the UK context, this standard invites scrutiny not only of the UK GDPR's formal provisions but of the broader legal environment within which it operates; the scope of the

²⁸⁸ *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (2020) C-311/18.

²⁸⁹ See Anastasia Choromidou (note 158) p 394; details in US Department of Commerce, EU-US Privacy Shield Framework Principles Issued by the US Department of Commerce <<https://www.privacyshield.gov/servlet/servlet.FileDownload?file%4015t000000004qAg>> accessed 1 September 2021; C-311/18, §§ 199–201.

²⁹⁰ C-311/18, § 43.

Investigatory Powers Act 2016,²⁹¹ the independence of the ICO under conditions of increased ministerial flexibility introduced by the DUAA 2025, and the accessibility and effectiveness of remedial mechanisms available to EU data subjects whose data is transferred to and processed within the UK. Each of these dimensions was implicitly evaluated in the 2021 adequacy decision, but each has also been subject to subsequent legislative and political developments that the Commission's renewal assessment will be required to address.

The UK also made several amendments to the GDPR and the DPA 2018 which took effect at the end of the transition period, through the Data Protection, Privacy and Electronic Communications Regulations (the 'DPPEC Regulations').²⁹² Before the GDPR was enacted, the lawful basis for processing personal data was regulated by the DPA 2018. A lawful basis for processing each of the data categories will be needed i.e. 'a lawful basis' to process 'personal data' and a separate lawful basis to process 'special category' data (these can sometimes be the same lawful basis).²⁹³ The GDPR, which came into force in 2018, addresses many of the shortcomings of the previous framework and sets a higher standard for data protection across the EU (including the UK at the time of implementation). It introduced more robust principles, increased the rights of individuals and imposed tougher penalties for non-compliance.

4.2.2 The current data protection model in the UK

The development of the legal framework of data protection in the UK relates to a range of

²⁹¹ Investigatory Powers Act 2016 (c. 25).

²⁹² See Anastasia Choromidou (note 158) p 391; and in detail, The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, SI 2019/419; The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020, SI 2020/1586.

²⁹³ Anastasia Choromidou (note 158) pp 390-391.

jurisprudence. A particular concern was highlighted in the Opinion in *Google Spain*;²⁹⁴ Advocate General Jääskinen argued that the scope of application of the EU data protection rules has become ‘surprisingly wide’ and highlighted ‘the wide interpretation given by the Court to the fundamental right to private life and privacy of personal information.’²⁹⁵ On appeal, the National High Court of Spain stayed the proceedings and presented a number of questions to the ECJ concerning the applicability of the EU Directive 95/46 (protection of personal data) to Internet search engines. The Court ruled that search engines, through their actions of locating, indexing, storing and disseminating personal data, are considered ‘controllers’ of the ‘processing’ of personal data.²⁹⁶ Additionally, it held that in order to guarantee the rights of privacy and the protection of personal data, operators of search engines can be required to remove personal information published by third party websites. But the data subject’s right to make that request must be balanced against the interest of the general public to access his or her personal information.

Google Spain,²⁹⁷ with the reference to EU Directive 95/46, has been very influential in shaping the reasoning of international and domestic courts which have tried to strike a balance between a claim to de-list information that relates to particular individuals from search engine results and the freedom of expression.²⁹⁸ The key question to be addressed is: how does the current data protection model in the UK regulate high-tech invasions of privacy? It will also be further discussed in the following Chapter 5.²⁹⁹

²⁹⁴ Opinion of Advocate General Jääskinen in Case C-131/12, *Google Spain SL & Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2013] ECR I-0000; see also Shakila Bu-Pasha, ‘Cross-Border Issues under EU Data Protection Law with Regards to Personal Data Protection’ (2017) 26 Information & Communications Technology Law p 217 *Google Spain*.

²⁹⁵ Ibid.

²⁹⁶ Case C-131/12, §§ 21-25.

²⁹⁷ Ibid.

²⁹⁸ Aidinlis Stergios, The Right to Be Forgotten as a Fundamental Right in the UK After Brexit [2020] 25(2) Communications Law, Available at SSRN: <https://ssrn.com/abstract=3554625>, p 12.

²⁹⁹ *supra* section 5.4.

The UK enacted the DPA in 1998 as an implementation of the directive, and other EU countries enacted corresponding Data Protection legislation as well. Over the years, technology evolved to blur the boundaries of data protection. To catch up and simplify a situation whereby each member state has slightly different laws and legal systems, the EU created the GDPR in 2016, which became law within the EU on 25 May 2018. The GDPR is a regulation rather than a directive that directly applies to all EU countries, without the need to pass separate local laws in each member state. However, the GDPR does allow for some differences between each country, such as the age of the child for data protection purposes (the default is 16, but it can be as low as 13).³⁰⁰ Partly to illustrate what these differences are in the UK the government updated the Data Protection Act in 2018. Prior to Brexit, therefore, data protection law in the UK was largely defined by a combination of the GDPR and the DPA 2018.

It has been recognised that since Brexit, there are two versions of the GDPR, the EU GDPR and the UK GDPR. After Brexit, the UK Government's Department for Digital Culture Media and Sport published 'Data: A New Direction'³⁰¹ in 2021 which put forward the data protection new framework reform and associated rules on electronic privacy in the UK.³⁰² Basically, the data protection structure within the EU remains compatible with the revised Council of the Europe framework, which is Data Protection Convention 108+ (DPC+)³⁰³ that both the EU and UK also committed to.³⁰⁴

³⁰⁰ See UK GDPR and An Overview of the UK's Data Privacy Regime' (*Stevens & Bolton LLP*) <<https://www.stevens-bolton.com/site/insights/briefing-notes/data-protection-general-data-protection-regulation-gdpr-overview>> accessed January 25, 2023.

³⁰¹ GOV.UK, 'Data: A New Direction' (GOV.UK2021) <<https://www.gov.uk/government/consultations/data-a-new-direction>>.

³⁰² David Erdos (note 15) p 2, para 2.

³⁰³ Council of Europe, Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data (2018), <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>.

³⁰⁴ Ibid, see David Erdos (note 224) pp 2-3; although the UK is a signatory to the protocol for its entry into force, not a party to the convention itself.

Data privacy compliance in the UK is always under the surveillance of the ICO. The data privacy regime of the UK may diverge from the European model in time, and there are constantly ongoing ICO consultations in this area. The notion of protecting private information in the ECHR and in the EU Charter of Fundamental Rights also highly influenced the legal policy and framework in the UK. When it comes to the misuse of personal information, art.8 provides for respect for private and family life in the ECHR and arts.7,8 do likewise in the EU Charter of Fundamental Rights; thus in human rights' terms data protection in the UK is related to these basic human rights principles as to protecting private information in the individual's life.³⁰⁵ The *Google Spain*³⁰⁶ case provided a preliminary ruling regarding the interpretation of Directive 95/46 by the ECJ. The HRA 1998 also provides privacy protection under the pre-digital era under the ECHR art.8, as discussed above in Chapter 3.³⁰⁷

Conversely, freedom of expression is also an important concept within the legal framework of protecting personal information which derived from art.10 in the ECHR and arts.10,11 in the EU Charter of fundamental rights.³⁰⁸ The conflicts between personal data and freedom of expression are becoming a more and more critical issue in the high-tech world;³⁰⁹ the concerns in the UK arise in the context of significant cases in the domestic courts in the areas of both data protection and the tort of misuse of private information; they have employed the same balancing test in terms of free expression and privacy given that the human rights' instruments affecting both areas of law should be read in harmony with each other.

³⁰⁵ Adam D Moore, 'Free Speech, Privacy, and Autonomy' (2020) 37 Social Philosophy and Policy 31, Available at: <https://doi.org/10.1017/s0265052521000030>, chapter IV, pp 40-41.

³⁰⁶ *Google Spain SL v Agencia Española de protección de Datos (AEPD)* [2014] Q.B. 1022.

³⁰⁷ See *supra* section 3.2.

³⁰⁸ Oliver Michael Butler, 'Confidentiality and Intrusion: Building Storm Defences Rather than Trying to Hold Back the Tide' (2016) 75 The Cambridge Law Journal 452, available at: <https://doi.org/10.1017/s0008197316000696>, p 453; also see ECHR Art.10, EU charter Art.10/11.

³⁰⁹ Adam D Moore, 'Free Speech, Privacy, and Autonomy' (2020) 37 Social Philosophy and Policy 31, Available at: <https://doi.org/10.1017/s0265052521000030>, chapter II, p 33.

To take the example of *PJS v News Group Newspapers Ltd*,³¹⁰ the Supreme Court upheld an interim injunction restraining further dissemination of celebrities' privacy online and overseas.³¹¹ The court focused on the discordance between the free expression interest in allowing coverage about sexual activities of a celebrity, and the privacy interests of the celebrity, his partner and young children. The Supreme Court considered that any public interest in publishing the sexual encounters of well-known people was incapable of exceeding the privacy rights in question.³¹² The situation brings scholars to consideration of a new perspective, that is how to resolve the problem of conflicts between the highly developed technology governing online personal privacy on social data platforms, and free expression.³¹³ All the historical discussions of the policy above bring us to the next stage, which is to define the scope of the UK GDPR.

4.3 The Scope of the UK GDPR

Before this section, it is important to bear in mind that when the UK was a member of the EU, the data policy in the UK was required to implement the data protection framework of the EU. After Brexit, the scope of the UK GDPR needed to be clarified, although nearly the whole of the EU GDPR provisions still remain in the UK GDPR. The GDPR is retained in domestic law

³¹⁰ See *PJS v News Group Newspapers Ltd* [2016] A.C. 1081.

³¹¹ *Ibid.*, § 1.

³¹² *Ibid.*, §§ 35,37.

³¹³ See, for example, GDPR: noyb.eu filed four complaints over 'forced consent' against Google, Instagram, WhatsApp and Facebook on https://web.archive.org/web/20180525211528/https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf; also see the survey on European Union Agency for Fundamental Rights. 12 June 2020, available at <https://fra.europa.eu/sites/default/files/frauploads/fra-2020-fundamental-rights-survey-data-protection-privacyen.pdf>; see also research work mentioned *supra*, Adam D Moore, 'Free Speech, Privacy, and Autonomy' (2020) 37 Social Philosophy and Policy 31, Available at: <https://doi.org/10.1017/s0265052521000030>.

as the UK GDPR, but the UK has an independent right to review the framework.³¹⁴ The UK GDPR is juxtaposed with the revised version of the DPA 2018 which reflects the key principles, rights and obligations that remain unchanged.³¹⁵

To explore these issues, it is necessary to define some concepts that will be needed in the following part of this section. In the first place, how does the GDPR define data controllers and processors? The distinction between data controllers and processors is foundational to the allocation of responsibility and liability under the UK GDPR; it is a distinction that is considerably more unstable and contested in practice than its formal legal definition suggests. A controller is defined as the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing personal data.³¹⁶ The controller is, in this sense, the prime decision-maker, the entity whose choices about why and how personal data is processed attract the heaviest regulatory obligations and the most significant exposure to enforcement action and civil liability. A processor, by contrast, is a natural or legal person, public authority, or other body which processes personal data on behalf of the controller, acting strictly under the controller's instructions and without making any independent use of the information so processed.³¹⁷

However, the roles of controller and processor are not mutually exclusive, nor are they necessarily stable across the lifecycle of a single processing operation. An entity may simultaneously perform both functions in respect of different aspects of the same dataset, acting

³¹⁴ Addis, Maria Chiara and Kutar, Maria, 'The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness' (2018) UK Academy for Information Systems Conference Proceedings 2018. 29, chapter 5, para 2.

³¹⁵ See Beverley Flynn, Gary Parnell and Charles Maurice, 'An Overview of the UK's Data Privacy Regime' (Stevens & Bolton LLP) <<https://www.stevens-bolton.com/site/insights/briefing-notes/data-protection-general-data-protection-regulation-gdpr-overview>> accessed January 25, 2023.

³¹⁶ See Article 4(12), GDPR and also see *Practice note, Data breach notification under the GDPR: What is a personal data breach?*.

³¹⁷ Ibid.

as a processor in relation to data it handles on behalf of a client, while acting as a controller in respect of the same data when it processes it for its own internal purposes, such as staff training, fraud detection, or service improvement. The CJEU acknowledged this complexity in *Fashion ID*,³¹⁸ where it recognised that joint controllership could arise even where entities participate in only one stage of a processing chain, provided that their participation influences the determination of the purposes and means of processing.³¹⁹ The implication is that the controller-processor boundary is not fixed at the outset of a processing relationship but may shift, or may be occupied simultaneously by the same entity, depending on the specific processing activity under examination.

Where a processor exercises meaningful discretion over the means of processing, selecting algorithms, determining retention periods, or making inferences from data, there is a credible argument that it has, in substance if not in form, assumed the role of controller, with corresponding obligations under Articles 24 to 26 of the UK GDPR that its contractual characterisation as a mere processor would otherwise allow it to evade. The ICO has acknowledged this interpretive difficulty, but the practical enforcement of controller obligations against entities that present themselves as processors remains an underdeveloped area of UK data protection law.

4.3.1 The meaning of personal data processing within GDPR

The problem of misusing and disclosing of private information online out of jurisdiction has been canvassed because the digital and social-tech elements in most human rights cases tend

³¹⁸ *Fashion ID v Verbraucherzentrale NRW* C-40/17, 2019 (*Fashion ID*).

³¹⁹ *Ibid*, §§ 68-70, 73.

to be complicated, but there is no doubt that such disclosures could not only lead to an ability to claim data protection remedies, but also impair any injunctions obtained against actors that are within the jurisdiction.³²⁰ The scope of private data protection in the legal framework of the UK could be described as territorial effects and extra-territorial effects. According to art.3 GDPR, it applies to data controllers and processors within the UK; those terms have a deliberately broad meaning, even if the data processing takes place outside the UK.

Furthermore, the relevant data subject is an important entity in relation to evaluating whether a case is under the jurisdiction of the UK courts or not, as discussed below. The UK GDPR applies to two kinds of personal data processing. For the first one, processing personal data is carried out wholly or partly by automated means. The second one is processing personal data that forms part of a physical or electronic filing system.³²¹ At this point, what can be counted as processing personal data exactly?

It could be assumed that the digital operation of personal data online like the back-stage algorithm is one practical form which counts as processing personal data. One can consider Facetime or talk with each other face to face: all these verbal communications cannot be counted as ‘processing’, but it is apparently a kind of personal information which might be disseminated online.³²² However, due to the main focus on online personal information, verbal communication which occurs face to face will not be discussed further under this sub-heading. On the other hand, if one company received and collected CVs online from potential job candidates and used them for commercial purposes like making electronic lists of personal

³²⁰ See Fiona Brimblecombe and Helen Fenwick, ‘Keeping Control of Personal Information in the Digital Age: Efficacy and Equivalence of Tortious and GDPR/DPA Relief?’ (2022) 138 Law Quarterly Review, p 468.

³²¹ See van Ooijen I and Vrabec HU, ‘Does the GDPR Enhance Consumers’ Control over Personal Data? an Analysis from a Behavioral Perspective’ (2018) 42 Journal of Consumer Policy 91, pp 95-96.

³²² See Fiona Brimblecombe and Helen Fenwick (note 11) p 42.

phone numbers and selling them to a third party, it definitely could be classified as a processing of personal data.

The question here comes as to how the GDPR affects the processing of personal data in the extra-territorial context.

4.3.2 The extra-territorial scope of the UK GDPR

One of the most pressing ongoing concerns about the policy is whether and how it should be applied internationally, given the cross-border nature of the internet. Advocates for the EU policy noted that the protections only applied to web searches from IP addresses within the European Union; those searching from elsewhere or EU-based searchers using virtual private networks (VPNs) to mask their location could still access any controversial content.³²³ The territorial scope is clearly highly significant. It is inevitable to highlight the legislative scope of EU GDPR when it comes to the extra-territorial effect of the UK GDPR. Although the EU GDPR may apply to vendors in the EU serving users outside the EU and to vendors outside the EU serving users in the EU, it does not, *de jure*, apply to vendors outside the EU serving consumers outside the EU.³²⁴

Nevertheless, Peukert et al observed a *de facto* change in their findings as to websites located outside the EU serving consumers outside the EU.³²⁵ This observation is most persuasively

³²³ See Eric Bullard, 'Right to Be Forgotten: Overview | EBSCO' (EBSCO Information Services, Inc. | www.ebsco.com2024) <<https://www.ebsco.com/research-starters/law/right-be-forgotten-overview>>.

³²⁴ See Christian Peukert and others, 'Regulatory Spillovers and Data Governance: Evidence from the GDPR' (2022) 41 Marketing Science 746, p 319.

³²⁵ Ibid, pp 319-320.

explained by reference to the ‘*Brussels Effect*,’³²⁶ a theory developed and systematised by Bradford, which has generated substantial attention in the legal and regulatory literature on the dynamics of global governance and regulatory competition. Bradford’s research holds that the EU possesses a unilateral capacity to regulate global markets by projecting its standards outward, across competition policy, privacy protection, hate speech regulation, and beyond,³²⁷ not through formal international agreement or coercive diplomatic pressure, but through the structural logic of market access and compliance economics. The Preliminary ruling in *Weltimmo sro*³²⁸ could be considered at this point. Weltimmo had carried out a real and effective activity in Hungary, and Weltimmo also had a representative in the country. The representative, whose address was in Hungary, acted as a point of contact between Weltimmo and advertisers representing the company in administrative and judicial proceedings. In addition, Weltimmo had opened a bank account in Hungary to collect its debts and used a mailbox in Hungary to manage its daily business affairs. This information was verified by submission to the court, which was able to establish the existence in Hungary of an ‘establishment’ within the meaning of the directive.³²⁹

If this was the case, then Weltimmo’s activities were subject to Hungarian data protection legislation. The court’s stance stated that an ‘establishment’ could be demonstrated by effective activity, even minimal, exercised through stable arrangements.³³⁰ The ECJ recalled that, according to Directive 95/46, each Member State must apply the provisions it has adopted under Directive 95/46 if the data processing is carried out within the scope of the activities by

³²⁶ Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

³²⁷ Ibid; chapter 2; with the further interview on <https://geopolitique.eu/en/articles/the-european-union-in-a-globalised-world-the-brussels-effect/>.

³²⁸ *Weltimmo sro v Nemzeti Adatvédelmi és Információs Zrt* (C-230/14) EU:C:2015:639, [2016] 1 W.L.R. 863, [2015] 10 WLUK 12.

³²⁹ Ibid, § 17.

³³⁰ Ibid, § 28.

the controller on its territory.³³¹ In this regard, the Court noted that the presence of only one representative was sufficient to constitute an institution, provided that the representative's behaviour was stable enough to supply the relevant services in the Member State concerned.³³²

A determined similar position can also be found in *Soriano v Forensic News LLC*.³³³ The courts found that the business scope of Forensic News was mainly in the US and did not relate to the UK; in fact, they had no employees or representatives in the UK which indicated that as a whole they did not fall within the scope of the GDPR under art. 3(1). When courts considered the term 'establishment' in art. 3(1), they did not accept that a few UK subscriptions with no 'core activities' on the social platform with the general payment for services could constitute 'establishment'.³³⁴ From this point of view, the courts did not grant this part of the application. Therefore, the general scope of UK GDPR can be illustrated as, if one single data invasion action happened in each data processing branch connected with the UK (it would need to prove 'stable enough'), which included the invasion of the third party and intermediaries, then the UK GDPR will apply.

The importance of this phenomenon for the present thesis substantially complicates any assessment of the UK's post-Brexit data protection framework. If global platforms are already operationally aligned with GDPR standards as a consequence of *Brussels Effect*, the UK government's pursuit of regulatory divergence through the DUAA 2025 may carry less practical deregulatory impact than its proponents suggest, companies subject to the *Brussels Effect* will continue to apply GDPR-equivalent standards to UK data subjects regardless of

³³¹ 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).

³³² C-230/14, EU:C:2015:639, [2016] 1 W.L.R. 863, [2015] 10 WLUK 12, §§ 28, 29.

³³³ *Soriano v Forensic News LLC* [2021] EWHC 56 (QB).

³³⁴ *Ibid*, § 64.

what domestic UK law requires. The effect of the ‘adequacy decision’³³⁵ of the EU on the current data protection scope in the UK is important. The UK still maintains an ‘adequate’ list of countries that allow international data transfer.³³⁶ The EU Commission’s own ‘adequacy decision’³³⁷ on which the list of the UK was originally based after Brexit, are likely to diverge. In order to transfer personal data to ‘inadequate’ countries, controllers and processors can make use of existing measures such as binding corporate rules and standard contract clauses (‘SCCs’). In 2021, the European Commission introduced the new SCCs for use within the EU, and after that, the UK has its own addendum to work with the EU’s new SCCs. To some extent, contractual requirements for international data transfers are complex and the UK still uses the EU’s old SCCs in some cases.

*Soriano v Forensic News LLC*³³⁸ suggests that the extraterritorial application is fact-dependent, and sometimes data protection claims are brought alongside other claims like defamation. Depending on the situation, entities in third countries that receive personal data from Europe may in future argue that since the GDPR regime applies to them, there is no need to establish an international data transfer gateway (standard contractual clause etc) to ensure the transfer is legal, which will effectively free up data flow from Europe.³³⁹ However, neither the UK nor the EU sees the U.S. as ‘adequate’. Following *Schrems II*,³⁴⁰ the EU-US Privacy Shield was deemed not to provide the level of protection needed for the secure transfer of personal data

³³⁵ ‘Adequacy’ (ICO) <<https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/adequacy/>> accessed May 1, 2023.

³³⁶ David Erdos, ‘The UK and the EU Personal Data Framework after Brexit: A New Trade and Cooperation Partnership Grounded in Council of Europe Convention 108+?’ (2022) 44 Computer Law & Security Review 105639, chapter 3, available at <https://doi.org/10.1016/j.clsr.2021.105639>.

³³⁷ ‘Adequacy’ (ICO) (note 335).

³³⁸ [2021] EWHC 56 (QB).

³³⁹ Ibid.

³⁴⁰ *supra* pp 99-100.

and was therefore ineffective.³⁴¹ The invalidation was not premised on procedural or administrative deficiencies in the Privacy Shield’s self-certification mechanism, but on a substantive finding that US surveillance law, in particular the bulk collection powers exercised under Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333, afforded US intelligence agencies access to EU personal data on a scale and with a degree of opacity that was irreconcilable with the principles of necessity and proportionality enshrined in EU fundamental rights law. The Court found that EU data subjects lacked access to effective judicial redress against the exercise of these surveillance powers, a deficiency that struck at the foundation of the adequacy framework, which requires not merely that protective rules exist on paper but that they are enforceable in practice by the individuals whose data is at stake. Lorna Woods³⁴² has observed that, despite differences in drafting between Articles 45 and 46 GDPR, the Court has interpreted Chapter V consistently so as to establish a common baseline of data protection standards applicable across different transfer mechanisms. Underpinning this interpretive approach is the Court’s broader commitment to fundamental rights, in particular the right to private life guaranteed by Article 7 of the EU Charter of Fundamental Rights. This commitment is further reflected in a line of cases concerning the bulk retention of communications and location data by telecommunications operators for access by law enforcement and intelligence bodies. The Court consistently held that retention requirements imposed indiscriminately across the entire population, without any threshold of suspicion, were disproportionate, reinforcing the principle that mass, untargeted surveillance cannot be justified under EU law regardless of the security objectives it purports to serve.

³⁴¹ Recent Case: ECLI:EU:C:2020:559, ‘*Data Protection Commissioner v Facebook Ireland Ltd.*’ (Harvard Law Review February 10, 2021) <<https://harvardlawreview.org/2021/02/data-protection-commissioner-v-facebook-ireland-ltd/>> accessed February 2, 2023.

³⁴² See Lorna Woods, “‘You Were Only Supposed to Blow the Bloody Doors Off!’: *Schrems II* and External Transfers of Personal Data’ (Blogspot.com 16 July 2020) <<https://eulawanalysis.blogspot.com/2020/07/you-were-only-supposed-to-blow-bloody.html>> accessed 8 March 2026.

It is also worth noting that the extra-territorial reach of data protection claims is not governed exclusively by substantive data protection law but is also shaped by the procedural framework through which such claims are litigated. As Brimblecombe and Fenwick observe, CPR PD 6B³⁴³ provides the relevant procedural gateway for serving proceedings out of the jurisdiction in cases with an international dimension. The availability of this gateway in data protection disputes turns, in significant part, on the characterisation of the underlying claim; where a data protection violation is framed as, or accompanied by, a tortious cause of action, such as misuse of private information, CPR PD 6B paragraph 3.1 may be engaged on the basis that the tort³⁴⁴ was committed within the jurisdiction, or that damage was sustained here, or that the claim is governed by the law of England and Wales. The jurisdictional reach of a data protection claim, and the court's willingness to permit extra-territorial service, may depend critically on whether the claimant can characterise their grievance in tortious terms sufficiently to satisfy the gateway conditions. This intersection between procedural jurisdictional rules and the substantive tort-based dimensions of data protection claims will be examined in detail in the following section.³⁴⁵

In conclusion, the scope of the UK GDPR was derived from the EU data protection framework as revised and remained the same (largely) with expansion after Brexit, but the new reform of the UK government may bring differences (the new DUAA 2025 mentioned above). It is apparent that the legal landscape of the UK data protection defines the jurisdiction attribution among courts and affects the free flow of information domestically and transnationally. Consequently, section 3 in this Chapter 4, discussed the meaning of personal data processing within the GDPR by using case studies and considering the extra-territorial scope of the UK

³⁴³ CPR PD6B at para. 3.1(9) provides that “A claim is made in tort where – (a) damage was sustained within the jurisdiction; or (b) the damage sustained resulted from an act committed within the jurisdiction...”.

³⁴⁴ Fiona Brimblecombe and Helen Fenwick (note 320) p 476.

³⁴⁵ See *infra* section 4.5.

GDPR in part 4.3.2. With these concepts in mind, the thesis will then move in the next section to the data protection principles of the UK GDPR.

4.4 The Principles of the UK's Domestic Personal Data Protection Regime

Following the above discussion of the scope of the UK GDPR, it is now worthwhile to analyse the embedded principles which consolidate and reflect the theoretical basis of the UK GDPR.

4.4.1 The principles of the UK GDPR

Following the standing point of the UK GDPR, there are seven key principles that need to be set out. According to art.5 of the UK GDPR, these are: ‘lawfulness fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and accountability’.³⁴⁶ Also, there are some clarifications from the ICO; the principles of the domestic data protection regime in the UK give the guidelines for judicial responses, legislation and legal practices.³⁴⁷ For example, Art.5 (1) of the GDPR, requires that personal data shall be lawfully and fairly and in a transparent manner processed (this covers digital information in relation to individuals).³⁴⁸

After the definitions of these principles, now this section turns to a more intensive analysis of the GDPR principles. The UK GDPR provides an appropriate, comprehensive legal basis for

³⁴⁶ See UK GDPR Art.5 and also see *Practice note, Data breach notification under the GDPR: What is a personal data breach?*

³⁴⁷ The Principles (ICO) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/>> accessed May 1, 2023.

³⁴⁸ See UK GDPR Art.5 and also see *Practice note, Data breach notification under the GDPR: What is a personal data breach?*

the protection of personal data and is intended to provide fair boundaries for data processing.³⁴⁹ From the viewpoint of Schade, the GDPR creates a comprehensive framework of principles (purpose limitation, data minimisation, fairness, transparency, accountability), and a range of legitimate bases for personal data processing (consent, contractual relationships, legal obligations, legitimate interests).³⁵⁰

Consent has become a cornerstone of personal data protection in the EU³⁵¹ and so that is now the case in the UK. Peukert et al put forward that although it is difficult to measure the influence of the consent and data minimisation in general, the principles of the GDPR set out above harmonise privacy law and enforcement and increase the protection of individuals' privacy while maintaining the benefits of data processing.³⁵² Following the cases of the Snowden revelations and the Cambridge Analytica scandal, the principles such as transparency showed their potential power in the regulation provided by the GDPR.³⁵³ Gil González et al³⁵⁴ mentioned in their research an interesting recent warning by the UK data protection authority (ICO) to the Washington Post,³⁵⁵ which was guided under the consent principle. In terms of key tenets of an ideal scenario, consent needs to be freely given, specific, informed and unambiguous.³⁵⁶ But the Washington Post cookie banner only allowed their users to give their

³⁴⁹ Addis, Maria Chiara and Kutar, Maria, 'The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness' (2018).UK Academy for Information Systems Conference Proceedings 2018. 29, chapter 5, 6.

³⁵⁰ Frederik Schade, 'Dark Sides of Data Transparency: Organized Immaturity after GDPR?' [2023] Business Ethics Quarterly 1, p 6, available at: <https://doi.org/10.1017/beq.2022.30>.

³⁵¹ Eleni Kosta, 'Consent in European Data Protection Law' (2013) *Martinus Nijhoff Publishers, Leiden*, chapter 3, available at: <https://doi.org/10.1163/9789004232365>.

³⁵² Christian Peukert and others, 'Regulatory Spillovers and Data Governance: Evidence from the GDPR' (2022) 41 Marketing Science 746, p 321.

³⁵³ Frederik Schade, 'Dark Sides of Data Transparency: Organized Immaturity after GDPR?' [2023] Business Ethics Quarterly 1, p 2, available at: <https://doi.org/10.1017/beq.2022.30>.

³⁵⁴ Elena Gil González and Paul de Hert, 'Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and Principles,' (2019) 19 ERA Forum 597, pp 597–621, available at: <https://doi.org/10.1007/s12027-018-0546-z>.

³⁵⁵ See Womble Bond Dickinson (US) LLP, 'ICO Warns Prominent US Company to Change Business Model: Paid Subscription versus FREE with Ads' (Natlawreview.com2018) <<https://natlawreview.com/article/ico-warns-prominent-us-company-to-change-business-model-paid-subscription-versus>> accessed 14 August 2023.

³⁵⁶ See UK GDPR Art 4.

consent under the premium subscription option which apparently payments included.³⁵⁷ It was considered distinctly unfair and against the consent principle that the users could not manage their own consent under the free services provided by this company.

Widespread data-driven monitoring and intervention will tend to have social and political consequences in terms of preventing similar incidents.³⁵⁸ In the wake of these incidents, public scepticism has led to far-ranging calls for greater transparency in data practices in both public and private institutions, now answered by the GDPR.³⁵⁹ The transparency principle focuses attention on the practices of the controllers and processors. But there remains the risk that they may sometimes tend to ignore the importance of principles like consent and transparency in order to satisfy their own commercial gain. Therefore, the section below will further discuss the importance in practice of the principles in the UK GDPR.

4.4.2 The importance in practice of the principles in the UK GDPR

The foundational distinction to establish is that not all data protection principles carry equal remedial weight. Certain principles function primarily as regulatory guides to good practice, breach of which may attract enforcement action by the Information Commissioner but does not in itself generate a private right to compensation. Other principles, those more akin to subjective rights, do attract the potential for individual compensation where breach causes damage. It is within this second category that the private law dimensions of data protection become most significant, and it is here that the case law examined in this section has done its

³⁵⁷ See Elena Gil González and Paul de Hert, 'Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and Principles,' (2019) 19 ERA Forum 597, section 2.3, p 602, available at: <https://doi.org/10.1007/s12027-018-0546-z>.

³⁵⁸ Ibid, p 3.

³⁵⁹ Ibid, p 8.

most consequential work.

The claim in *Lloyd v Google*³⁶⁰ was founded on s 13 of the DPA 1998, which conferred on individuals a right to compensation where they had suffered damage by reason of any contravention by a data controller of any of the requirements of the Act.³⁶¹ The Supreme Court's ultimate rejection of the representative action in *Lloyd*³⁶² turned not on the unavailability of s 13 as a cause of action but on the Court's refusal to accept that every member of the represented class had suffered the same damage, specifically its rejection of the proposition that loss of control over personal data, without proof of individualised damage, could constitute compensable damage under the DPA 1998. The DPA 1998, as interpreted in *Lloyd*, required damage of a sufficiently concrete and individualised character to ground a compensation claim, creating a remedial threshold that may exclude precisely those data subjects whose data has been systematically misused at scale but who cannot point to specific, quantifiable harm.

This threshold was partially addressed, in the context of distress, by *Vidal-Hall v Google*,³⁶³ in which the Court of Appeal accepted that financial loss was not a prerequisite for an award of damages under s 13 of the DPA 1998 in respect of distress.³⁶⁴ This was a significant doctrinal development: by decoupling compensation from financial loss, *Vidal-Hall* acknowledged that the harms attendant on unlawful data processing are frequently non-pecuniary in character, dignitary, psychological, and relational, and that a compensation framework that required proof of financial damage would systematically under-remedy the most common forms of data

³⁶⁰ *Lloyd v Google LLC* [2020] Q.B. 747.

³⁶¹ See s.13 of Data Protection Act (DPA) 1998 compensation for failure to comply with certain requirements.

³⁶² [2021] UKSC 50.

³⁶³ *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] Q.B. 1003, [2015] 3 WLUK 852.

³⁶⁴ *Ibid.*, §§ 95-105.

protection injury. However, *Vidal-Hall* left unresolved a deeper question that how should damages for non-material harm be assessed, and on what normative basis?

It is at this point that *Gulati v MGN*³⁶⁵ assumes critical importance, and where its relevance to data protection law, though not always made explicit in the scholarship, is most analytically productive. *Gulati* was not a data protection case; it concerned the tort of misuse of private information, specifically the unlawful interception of voicemails by the defendant's journalists. However, the Court of Appeal's approach to damages in *Gulati* has profound implications for the data protection compensation framework that extend well beyond its immediate tortious context. The Court held that damages for misuse of private information are available on two distinct bases: first, damages for the misuse itself, characterised as compensation for loss of control over private information, without any requirement to prove distress or consequential harm; and second, damages for distress caused by the misuse, which may be awarded in addition. The recognition of loss of control as an independently compensable head of damage is doctrinally significant because it provides a normative foundation,³⁶⁶ rooted in the dignitary wrong of having one's private information misused, that does not depend on proof of psychological injury or financial loss. The link between *Gulati* and data protection law is made most directly through the parallel between the loss of control damages recognised in *Gulati* and the loss of control argument that was advanced, and rejected in its class action form, in *Lloyd v Google*.

4.5 Explanation of the GDPR implementation in the UK

³⁶⁵ *Gulati v MGN* [2017] Q.B 149.

³⁶⁶ See Fiona Brimblecombe and Helen Fenwick (note 320) p 462.

In the UK, the GDPR was adopted in domestic law in the UK GDPR post-Brexit and partly reflected through the DPA 2018. The DPA 2018 supplements the GDPR and provides additional details and exemptions specific to the UK's legal framework. It also addresses areas not covered by the GDPR, such as law enforcement and national security. Moreover, the GDPR grants individual certain rights regarding their personal data, including the right to access, rectify, erase, restrict processing, data portability, object to processing, and not to be subject to automated decision-making.³⁶⁷ There are also included lawful bases for processing, which were also discussed above in relation to the previous data protection framework in Chapter 3.³⁶⁸ It provides remedies including, in particular, under Art 17, 'the right to be forgotten'. The doctrinal origins of the right to be forgotten are most directly traceable to *Google Spain*,³⁶⁹ in which the CJEU held that a data subject may request the removal of links from a search engine's results where the information is inadequate, irrelevant, or no longer relevant, or excessive in relation to the purposes for which it was processed, even where the underlying third-party publication from which the link derives remains lawful. *Google Spain* established that search engines are data controllers in respect of the indexing and display of search results, and therefore bear independent data protection obligations that are distinct from, and may go further than, the obligations of the original publisher of the information. More profoundly, the Court recognised that the passage of time is itself a legally relevant factor in the assessment of data processing; information that was lawfully published and legitimately accessible at the time of its original disclosure may, with the passage of time, become disproportionate to retain in a form that renders it immediately and universally accessible through a simple name search.

It is against this framework, established and refined in *Google Spain*, that the claims in *NTI &*

³⁶⁷ Article 15-23 of the UK GDPR.

³⁶⁸ *supra* pp 78-79.

³⁶⁹ *Google Spain SL v Agencia Española de Protección de Datos*, Case C-131/12, 13 May 2014.

*NT2 v Google LLC*³⁷⁰ must be understood. Both claimants were unrelated individuals who brought proceedings against Google for breach of the DPA 1998 and for misuse of private information, each seeking the removal from Google's search results of persistent links to media reports concerning their respective criminal convictions. NT1 was convicted of conspiracy in relation to his business activities. NT2 pleaded guilty to two counts of conspiracy relating to his business. Each asked Google to remove from its listings the persistent links returned by its online search engine to various media reports about their respective convictions, on the basis that they each had a 'right to be forgotten' about their offences and that the third-party reports were, in any event, inaccurate in some respects. But Google refused their request.

The High Court handed down its first judgment on the 'right to be forgotten', ordering Google to remove search results relating to the conviction of a businessman named NT2, but rejecting a similar request from a second businessman, NT1.³⁷¹ The plaintiffs were convicted of criminal offences many years ago and complained that the search results returned by Google contained links to third-party reports of convictions that were inaccurate and/or stale, irrelevant and not in the public interest, or otherwise unlawfully interfered with their rights. The claims were brought under the DPA 1998 and the tort of misuse of private information. The court rejected NT1's claim on the basis that he was and still is a public figure with a role in public life and therefore the offences and their penalties could not be regarded as private in nature, but rather as a matter of public interest, in particular commercial interest offences, prosecutions and penalties.³⁷²

Furthermore, the court stated that NT1 pleaded not guilty, misled the public and the court and

³⁷⁰ [2018] EWHC 799 (QB).

³⁷¹ *Ibid.*, § 173.

³⁷² *Ibid.*, § 170.

showed no remorse. In contrast, the court upheld NT2's de-listing claims on the grounds that his offence did not involve dishonesty, that his punishment was based on a guilty plea, and that information about offences and their penalties was outdated, irrelevant to Google users and there was insufficient legitimate interest to justify its continued provision.³⁷³ In reaching their decision, the judges emphasised that, while a spent conviction is an important factor in favour of de-listing, privacy does not always prevail in such cases. Rather, 'the specific rights claimed by the individual concerned still need to be assessed and weighed against any competing freedom of expression or freedom of information considerations or other relevant factors that may arise in a particular case'.³⁷⁴

In deciding on the right to be forgotten claim, the Court referred to the applicable guidelines of *Google Spain*³⁷⁵ and the EU Working Party.³⁷⁶ The Court held that NT1 was a public figure with a limited role in public life and that information about his offences and penalties could not be considered to be of a private nature in relation to his personal life, but rather a matter of public interest, i.e., there had been a commercial offence, its prosecution and penalties. In addition, NT1 had it was found no expectation of privacy as the information had initially appeared in the context of crime and court reporting in the national media as a natural and predictable consequence of the plaintiff's own criminal behaviour. Importantly, as a result of the change in the law, NT1 spent less time in prison than expected, and his business career after his release made information about his past relevant to the public's ongoing assessment of his honesty.³⁷⁷ The significance of *NT1 & NT2* lies not merely in its application of *Google Spain* to the domestic legal context, but in the granular and contextually sensitive balancing exercise

³⁷³ Ibid, § 223.

³⁷⁴ Ibid, § 37.

³⁷⁵ Case C-131/12.

³⁷⁶ Ibid, §§ 103-105.

³⁷⁷ [2018] EWHC 799 (QB), § 168.

that Warby J undertook in respect of each claimant separately, reaching different conclusions in each case.

*JQL v NTP*³⁷⁸ is a particularly instructive case in this regard, and its significance for the present thesis extends well beyond its immediate facts. The case concerned the malicious invasion of the claimant's mental health privacy, a category of special category data attracting the highest level of protection under Article 9 of the UK GDPR, and it required the court to grapple directly with the question of how compensation should be assessed and structured where the harm is primarily non-material in character. Lewis J awarded the claimant £15,000 in damages, comprising (i) general damages relating to distress, injury, feelings of anxiety and embarrassment, and C's loss of control and autonomy; and (ii) serious damages.³⁷⁹ The inclusion of loss of control and autonomy as a distinct head of general damages is directly relevant to the broader remedial argument developed in this thesis. As the preceding discussion of *Gulati* and *Lloyd v Google* has established, the question of whether loss of control over personal information constitutes an independently compensable harm, or whether it must be parasitic upon proof of distress or consequential damage, remains one of the most contested issues at the intersection of tort and data protection law. *JQL* is significant because it treats loss of control and autonomy not as a freestanding head of damage but as a component of the general damages award alongside distress and injury to feelings, implicitly recognising that the wrongful disclosure of sensitive personal data involves a composite harm whose full extent cannot be captured by a purely distress-based assessment. This approach is more consistent with the dignitary foundations of privacy protection identified in *Gulati* than with the restrictive approach to loss of control adopted by the Supreme Court in *Lloyd*, and it suggests a judicial

³⁷⁸ *JQL v NTP* [2020] EWHC 1349 (QB).

³⁷⁹ *Ibid.*, § 164.

willingness, at least at first instance, to award compensation that reflects the full normative gravity of a serious privacy violation rather than merely its measurable psychological consequences.

The court's approach to injunctive relief in *JQL* is equally revealing, and its reasoning illuminates the conditions under which prospective protection will be granted in cases involving the wrongful disclosure of sensitive personal data. Lewis J identified five reasons³⁸⁰ for granting the injunction: the remedy naturally flowed from the finding that the information ought not to have been disclosed; the defendant's undertakings given at trial were of uncertain reliability given the judge's concerns about subsequent disclosure; the defendant's account of his conduct during proceedings had been far from straightforward, warranting express judicial limitation; the claimant had a history of family conflict that gave rise to a credible risk of future misuse of the information; and an injunction would help to contain the ongoing harm she had suffered. This is analytically important because it demonstrates that the remedial framework in this area extends beyond backward-looking compensation for past violations to encompass forward-looking protection against the continuation or repetition of harm, a dimension of the remedial landscape that is insufficiently theorised in the existing scholarship and which this thesis addresses directly in Chapter 8.

4.5.1 Remedies, liability and penalties

Chapter VIII of the UK GDPR (supplemented by DPA 2018) sets out the remedies available to data entities for breaches of the UK GDPR and DPA 2018, and the penalties that may be imposed by the ICO, which may be considered in court, in the event of a data breach. Under

³⁸⁰ Ibid, § 167.

the UK GDPR supplemented by the DPA 2018, it is reasonable to find that there are to an extent sufficient remedies under the current legal data protection regime as interpreted in the case law. It is normal business practice for businesses or intermediaries to record the personal data to improve online services, such as by noting the favourite products of customers, thereby making the online experience more convenient. But that presupposes consent. There may be circumstances where processors collect and gather personal data and then disclose it for commercial or other purposes. There is some evidence, discussed in chapter 3, of dramatic increases in the area of harvesting and disclosing personal data online without consent.³⁸¹ Therefore, the remedies and penalties for victims of misuse of personal data must be taken into account.

a) Remedies

The remedial framework for privacy violations operates across two distinct but increasingly intersecting tracks: the tort of misuse of private information, which provides compensation for individual victims through the courts; the right ‘to be forgotten’ under art. 17 GDPR provides a legal basis for awarding a remedy. The interpretation of art. 17 could be flexible to perform a role which is somewhat similar to that underlying injunctions, ‘to ensure its own efficacy and to create the equivalence of relief as between the tort and data protection remedies’.³⁸² From the view of Helen Fenwick and Fiona Brimblecombe, the right in art. 17(1) can be invoked by a data subject who requests a data controller to delete the content that invades its privacy online.³⁸³ Understanding the relationship between these two tracks, and the structural tension between them, is essential to evaluating the overall effectiveness of the legal framework for

³⁸¹ van Ooijen I and Vrabec HU, ‘Does the GDPR Enhance Consumers’ Control over Personal Data? an Analysis from a Behavioral Perspective’ (2018) 42 Journal of Consumer Policy, p 92.

³⁸² Fiona Brimblecombe and Helen Fenwick (note 320) p 462.

³⁸³ Ibid, p 469.

protecting informational privacy, and it is this relationship that the cases discussed in this section collectively illuminate.

The recognition that informational autonomy constitutes a legally protected interest whose violation is compensable without proof of financial loss or health impact represents a significant doctrinal development,³⁸⁴ the implications of which run through each of the cases considered below. The cause of action in each case is the tort of misuse of private information, a tort whose relationship with the data protection statutory framework is one of parallel operation rather than mutual exclusivity, in that a single set of facts may simultaneously engage both the tort and the UK GDPR's prohibition on unlawful processing of personal data. Where this is the case, the claimant may in principle pursue remedies under both frameworks, though the practical relationship between tortious compensation and statutory compensation under s 168 of the DPA 2018 raises questions of coordination and potential overlap that the courts have not yet resolved with full clarity.

The coexistence of these two remedial frameworks, one compensatory and individually focused, the other punitive and institutionally focused, means that the protective effect of the law depends on how effectively they operate in combination, and whether the gaps left by each are addressed by the other. As the preceding analysis of *Gulati*, *Lloyd*, and *JQL* has demonstrated, those gaps are considerable, and this section examines the extent to which the developing case law has begun, imperfectly and inconsistently, to address them.

*Mosley v United Kingdom*³⁸⁵ illustrates the ceiling of tortious compensation in high-profile

³⁸⁴ Fiona Brimblecombe and Helen Fenwick (note 320) p 461.

³⁸⁵ *Mosley v News Group Newspapers Ltd* [2008] E.M.L.R 20.

privacy cases and its limitations as a deterrent mechanism. The cause of action was misuse of private information, arising from the News of the World's publication of footage of the claimant's private sexual activities. Mosley received a substantially higher award than many comparable claimants, the ECtHR subsequently declined to hold that the absence of a pre-notification requirement in English law violated Article 8, a finding that itself speaks to the structural insufficiency of after-the-fact compensation as a mechanism for protecting privacy where the harm, once publication has occurred, cannot be meaningfully undone. The relevance of *Mosley* to the data protection framework lies in this insufficiency; where the harm is irreversible, compensatory damages, however substantial, cannot perform the protective function that the right to erasure under Article 17 of the UK GDPR, or an effective pre-publication injunction regime, might in principle provide.

*Sicri v Associated Newspapers*³⁸⁶ involved a claim in the tort of misuse of private information arising from the publication of information linking the claimant to a possible criminal prosecution. The award of £83,000 in damages, of which £33,000 represented financial loss and the remainder non-material harm,³⁸⁷ is significant. It demonstrates that the quantum of tortious damages in privacy cases has developed considerably beyond the modest awards that characterised the early development of the tort, reflecting the courts' growing willingness to treat serious privacy violations as generating substantial compensable harm. It confirms that the non-material dimensions of privacy harm, distress, loss of autonomy, reputational injury, are independently compensable and carry significant weight in the court's assessment, a point whose implications for the data protection compensation framework are examined in the

³⁸⁶ [2020] EWHC 3541 (QB); [2021] E.M.L.R. 10, §§ 189,190.

³⁸⁷ *Ibid.*

preceding discussion of *Gulati v MGN*³⁸⁸ and *JQL v NTP*.³⁸⁹ The relationship between *Sicri* and the data protection framework arises from the fact that the wrongful publication of information linking an individual to a possible prosecution engages not only the tort but also the UK GDPR on the processing of personal data relating to criminal convictions and offences under Article 10, a dimension of the case that has received insufficient attention in the existing commentary and to which this thesis returns in Chapter 8.

The newspaper defendants' argument, raised in *Google Inc v Vidal- Hall*³⁹⁰ and *Murray v Ministry of Defence*,³⁹¹ that damages in privacy cases 'should be limited,'³⁹² reflects the persistent institutional resistance of the press to the expansion of tortious privacy protection, a resistance grounded in Article 10 and the competing public interest in freedom of expression. It was found that *Vidal-Hall*³⁹³ was not authority to propose that damages for misuse of private information could be awarded only for distress and painful feelings.³⁹⁴ It could be certainly seen from the discussion of these cases that 'the damages are an award to compensate for the loss or diminution of a right to control formerly private information and for the distress that the respondents could justifiably have felt because their privacy had been exploited.'³⁹⁵ This argument must be taken seriously, not because it is ultimately persuasive, but because it identifies a genuine tension that the courts have been required to navigate in every significant privacy damage case. The resolution of that tension in *ML and WW v Germany*,³⁹⁶ where the ECtHR held that the public interest in freedom of expression outweighed the right to privacy

³⁸⁸ See *Gulati v MGN* [2017] Q.B 149.

³⁸⁹ [2020] EWHC 1349 (QB); even though the post was only available on a Facebook Page for about 3 hours and viewed by only about 35 people.

³⁹⁰ *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] Q.B. 1003, [2015] 3 WLUK 852.

³⁹¹ *Murray v Ministry of Defence* [1988] 1 W.L.R. 692, [1988] 5 WLUK 256.

³⁹² [2017] Q.B 149, §§ 44-49.

³⁹³ [2015] EWCA Civ 311.

³⁹⁴ *Ibid*, §§ 59,75,80.

³⁹⁵ [2017] Q.B 149, §§ 44-49.

³⁹⁶ App. Nos. 60798/10 and 65599/10, §§ 31, 33.

and that no Article 8 infringement had been established, illustrates that the balance between Articles 8 and 10 is not invariably struck in favour of the privacy claimant, and that the remedial framework examined in this section operates within the Convention framework that imposes real constraints on the scope and quantum of available relief.

b) Penalties

The foundational distinction to establish is that damages awarded under the tort of misuse of private information are compensatory in nature and are not intended as punishment.³⁹⁷ Their purpose is to remedy the specific harm suffered by the individual claimant, whether that harm takes the form of distress, loss of autonomy, reputational damage, or financial loss, and their quantum is therefore calibrated to the claimant's individual circumstances rather than to the gravity of the defendant's conduct as such. This stands in sharp contrast to the fining regime under the UK GDPR,³⁹⁸ where penalties of up to £17.5 million or four percent of global annual turnover are expressly designed to create deterrence and are directed primarily at private companies and public authorities rather than at vindicating individual claimants.

In *Lloyd v Google LLC*,³⁹⁹ the courts discussed the potential scope to claim damages. The special position, in this case, was that *Lloyd* was a representative action and limited by the compensatory principle. As this usually requires an individualised assessment, a representative action was not found to be appropriate for doing so. However, if entitlements can be calculated on a basis common to all class members, there is no reason why compensation or other

³⁹⁷ Fiona Brimblecombe and Helen Fenwick (note 11) pp 36, 37.

³⁹⁸ Art. 83 of the UK GDPR grants the right to ICO to seek compel administrative fines for violations of the regulation provided by the UK GDPR as regards data controllers and processors.

³⁹⁹ *Lloyd v Google LLC* [2020] Q.B. 747.

monetary remedies cannot be sought in a representative action.⁴⁰⁰ The Supreme Court rebuffed Mr Lloyd's argument and then considered the suggestion to bring claims on a 'lowest common denominator' basis.⁴⁰¹ The Court held that the facts to be proved by Mr Lloyd in each individual case were not sufficient to cross any threshold of seriousness (which in his own case had to be crossed for a breach of the 1998 Act to give rise to a right to compensation).⁴⁰²

According to the DPA 1998 s. 13, compensation is payable to any individual who suffers material damage or suffering as a result of a breach of the Act by the data controller. However, the claimant argued that the word 'damage' in s.13(1) went beyond material damage to include suffering and included 'loss of control' over personal data.⁴⁰³ He therefore claimed that individuals were entitled to compensation under s. 13 without having to provide evidence of material damage or suffering, as long as the data controller failed to comply with any of the requirements of the Act in relation to any personal data. Even if it were unnecessary to illustrate that because of unlawful processing of their personal data, an individual had suffered material damage or distress, it would be indispensable to establish the extent of that unlawful processing in each individual case.⁴⁰⁴

The Supreme Court in this case then unanimously dismissed Lloyd's representative action brought against Google. The Supreme Court also confirmed that a claim for damages for the unlawful processing of personal data under the DPA 1998 can only be made if the data subject has suffered some form of material damage (such as financial loss or physical injury) or mental distress (such as psychiatric illness).⁴⁰⁵ The Court decided that interpreting 'damage' under the

⁴⁰⁰ Ibid, §§ 46,48,50,82.

⁴⁰¹ Ibid, section F and § 145.

⁴⁰² Ibid, section F and §§ 152, 153.

⁴⁰³ Ibid, §§ 5-7

⁴⁰⁴ Ibid, §§ 29, 32, 50.

⁴⁰⁵ Ibid, §§ 133, 134, 159.

1998 Act to include a pure ‘loss of control’ claim was untenable and disallowed a representation action. Distress would be enough; it would not need to amount to an actual illness. The damage could not be the unlawful processing itself.

4.5.2 Lack of injunctive relief under the UK GDPR

The framework of remedial provisions in the UK GDPR could be viewed as insufficient in other respects, and the insufficiency becomes most apparent when the statutory compensation regime is examined alongside the parallel development of tortious privacy protection in English law.⁴⁰⁶ The relationship between these two frameworks is not merely one of historical co-existence; it is one of ongoing doctrinal interaction in which the development of the tort of misuse of private information has both informed and exposed the limitations of the statutory data protection regime, and *vice versa*.

*Campbell v MGN Ltd*⁴⁰⁷ is foundational to this analysis, and its significance for data protection law extends well beyond its immediate contribution to the development of the tort of misuse of private information. The cause of action in *Campbell* was the tort of misuse of private information, or, as it was then more commonly framed, breach of confidence in its extended, privacy-protective form, arising from the Mirror’s publication of details of the claimant’s attendance at Narcotics Anonymous meetings, together with photographs taken covertly in a public street. The House of Lords held, first, that the claimant had a reasonable expectation of privacy in respect of the published information,⁴⁰⁸ and second, that her Article 8 right to respect

⁴⁰⁶ As in *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] Q.B. 1003, [2015] 3 WLUK 852 and in *Gulati v MGN* [2017] Q.B. 149.

⁴⁰⁷ [2004] 2 A.C. 457.

⁴⁰⁸ *Ibid.*, §§ 17-20.

for private life outweighed the defendant's Article 10 right to freedom of expression,⁴⁰⁹ with the consequence that MGN Ltd was ordered to pay damages, modest in quantum but significant in doctrinal terms.

The relationship between *Campbell* and data protection law operates on several distinct levels. The information at the heart of *Campbell*, details of the claimant's health and treatment for drug dependency, constituted special category data within the meaning of what is now Article 9 of the UK GDPR, attracting the highest level of protection under the statutory framework by reason of its medical character. The Mirror's publication of this information without consent was therefore simultaneously an act of unlawful processing of special category personal data under the data protection regime. The claimant's decision to pursue the tort rather than the statutory framework reflects the remedial choices available at the time, the DPA 1998 was technically applicable but offered a less developed and less generous compensatory regime than the emerging tort, and it illustrates the practical significance of the parallel operation of tort and statute that this thesis has identified as a structural feature of the current remedial landscape.

Campbell made a foundational contribution to the normative architecture of data protection law by establishing the reasonable expectation of privacy as the threshold criterion for determining whether Article 8 is engaged. This criterion, which the House of Lords developed in the context of the tort, has since been adopted and applied in data protection contexts, informing the assessment of whether particular categories of processing constitute an unjustified interference with the data subject's right to private life. The modest quantum of damages awarded in *Campbell*, notwithstanding the House of Lords' unequivocal finding that

⁴⁰⁹ Ibid, § 124.

a serious privacy violation had occurred, illustrates precisely the remedial insufficiency identified at the outset of this section. Where the harm is primarily dignitary and non-material in character, the compensatory tort framework has historically generated awards that many commentators have regarded as disproportionately low relative to the gravity of the violation.

This insufficiency is directly relevant to the data protection framework because it raises the question of whether the statutory compensation regime under s 168 of the DPA 2018, read in conjunction with the tort, provides adequate remediation for serious privacy violations, or whether the combined effect of modest tortious awards and the individualised character of statutory compensation leaves a structural remedial gap that neither framework alone, nor both together, adequately fills. As the preceding analysis of *Gulati*, *Sicri*, and *JQL* has demonstrated, the quantum of privacy damages has developed considerably since *Campbell*, but the underlying question of whether compensation alone, as opposed to injunctive relief, regulatory fines, or structural accountability mechanisms, constitutes an effective remedy for serious informational privacy violations remains one of the central unresolved tensions in this area of law, and one to which this thesis returns in Chapter 5.

Even now, the concept of an injunction is not recognised explicitly in the UK GDPR. The absence of injunctions renders reliance on the UK GDPR less effective to some extent. As in *Von Hannover*,⁴¹⁰ covering the privacy concerns of a particular celebrity, the German courts granted injunctive relief in respect of the second and third *Frau im Spiegel* photos. The injunction provided secure protection, on the level of material loss or mental harm, to the claimants. However, the German courts did not provide a remedy for certain of the photos; thus a breach of art.8 ECHR was found at Strasbourg.

⁴¹⁰ *Von Hannover v Germany* [2005] ECHR 555; (2006) 43 E.H.R.R. 7.

In a range of domestic cases, injunctions provided relief in respect of the misuse of private information under the tort. Remedies under the tort were created with the traditional press, like newspapers, mostly in mind.⁴¹¹ The grant of injunctive relief governed by s.12(3) HRA under the tort is granted before the personal information has been disclosed, or fully disclosed, which means the personal information in this situation will be enabled to retain its internal privacy quality.⁴¹² *CG v Facebook Ireland Ltd and McCloskey*⁴¹³ involved the not interchangeable value between the torts of harassment and misuse of private information; CG had a reasonable privacy expectation, and an injunction had been granted to terminate the ‘Predators 2’ page which Mr McCloskey created on Facebook. Likewise, in *J20 v Facebook Ireland*,⁴¹⁴ when Facebook did not follow the request to remove the sensitive posts which were marked ‘extremely urgent’, J20’s solicitors applied for emergency interim injunctive relief to have the posts removed.⁴¹⁵ Such an order was granted in order to protect the claimant’s privacy.

But if the personal information has already been known or disseminated into the public domain, then the injunction will be less meaningful and might be set aside by the courts. In *PJS v News Group Newspapers Ltd*,⁴¹⁶ a magazine in the USA published a story on the sexual activities of PJS. Subsequently, similar stories were published in Scotland and on numerous websites. As a result, NGN applied to the Court of Appeal to set aside the interim injunction, arguing that it was no longer justified because the information it restricted had entered the public domain and therefore it was unlikely that PJS would be granted a permanent injunction at trial.⁴¹⁷ In

⁴¹¹ See Fiona Brimblecombe and Helen Fenwick (note 320) p 458.

⁴¹² *Ibid*, p 471.

⁴¹³ *CG v Facebook Ireland Ltd and McCloskey* [2015] NIQB 11, an injunction was obtained.

⁴¹⁴ *J20 v Facebook Ireland Ltd* [2016] NIQB 98.

⁴¹⁵ Fiona Brimblecombe and Helen Fenwick (note 320) p 472.

⁴¹⁶ *PJS v News Group Newspapers Ltd* [2016] A.C. 1081.

⁴¹⁷ *Ibid*, §§ 7, 9, 10.

addition, NGN argued that the injunction was an unjustified interference with NGN's article 10 right to freedom of expression in the ECHR. The Court of Appeal agreed to discharge the injunction. On appeal, the Supreme Court reinstated the injunction, pending a decision on PJS's application for permission to appeal.⁴¹⁸

The grant of an injunction is without doubt needed since compensation cannot fully address the concern in question. A particular example can be also found in *PJS*;⁴¹⁹ the Supreme Court focused on the question of whether the celebrities' sexual affairs could be of public interest or not. In relation to the HRA 1998 s.12(3) and the rights of the ECHR art.8/art.10, the Court of Appeal had set the interim injunction aside, on the ground that this personal information had spread already and was no longer private. The Court found that the injunction served no useful purpose and was an unwarranted interference with the newspaper's rights under art.10 of the ECHR. In this case, however, the Supreme Court found that the Court of Appeal had focused too restrictively on information already disclosed on the internet, without giving due weight to the qualitative differences in intrusion and distress that may be involved in unrestricted publication in media.⁴²⁰ It could then be found that the remedies for misuse of personal information online in the case-law, under the tort, since injunctions are available, show superiority in terms of effectiveness. Conversely the lack of injunctions under data protection demonstrates that there is a weakness in the remedies available.

To sum up, there are possible remedies available under both tort and data protection that individuals can rely on. However, to what extent the remedies can be effectively applied in relation to unconsented-to disclosures of personal information must be fully evaluated.

⁴¹⁸ Ibid, §§ 44-45

⁴¹⁹ Ibid.

⁴²⁰ Ibid, §§ 1, 9, 21.

Consequently, Chapter 5 will further consider the effectiveness of the GDPR model in the UK. That is the main topic in Chapter 5; Article 17 GDPR will also be considered further.

4.6 Conclusion

In conclusion, Chapter 4 has been divided into 4 parts to discuss the history of UK data protection and the background to the GDPR and its nature. It has covered history, scope, principles and remedies separately. Firstly, section 1 considered the history of the UK data protection regime. Section 2 further discussed the scope of the current UK GDPR, taking into account certain rules and cases. Thirdly, section 3 gave an illustration of the principles of the UK GDPR based on Chapter 2 of the UK GDPR. Finally, section 4 explained the specific remedies, liability and penalties available under the UK GDPR, examining comparisons with the tort.

The discussion of Chapter 4 in this thesis provided consideration of the basic framework of the UK GDPR. It is intended to provide a solid basis, enabling the next chapters to evaluate the effectiveness of the UK GDPR model. The potential for the misuse of personal data due to its dissemination via social media platforms, means that the UK GDPR has the essential role of creating protection for personal information online and creating a balance between business needs and private and family life. Most significantly, it must promote a reconciliation between data protection and freedom of expression. With the discussion here in mind, the thesis will now move to Chapter 5 which considers the effectiveness of the data protection model in the UK as it is used in practice, with a view to considering its efficacy in the later chapters, including in particular Chapter 7, as a global data protection model.

CHAPTER 5 AN ANALYSIS OF THE EFFECTIVENESS OF THE CURRENT PERSONAL DATA PROTECTION ENFORCEMENT IN THE UK

5.1 Introduction

The preceding chapters have established the analytical foundations upon which this chapter's evaluation of the current UK data protection model is built. Chapter 2 traced the historical and conceptual origins of the data protection and privacy, identifying main concepts of privacy and personal information that continue to shape and constrain the current regime. Chapter 3 examined the core architecture of the previous data protection regime. Chapter 4 developed the remedial analysis in depth, examining the parallel operation of the statutory compensation regime and the tort of misuse of private information, and establishing that the current framework generates significant structural gaps in the protection it affords to data subjects. It is the cumulative weight of these preceding analyses, historical, doctrinal, and remedial, that makes the evaluative exercise undertaken in this chapter both necessary and possible. This chapter therefore builds directly on what has gone before, bringing together the threads developed across the preceding chapters into a sustained and integrated evaluation of the current UK data protection model. It does so not by repeating the doctrinal analysis already undertaken, but by deploying that analysis as the evaluative lens through which the practical operation and practical effectiveness of the framework can be most rigorously assessed.

According to social theory as put forward by Hartmut Rosa, 'a major feature of modernised social communication is the shift from spatial to time superiority'.⁴²¹ He pointed out that the

⁴²¹ See Main social theory in, Hartmut Rosa, *Social Acceleration: A New Theory of Modernity* (Columbia University Press 2013).

shortage of time resources and the resulting increase in the pace of life had led to the acceleration of technology, and that the direct consequence of technological acceleration was the acceleration of social change. The theory showed that the regulations for personal privacy should also follow the pace of social change. Thus, data protection legislation in the UK is going through an important phase of transition, in particular with the localisation of the GDPR⁴²² following the adoption of the GDPR by the EU in 2016. The DUAA 2025, referred to Chapter 4, aims to update and simplify the current UK data protection framework through a wide range of provisions.

The first dimension of this evaluation concerns the institutional architecture of data protection enforcement in the UK, specifically the role of the ICO and its relationship with the UK GDPR regime. It is simultaneously a regulatory authority with significant investigative and enforcement powers, a public body whose independence is a condition of the UK's adequacy status, and an institution whose practical effectiveness determines whether the rights and obligations established by the UK GDPR translate into meaningful protection for data subjects in practice. The analysis of the ICO's institutional position under the UK GDPR/DPA 2018, and specifically the concern in the DUAA that increased ministerial flexibility over regulatory standards threatens the supervisory independence upon which adequacy depends, provides the critical context within which this section's evaluation of the ICO's role must be understood.

The second dimension examines GDPR enforcement comparatively, across both the UK and the EU, with a view to assessing whether the enforcement architecture produces outcomes that are proportionate to the scale and seriousness of data protection violations, sufficiently deterrent to modify the behaviour of powerful data controllers, and sufficiently accessible to

⁴²² See *supra* chapter 3, section 2 Processing personal data prior to the GDPR.

provide meaningful redress for individual data subjects. The third dimension evaluates the impact of the GDPR on the protection of private information across two contrasting contexts, the celebrity industry and the privacy of ordinary individuals, drawing on the specific cases examined in Chapter 4 to assess whether the current framework operates equitably across different categories of data subject.

These three dimensions of evaluation are designed to produce an assessment of the current UK data protection model that is both analytically rigorous and practically grounded, one that moves beyond formal doctrinal compliance to ask whether the framework, as it actually operates, delivers the substantive protection of informational privacy that its stated objectives demand.

5.2 The Role of the ICO, the UK GDPR Compared with that of the Tort of Misuse of Private Information (MPI)

Disputes between individuals and traditional media bodies or tech companies showed a tendency towards increasing court-based reliance on both areas of liability (data protection and MPI) in the last 15 years.⁴²³ Where two causes of action may arise in the same online privacy claim, claimants may be advised that in their particular circumstances, it is more appropriate to rely on one or the other, or that it may be more advantageous to proceed under both causes of action, although obviously they clearly cannot ‘double recover’.⁴²⁴ The relationship between the two causes of action was addressed directly,⁴²⁵ if not definitively, in *NT1 & NT2 v Google*

⁴²³ Fiona Brimblecombe and Helen Fenwick (note 11) p 30.

⁴²⁴ Ibid, see also to similar effect *NT1 and NT2 v Google LLC* § 43; *Lloyd v Google LLC* [2019] EWCA Civ 1599 [53].

⁴²⁵ See *supra* chapter 4, section 4.5.

LLC,⁴²⁶ where Warby J observed that the laws of misuse of private information and data protection are often considered to lead to the same conclusion for ‘much the same reasons.’⁴²⁷ As noted in Chapter 4, where this case was discussed in the context of the right to be forgotten under Article 17 of the UK GDPR, this observation captures an important practical truth, in the majority of cases involving the wrongful retention or publication of personal information, the analytical frameworks applicable under the tort and under the data protection statute will converge on the same outcome, because both are ultimately grounded in the same foundation, the individual’s reasonable expectation of privacy in respect of the information in question. However, as Chapter 4 also established, this convergence is not invariable, and the cases in which the two frameworks diverge, whether in respect of the threshold for liability, the defences available, or the remedies accessible, are precisely those in which the choice between causes of action, or the decision to pursue both, becomes most consequential. The observation in *NT1 & NT2* that the two regimes often lead to the same conclusion should therefore be read not as a statement that they are interchangeable, but as an empirical observation about their frequent overlap that leaves entirely open the analytically critical question of what happens when they do not overlap, and it is that question which the present chapter is principally concerned to address.

In terms of analysing the relationship between individuals’ privacy and media, it is necessary to look into the function and process of ICO’s role. They uphold information rights for the public in the digital age, when considering data controllers or processors failing to comply with the UK GDPR. Part 2 of Chapter 4⁴²⁸ discussed that DPA 2018 now reflects aspects of the GDPR, after Brexit, with some modifications: the DPA reflects certain GDPR rules in UK law

⁴²⁶ *NT1 and NT2 v Google LLC* [2018] EWHC 799 (QB).

⁴²⁷ *Ibid*, § 43; see further Fiona Brimblecombe and Helen Fenwick (note 11) p 30, fn 16.

⁴²⁸ *supra* chapter 4, The current legal protection of the UK, considering the background of the EU GDPR and its nature, p 95.

and includes extra requirements or exemptions to the GDPR. The ‘UK GDPR’ sits alongside the amended version of the DPA 2018. The key principles, rights and obligations remain the same.

The fines are much higher than the average amount awarded in compensation in MPI cases;⁴²⁹ therefore reliance on the GDPR, if appropriate on the facts, may create greater deterrence to privacy-invading bodies than reliance on MPI. This section will therefore focus on the GDPR; MPI is discussed mainly in Chapter 3.⁴³⁰ However, under the GDPR, individuals are generally not subject to fines for data protection violations.⁴³¹ It primarily focuses on regulating the behaviour of organisations and entities that process personal data.⁴³² There are no custodial sentences or powers of arrest for offenses under the DPA 2018; violations are punishable solely by fines. Similarly, the EU-GDPR text contains no provisions for arrest powers or custodial sentences.⁴³³ The principles established in *Gulati v MGN*,⁴³⁴ regarding the assessment of damages for the tort of misuse of private information, are relevant to claims under s. 13(1) of the DPA 1998. Both claims aim to protect privacy rights as guaranteed by Article 8 of the ECHR and share a ‘common source’ in this objective.⁴³⁵ The *Gulati*⁴³⁶ case recognised that claimants could receive compensation for the misuse of private information itself, as they were

⁴²⁹ For example, in *Campbell v MGN Ltd* [2004] UKHL 22, Naomi Campbell was awarded £2,500 for distress (along with £1,000 for aggravated damages) arising from articles and accompanying photographs showing her leaving a Narcotics Anonymous meeting; see also in *McKennitt v Ash* [2006] E.M.L.R 10 at [178], the claimant (a well-known folk musician) was awarded £5,000 after a previous colleague wrote a book containing personal and sensitive information detailing various sexual relationships, the claimant’s emotions regarding her deceased fiancé, and her general emotional vulnerability.

⁴³⁰ See Chapter 4, section 4.5.2. Lack of injunctive relief under the GDPR.

⁴³¹ Harry Mulhern, ‘Can an Individual Get a GDPR Fine?’ (*Measured Collective* 13 June 2021) <<https://measuredcollective.com/can-an-individual-get-a-gdpr-fine/>>.

⁴³² ICO, ‘Collecting Personal Data’ (*ico.org.uk* 19 May 2023) <<https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/collecting-personal-data/>>.

⁴³³ See Harry Mulhern, ‘Can an Individual Get a GDPR Fine?’ (*Measured Collective* 13 June 2021) <<https://measuredcollective.com/can-an-individual-get-a-gdpr-fine/>>.

⁴³⁴ *Gulati v MGN* [2015] EWHC 1482 (CH).

⁴³⁵ *Ibid*, §§ 108, 110, 112.

⁴³⁶ *Ibid*.

deprived of their fundamental ‘right to control [its] use,’ underscoring the intrinsic value of privacy and individual control over personal information.⁴³⁷ However, once privacy has been infringed, no amount of monetary compensation or subsequent injunctive relief can adequately remedy the harm caused.

Mr Justice Mann described this in *Gulati* as:⁴³⁸

‘a regime in which damages were confined to damages for distress would render the rights (to a degree) ‘illusory’ (to use the word used by the ECHR) and would, to a degree, fail to provide an effective remedy.’

As for mass media, online news sites, or private individuals misusing private information through publication, any deterrent effect is unlikely to result from the relatively low levels of damages, often below £20,000, that have been awarded in tort cases. This issue has raised concern among judges, as these amounts may not be sufficient to discourage such behaviour.⁴³⁹ In *Spelman v Express Newspapers*,⁴⁴⁰ Tugendhat J. provided: ‘If a remedy in damages is to be an effective remedy, then the amount ... [awarded] must not be subject to too severe a limitation.’⁴⁴¹ This highlights the concern that inadequate damages could undermine the effectiveness of the remedy for the wronged party.⁴⁴² Nevertheless, in certain tort cases in the

⁴³⁷ See Damages for Data Breaches - What If *Lloyd v Google* Had Been Decided under the GDPR? - Edwin Coe LLP’ (*Edwincoe.com*2021) <<https://www.edwincoe.com/blogs/main/damages-for-data-breaches-what-if-lloyd-v-google-had-been-decided-under-the-gdpr/>>; see also in Ben Gallop , Lily Walker-Parr of 5RB and Daniel Bishop, ‘Privacy Law-Misuse of Private Information Produced in Partnership with Ben Gallop and Lily Walker-Parr of 5RB and Daniel Bishop’ (2021) <<https://www.5rb.com/wp-content/uploads/2021/09/Privacy-law%E2%80%94misuse-of-private-information.pdf>>.

⁴³⁸ *Ibid*, § 113.

⁴³⁹ See Fiona Brimblecombe and Helen Fenwick (note 320) p 463.

⁴⁴⁰ *Spelman v Express Newspapers* [2012] EWHC 355 (QB).

⁴⁴¹ *Ibid*, § 114.

⁴⁴² See Fiona Brimblecombe and Helen Fenwick (note 320) fn 45.

UK, monetary compensation is usually minimal.⁴⁴³ In *ZXC v Bloomberg LP*,⁴⁴⁴ only £25,000 was awarded for the misuse of private information after a media organisation published details online regarding a criminal investigation into the claimant.

Although the award in *Bloomberg* was relatively low, it was coupled with an injunction to prevent further publication.⁴⁴⁵ Likewise in *Mosley*,⁴⁴⁶ the Strasbourg concluded that monetary compensation could serve as an adequate domestic remedy for violations of Article 8 rights due to the unauthorised press publication of private information.⁴⁴⁷ However, the Court's findings indicated a reluctance based on the effects of the margin of appreciation, to delve into the specific domestic arrangements for providing redress, particularly where the only alternative would be the award of an injunction.⁴⁴⁸

5.2.1 Informational security and consent under the UK GDPR/DPA

The preceding analysis of the ICO's enforcement role and the comparative GDPR enforcement landscape established that the effectiveness of the UK data protection framework depends not only on the formal adequacy of its legal provisions but on the practical mechanisms through which data subjects can exercise meaningful control over their personal information. It is precisely this question of practical control, and the structural conditions under which it is systematically undermined, that makes the regulation of informational security so analytically

⁴⁴³ Ibid, see further in cases, for example, in *Campbell v MGN Ltd* [2004] 2 A.C. 457, the award was £2,500, in *Douglas v Hello! Ltd (No.2)* [2003] EWCA Civ 139; [2003] E.M.L.R. 28, it was £14,600; and in *McKennitt v Ash* [2006] EWCA Civ 1714; [2008] Q.B. 73, the award was £5,000.

⁴⁴⁴ *ZXC v Bloomberg LP* [2021] Q.B. 28, see further in comment of Gavin Phillipson, 'Supreme Court Confirms Suspects' Privacy Rights: The Judgment Clarified, Two Criticisms Answered' (2022) 14 Journal of Media Law 1, pp 257-265.

⁴⁴⁵ Fiona Brimblecombe and Helen Fenwick (note 320) p 464.

⁴⁴⁶ *Mosley v United Kingdom* [2011] 53 E.H.R.R. 30.

⁴⁴⁷ Fiona Brimblecombe and Helen Fenwick (note 320) p 463.

⁴⁴⁸ Ibid, pp 463; (2011) 53 E.H.R.R. 30, § 120.

significant, and it is to this dimension of the current data protection model that this section now turns.

Cookies occupy a peculiar and revealing position in the data protection landscape. They are, in technical terms, small data files placed on a user's device that enable websites and third-party advertising networks to track browsing behaviour, build user profiles, and deliver targeted content. In legal terms, their placement constitutes the processing of personal data and therefore engages the full apparatus of the UK GDPR's consent and transparency requirements. Article 7 and Recital 32 of the UK GDPR mandate that consent must be freely given, specific, informed, and unambiguous, standards that, as the preceding theoretical analysis established, are routinely subverted by the design architecture of cookie consent interfaces. Any cookie banner that provides misleading or incomplete information therefore constitutes not merely a design failure but a violation of the legal conditions for valid consent,⁴⁴⁹ rendering the processing that follows it unlawful from the outset. The gap between this formal legal requirement and the reality of how cookie consent operates in practice is one of the most significant, and most systematically underenforced, failures of the current data protection model, and it connects directly to the consent fatigue and structural information asymmetry arguments developed in the earlier chapters of this thesis.

This structural gap between formal consent requirements and practical reality is further complicated by the broader policy context within which the UK's cookie regulation operates. Digital rights groups have raised serious concerns that the UK is laying the groundwork for a

⁴⁴⁹ See Dino Bollinger and others, 'Automating Cookie Consent and GDPR Violation Detection Automating Cookie Consent and GDPR Violation Detection' (2022) <<https://www.usenix.org/system/files/sec22-bollinger.pdf>>, section 6.

so-called ‘soft engagement’ approach to adequacy agreements with third countries,⁴⁵⁰ positioning itself as a data processing hub whose regulatory environment is sufficiently flexible to attract international data flows. If local data processors transfer personal information to jurisdictions whose data protection standards are materially lower than those the UK GDPR purports to guarantee, the knock-on risks for UK citizens, and for individuals whose data has been transferred to the UK from other jurisdictions, are considerable. This concern connects directly to the adequacy and *Brussels Effect* analysis developed earlier; a UK regulatory environment that prioritises its attractiveness as a data centre over the substantive protection of data subject risks undermining not only its own adequacy status but the informational security that its cookie regulation is designed to protect.

The most significant judicial illustration of what is at stake when cookie consent mechanisms are circumvented, and of the remedial challenges that follow, is provided by the Supreme Court’s decision in *Lloyd v Google*,⁴⁵¹ which must be understood in this section not merely as a class action procedural case but as a case fundamentally about the failure of technical consent architecture and its consequences for the enforceability of data protection rights at scale. Google introduced a ‘social ads’ feature on its now-discontinued Google+ platform, nominally designed to protect user privacy by isolating data. To implement this feature for Safari users, Google developed a technical workaround that inadvertently, or, on Mr Lloyd’s case, deliberately, allowed its DoubleClick advertising cookies to be placed in a third-party context, contrary to Apple’s policy of blocking such placements. The consequence was that DoubleClick cookies were placed on the devices of Safari users without their knowledge or

⁴⁵⁰ See Report on DSIT statistical public engagement and data standards; see also Natasha Lomas, ‘UK pauses data reform bill to rethink how to replace GDPR’, TechCrunch 4 October 2022, <https://techcrunch.com/2022/10/03/uk-data-reform-bill-replace-gdpr/>.

⁴⁵¹ *Lloyd v Google LLC* [2021] UKSC 50.

informed consent,⁴⁵² enabling Google to track their browsing behaviour across websites for advertising purposes in direct contravention of the DPA 1998's requirements.

Mr Lloyd's claim was founded on s 13 of the DPA 1998, which granted individuals the right to seek compensation for damage suffered 'by reason of any contravention by a data controller of any of the requirements of the Act.'⁴⁵³ This provision underpins the claim by linking the right to compensation directly to breaches of statutory obligations, a link that, as the preceding analysis of the compensation framework has established, is considerably more difficult to operationalise in practice than its statutory formulation suggests. The Supreme Court's treatment of the damage requirement in *Lloyd* is directly continuous with the remedial analysis undertaken in the preceding section. The Court confirmed that a statutory infringement alone does not constitute compensable damage, and that distress can only be compensated where one of the conditions in s 13(2) is satisfied.⁴⁵⁴ More fundamentally, the Court concluded that to sustain a damages award it must be demonstrated that Google unlawfully used personal data relating to the specific individual claimant and that this use resulted in damage to that individual, a requirement that, in the context of a representative action on behalf of millions of Safari users, the claim as pleaded was structurally incapable of satisfying. Without individualised evidence of these elements, the claim was, in the Court's terms, 'doomed to fail.'⁴⁵⁵

The implications of this outcome for the cookie consent framework, and for the broader data protection model evaluated in this chapter, are significant and deserve explicit articulation, building on the remedial analysis already undertaken. *Lloyd* demonstrates that breaches of

⁴⁵² Kenny Henderson and Alex Askew, 'Case Comment: *Lloyd v Google LLC* [2021] UKSC 50' (*UKSC Blog* 31 January 2022) <<https://uksblog.com/case-comment-lloyd-v-google-llc-2021-uksc-50/>>.

⁴⁵³ *Ibid.*, § 19.

⁴⁵⁴ *Ibid.*, § 92.

⁴⁵⁵ *Ibid.*, § 8.

online privacy at scale, facilitated by the circumvention of technical consent mechanisms, generate precisely the kind of diffuse, individualised harm that the current compensation framework is least equipped to remedy.⁴⁵⁶ The loss suffered by each individual Safari user was real, their browsing behaviour was tracked without consent, their personal data was processed unlawfully, and their informational autonomy was violated. The quantum of that loss, assessed on an individual basis, was insufficiently concrete and quantifiable⁴⁵⁷ to satisfy the damage threshold that s 13 of the DPA 1998, as interpreted by the Supreme Court, required. The result demonstrates that the larger the scale of the data protection violation, and the more it is facilitated by technical circumvention of consent mechanisms rather than targeted individual disclosure, the less effective the current compensation framework becomes as a mechanism for vindicating data subjects' rights.

This remedial gap has direct implications for the reform agenda considered in the following section. If the compensation framework cannot effectively address large-scale privacy violations, as *Lloyd* demonstrates, then the question of whether the Data (Use and Access) Act 2025's reforms to the current framework adequately address the structural conditions that make such violations both possible and practically unremedied becomes analytically urgent. As this thesis has argued throughout, the effectiveness of the UK data protection model cannot be assessed purely by reference to the formal adequacy of its legal provisions; it must be evaluated against the practical reality of how those provisions operate, and fail to operate, in the specific technological contexts within which personal data is most extensively and opaquely processed.

5.2.2 Reform of the UK GDPR under the Data Use (and Access) Act

⁴⁵⁶ John Hartshorne, 'The Standard of Liability in Claims for Misuse of Private Information' (2021) 13 *Journal of Media Law* pp 216-217.

⁴⁵⁷ *Ibid*, § 152, 153; see further in John Hartshorne, 'The Standard of Liability in Claims for Misuse of Private Information' (2021) 13 *Journal of Media Law* pp 216-217.

The DUAA's stated aim is to 'make the rules simpler ... encourage innovation ... [and] allow responsible data-sharing while maintaining high standards,'⁴⁵⁸ and the ICO confirms it amends, but does not replace, the core data-protection instruments, which provides incrementalism: easing compliance frictions (e.g., SAR proportionality; cookie carve-outs)⁴⁵⁹ while preserving the GDPR's architecture of principles, rights and accountability. By expanding lawful basis (recognised legitimate interests)⁴⁶⁰ and clarifying research uses (including commercial research and broad consent),⁴⁶¹ the DUAA continues the UK trend of treating data protection as an operational governance regime with its own toolkit, rather than a mere emanation of privacy. That shift strengthens data protection's institutional autonomy but heightens the need for robust safeguards and interpretive guidance to avoid rights dilution in practice. The litigation involving Clearview AI Inc.⁴⁶² is a striking example of this trend. The company, a provider of facial recognition software, faced a £7.5 million fine from the ICO for data protection violations. However, the First-tier Tribunal ultimately overturned the fine on jurisdictional grounds, holding that UK data protection law did not apply to services offered exclusively to foreign law enforcement agencies,⁴⁶³ which are the distinct challenges AI poses for data protection enforcement.

The DUAA also seeks in part to address these technological developments by introducing a more flexible framework for automated decision-making (ADM) under the UK GDPR.⁴⁶⁴

⁴⁵⁸ Data (Use and Access) Act 2025, (Legislation.gov.uk/2025) <<https://www.legislation.gov.uk/ukpga/2025/18>>; See Guidance, 'Data (Use and Access) Act Factsheet: UK GDPR and DPA' (GOV.UK/27 June 2025) <<https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa>>.

⁴⁵⁹ Ibid, Sections 75-78; section 104, Data subjects' rights.

⁴⁶⁰ Ibid, Section 70; Schedule 4, Lawfulness of Processing.

⁴⁶¹ Ibid, Section 67; Meaning of research and statistical purposes.

⁴⁶² *Clearview AI Inc v The Information Commissioner* [2023] UKFTT 00819 (GRC).

⁴⁶³ Ibid, § 153.

⁴⁶⁴ Data (Use and Access) Act, Section 80; Schedule 6, Automated decision-making.

While relaxing certain procedural requirements, the Act embeds mandatory safeguards, including obligations to provide individuals with information about significant automated decisions, mechanisms to contest such decisions, and avenues for human involvement where appropriate.⁴⁶⁵ At the same time, the Act clarifies timelines for subject access requests (SARs) by introducing ‘stop-the-clock’ provisions for complex cases,⁴⁶⁶ expands the lawful bases for processing through the introduction of ‘recognised legitimate interests,’⁴⁶⁷ and revises definitions relevant to scientific and commercial research.

This iterative relationship is of particular analytical importance in the context of the DUAA because the Act’s reforms do not operate on a blank slate. They intervene in a legal landscape already substantially shaped by judicial development, one in which the courts have, over the past two decades, acted not merely as interpreters of legislative provisions but as *de facto* gap-fillers, developing what might aptly be described as a ‘common law of technology’ in areas where statutory provisions have proved absent, ambiguous, or ill-adapted to the realities of data processing. Understanding the character and direction of this judicial development is therefore a precondition for evaluating whether the DUAA’s legislative reforms represent a coherent and effective response to the structural problems that judicial interpretation has identified, or whether they risk creating new ambiguities and new gaps that the courts will again be required to resolve.

The tort of misuse of private information did not emerge fully formed from that single decision but has been developed incrementally through a substantial and analytically rich body of

⁴⁶⁵ Ibid, section 80(1).

⁴⁶⁶ ICO, ‘For the Public - the Data Use and Access Act (DUAA) 2025 - How Does This Affect Me?’ (Ico.org.uk30 June 2025) <<https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-how-does-this-affect-me/>> accessed 14 August 2025.

⁴⁶⁷ See DUAA Section 70; Schedule 4, Lawfulness of Processing.

subsequent case law, each decision refining, extending, or qualifying the reasonable expectation of privacy standard in ways that have progressively shaped both the scope of tortious protection and the normative framework within which the UK GDPR's provisions are interpreted and applied. To move directly from *Campbell* to the recent judicial developments would be to elide a doctrinal trajectory of considerable sophistication, and it is that trajectory, traced through the key decisions between these landmarks, that provides the most accurate account of the judicial 'common law of technology' against which the DUAA's reforms must be evaluated.

*Mosley v News Group Newspapers*⁴⁶⁸ represented a further and particularly significant development, both doctrinally and remedially. Eady J's award of £60,000 in damages for the News of the World's covert filming and publication of the claimant's private sexual activities established that substantial damages are available for serious misuse of private information without proof of financial loss, a holding whose relationship with the data protection compensation framework has been examined in the preceding section. More significantly for present purposes, Mosley engaged directly with the question of whether a pre-notification requirement should be imposed, obliging the press to notify a subject before publishing private information, thereby enabling injunctive relief to be sought. Eady J declined to impose such a requirement as a matter of domestic law, and the ECtHR subsequently confirmed in *Mosley v United Kingdom* that Article 8 did not mandate pre-notification. The significance of this for the DUAA reform context is considerable: the absence of a pre-notification requirement means that the primary protective mechanism available to data subjects in respect of imminent privacy violations remains reactive rather than preventive, a structural limitation of the current protective architecture that the DUAA does not address, and that leaves data subjects whose

⁴⁶⁸ [2008] EWHC 1777 (QB).

personal information is about to be published or processed unlawfully without an effective prospective remedy under the statutory framework. The cumulative significance of this judicial trajectory for the evaluation of the DUAA's reforms is substantial and deserves explicit articulation. Each of the decisions traced above has identified, whether explicitly or implicitly, a structural gap or normative inadequacy in the legislative framework as it stood at the time of decision, and the courts have responded by developing the common law to fill that gap. The DUAA's reforms intervene in this context as a legislative attempt to address some of these inadequacies, but the preceding analysis raises serious questions about whether they do so with sufficient coherence, precision, and normative depth to displace the need for continued judicial gap-filling.

This dynamic extends beyond the misuse of private information into the broader regulatory framework governing the online information environment, and nowhere is this more apparent than in the litigation surrounding the OSA.⁴⁶⁹ The most significant challenge to date is *Wikimedia Foundation v Secretary of State for Science, Innovation and Technology*,⁴⁷⁰ in which the Wikimedia Foundation brought judicial review proceedings against the Secretary of State's decision to categorise Wikipedia as a Category 1 service under the OSA 2023. Category 1 status subjects a service to the Act's most onerous obligations, including enhanced transparency and freedom of expression duties under sections 19 and 20 of the OSA. The Foundation's challenge was grounded principally in the argument that the categorisation failed to adequately account for Wikipedia's unique operational character as a volunteer-edited,⁴⁷¹ non-commercial encyclopaedia, and that the imposition of Category 1 obligations constituted

⁴⁶⁹ Online Safety Act 2023 (Legislation.gov.uk2023) <<https://www.legislation.gov.uk/ukpga/2023/50>>.

⁴⁷⁰ *Wikimedia Foundation v Secretary of State for Science, Innovation and Technology* [2025] EWHC 2086 (Admin).

⁴⁷¹ *Ibid.*, §§ 71, 74.

a disproportionate interference with the freedom of expression rights of the Foundation and its users, contrary to Article 10 of the ECHR.⁴⁷²

The analytical relevance of *Wikimedia* to the data protection framework, and specifically to the evaluation of the DUAA's reforms. *Wikimedia* raises freedom of expression concerns that intersect directly with the data protection framework. Wikipedia's content moderation model is inseparable from its data processing practices, and the imposition of Category 1 OSA obligations on Wikipedia necessarily affects the data processing architecture through which its editorial functions are performed. *Wikimedia* therefore exemplifies the judicial role in adjudicating the tensions between privacy, freedom of expression, and regulatory imperatives that this section has identified as a defining characteristic of the current digital legal landscape. The Administrative Court's engagement with the proportionality of the OSA categorisation decision mirrors precisely the balancing exercise that courts undertake when weighing Articles 8 and 10, and that data regulators perform when assessing whether processing is proportionate to its stated legitimate purpose.

The DUAA also adjusts the ICO's structure and duties, with the regulator providing forthcoming guidance updates across the amended areas. The effectiveness of the reform thus depends not only on statutory text but on the ICO's interpretive choices (e.g., what counts as 'reasonable and proportionate' SAR searches; the contours of 'recognised legitimate interests') and on organisational uptake within the staggered commencement windows. The courts' reactive and often slow pace presents structural limitations. In a fast-moving technological environment, the lag between the emergence of a privacy harm and the eventual judicial resolution can leave extended periods of uncertainty. This structural limitation is illustrated by

⁴⁷² Ibid, §§ 124, 135.

Farley v Paymaster,⁴⁷³ decided in 2024, in which claims arising from alleged data protection violations were dismissed despite the alleged infringements having occurred years earlier. The case concerned the processing of personal data in the context of payroll and pension administration services, a processing context that, while less technologically dramatic than the platform-based data harvesting considered in *Lloyd v Google* or the search engine indexing at issue in *NT1 & NT2*, is of considerable practical significance given the volume and sensitivity of the financial and personal data processed by payroll and pension administrators on behalf of large numbers of data subjects. The claimants alleged that the defendant had processed their personal data in breach of the applicable data protection legislation, causing them damage and distress of the kind that the compensation framework examined in the preceding section is designed to remedy. The case, however, exposes an underappreciated paradox within that framework. The act of breach notification may itself generate the liabilities it is intended to address. Where a data controller discharges its obligation to notify affected individuals of a breach, that notification may foreseeably induce anxiety, distress, or other forms of non-material harm grounded in reasonable fears about the consequences of the breach.⁴⁷⁴ In *Farley*, a significant number of claimants indicated that it was precisely the receipt of notification letters, rather than any independently ascertained misuse of their data, that first gave rise to their concerns about identity theft and the potential for further harm.⁴⁷⁵

While the UK GDPR remains ‘almost verbatim’⁴⁷⁶ in relation to the EU GDPR, UK courts have signalled a departure from certain EU interpretations, notably through decisions suggesting that breaches of data protection law do not automatically confer a right to

⁴⁷³ *Farley v Paymaster* [2024] EWCA Civ 781.

⁴⁷⁴ See Georgia Grisaffe, ‘English Court of Appeal Rules on Compensation for Data Breaches - Cyber/Data/Privacy Insights’ (cyber/data/privacy insights 4 September 2025) <<https://cdp.cooley.com/english-court-of-appeal-rules-on-compensation-for-data-breaches/>> accessed 9 February 2026.

⁴⁷⁵ *Ibid.*

⁴⁷⁶ See *supra* chapters 3 and 4.

compensation. Such developments risk creating divergences from the case law of the CJEU, potentially undermining the UK's adequacy status, which is contingent upon maintaining 'essentially equivalent' levels of protection and is currently time-limited to June 2025. Civil society groups within the EU have already called for a reassessment of this status in light of the DUAA's provisions, particularly its expanded definitions and relaxed ADM framework.

The judiciary thus remains an indispensable mediator in balancing competing societal values in the digital age. Cases like *Bloomberg* exemplify the reconciliation of privacy rights under Article 8 of the ECHR with freedom of expression under Article 10, while disputes such as the Apple iCloud matter demonstrate the tension between privacy (and encryption) and national security or economic objectives. Although legislation such as the DUAA attempts to reconcile these competing interests, the ultimate calibration of rights and obligations often occurs in the courts, ensuring their continuing centrality in the governance of technology and privacy. In this sense, the development of UK data protection law is best understood as a cyclical and interactive process, in which legislative reform prompts judicial interpretation, which in turn informs further statutory evolution, a dynamic unlikely to diminish as technological innovation continues to test the limits of existing legal frameworks.

The Apple iCloud encryption dispute⁴⁷⁷ raises analogous concerns from a different direction, not the over-regulation of non-commercial platforms but the regulatory compulsion of commercial ones to undermine the encryption architecture upon which informational security depends. The Home Office's reported use of the Investigatory Powers Act 2016 to require Apple to create a backdoor capability in its Advanced Data Protection encryption system for

⁴⁷⁷ See Adrian Kingsley-Hughes, 'Why Apple's Disabling of iCloud Encryption in the UK Is Bad News for Everyone' (ZDNET25 February 2025) <<https://www.zdnet.com/article/why-apples-disabling-of-icloud-encryption-in-the-uk-is-bad-news-for-everyone/>> accessed 11 August 2025.

iCloud,⁴⁷⁸ a requirement Apple contested and which resulted in the withdrawal of end-to-end encryption for UK users, illustrates the fundamental tension between the state's surveillance imperatives and the data protection framework's requirement that personal data be processed securely and protected against unauthorised access under Article 5(1)(f) of the UK GDPR. This tension is one that the DUAA's reforms do not address, and its resolution, or non-resolution, will have direct and significant consequences for the practical informational security of UK data subjects whose personal data is stored on cloud platforms subject to competing regulatory demands from different jurisdictions. The Apple dispute confirms that the most consequential threats to informational privacy in the current digital environment arise not only from the unlawful conduct of private data controllers but from the structural conditions created by the interaction of multiple, imperfectly coordinated regulatory regimes, conditions that the DUAA, for all its ambition, does not adequately resolve.

5.3 The Enforcement of the GDPR in the UK and EU

This section will discuss the effectiveness of the current data protection model in the UK through an analysis of 2 aspects: 1) effectiveness of the current data protection model, including in particular the impact of the GDPR on data protection practices in the UK; 2) challenges and loopholes in the implementation of the current data protection model.

5.3.1 Use of fines as an aspect of enforcement

⁴⁷⁸ See Ioannis Kouvakas, 'You Can't Have Your Apple and Eat It Too: Decryption Orders and the Perilous Future of U.K. Data Adequacy', U.K. Const. L. Blog (13th March 2025) (available at <https://ukconstitutionallaw.org/>).

As Lynskey has observed, the regulatory model is designed not only to compensate but to deter and prevent systemic infringements.⁴⁷⁹ The significance of escalating fines⁴⁸⁰ lies not in the fines *per se*, but in what they reveal about the regulatory priorities and the effectiveness of data protection law compared with MPI. The argument advanced here is therefore that fines, should not be understood merely as punitive, but as part of a deterrence-oriented governance model.

Moreover, as Moreham argues, the tort of misuse of private information serves an individualised compensatory purpose, for the loss of privacy itself.⁴⁸¹ The remedial logic of the tort exposes important limitations. The ongoing embarrassment and psychological harm suffered by claimants prior to trial cannot be adequately addressed through *ex post* damages alone, since financial compensation delivered after the event fails to arrest the continuing harm at its source; there is no guarantee that a defendant will possess the financial capacity to satisfy an award of damages.⁴⁸² Nonetheless, the imposition of fines, while symbolically and economically significant, raises fundamental questions regarding their actual efficacy in protecting individual privacy. Fines, though often substantial, may fail to capture the full scope of harm incurred through personal data breaches. The reputational damage and psychological distress experienced by data subjects are often irreparable, and monetary compensation, where available, is seldom sufficient to redress the dignity-based harms occasioned by privacy violations.⁴⁸³ Thus, the efficacy of fines as a means of enforcement of the GDPR in truly protecting personal information held by such companies remains to be seen. It responds to

⁴⁷⁹ See Orla Lynskey, 'Complete and Effective Data Protection' (2023) 76 *Current Legal Problems* 297 <<https://academic.oup.com/clp/article/76/1/297/7304257>>; p 317.

⁴⁸⁰ See CMS, 'GDPR Enforcement Tracker - List of GDPR Fines' (www.enforcementtracker.com2025) <<https://www.enforcementtracker.com/?insights>>; by Aug 2025, supervisory authorities had issued 2,578 fines, with cumulative penalties exceeding €6 billion.

⁴⁸¹ See N.A. Moreham, *Compensating for Loss of Dignity and Autonomy in the Misuse of Private Information Tort* (December 20, 2017). in 'Remedies for Breach of Privacy' Varuhas & Moreham eds (2018, Hart Publishing), Victoria University of Wellington Legal Research Paper No. 6/2019, Available at SSRN: <https://ssrn.com/abstract=3091461>, pp 3, 25.

⁴⁸² *JRV & Anor v BRG* (Re Injunction) [2023] EWHC 2238 (KB), § 41.

⁴⁸³ *Ibid*, § 41.

privacy violations after they have occurred, after the harm has been sustained, and after the data subject's informational autonomy has already been compromised. As a mechanism for incentivising prospective compliance, its effectiveness depends on the assumption that the prospect of financial penalty is sufficient to alter the behaviour of data controllers, an assumption that the conduct of major technology platforms, which have absorbed substantial GDPR fines as a cost of doing business without materially changing their data processing practices, gives considerable reason to doubt.

The question of what alternative or complementary mechanisms might more effectively protect individual privacy is therefore practically urgent, and it is one that the DUAA's reform agenda has addressed only partially and insufficiently. Several alternatives and supplements to the fine-based model merit serious consideration, each addressing a different dimension of the structural inadequacy identified above. The most immediately promising alternative is the development of a more robust and accessible regime of individual compensation, one that closes the remedial gap identified in the preceding analysis of *Lloyd v Google* and *Gulati* by enabling data subjects to recover meaningful compensation for non-material harm, including loss of control and dignitary injury, without the prohibitive burden of individualised damage proof that the Supreme Court's decision in *Lloyd* currently imposes. This could be achieved through legislative reform of the damage threshold under s 168 of the DPA 2018, aligning it more closely with the loss of control damages recognised under the tort following *Gulati*, or through the development of a statutory small claims or collective redress mechanism that makes compensation practically accessible to data subjects who have suffered privacy violations at scale.

5.3.2 Evaluation of the effectiveness of the current data protection model, centred on the impact of the GDPR

With Brexit, the UK's legal framework for privacy rights in relation to information now operates under three main protective systems: statutory data protection legislation, human rights protections, and tort law.⁴⁸⁴ The GDPR has had and is having a relatively profound impact on data protection practices in the UK, influencing regulatory compliance, international data transfers, regulatory enforcement, and organisational culture.⁴⁸⁵ Section 100 of the DPA 2018 enshrines the right to 'rectification and erasure,' for purposes of Part 4, Intelligence Services Processing.⁴⁸⁶ Erasure arises as a general right of the data subject under Art. 17 UK GDPR; s.47 also reflecting the incorporating of Article 17(1) of the GDPR's 'right to erasure' into UK law.

Strasbourg emphasises that respect for 'private life' under Article 8 ECHR is a broad concept, inherently open-ended and not exhaustively defined.⁴⁸⁷ This leaves room for a variety of information to potentially meet the initial threshold for protection. The HRA 1998⁴⁸⁸ constrains the domestic reach of Article 8 ECHR, by virtue of s.6, only public authorities are directly bound, with the result that its application in private disputes depends on judicial mediation. Although the restrictive stance in *Wainwright v Home Office*⁴⁸⁹ declined to recognise a

⁴⁸⁴ Stergios Aidinlis, 'The Right to Be Forgotten as a Fundamental Right in the UK after Brexit' (*Ssrn.com* 9 March 2020) <<https://ssrn.com/abstract=3554625>>, p 8.

⁴⁸⁵ Oluwatosin Reis and others, 'Privacy Law Challenges In The Digital Age: A Global Review Of Legislation And Enforcement' (2024) 6 *International Journal of Applied Research in Social Sciences* 73 <<https://www.fepbl.com/index.php/ijarss/article/view/733>>, p 79.

⁴⁸⁶ *Ibid*, pp 8-9.

⁴⁸⁷ Ben Gallop, Lily Walker-Parr of 5RB and Daniel Bishop, 'Privacy Law-Misuse of Private Information Produced in Partnership with Ben Gallop and Lily Walker-Parr of 5RB and Daniel Bishop' (2021) <<https://www.5rb.com/wp-content/uploads/2021/09/Privacy-law%E2%80%94misuse-of-private-information.pdf>>, p 3.

⁴⁸⁸ Article 8 of the HRA 1998, Schedule 1, Part I.

⁴⁸⁹ *Wainwright v Home Office* [2003] UKHL 53.

standalone tort of invasion of privacy, the House of Lords in *Campbell*⁴⁹⁰ demonstrated that Article 8 can exert indirect horizontal effect, reshaping the common law of misuse of private information.⁴⁹¹ At Strasbourg and domestically, while ‘private life’ can cover more than strictly personal matters, it generally excludes certain aspects of an individual’s business or professional activities, as well as some leisure pursuits conducted in public. Thus, only selected personal aspects fall within this protected sphere, focusing primarily on information where privacy can be deemed to be genuinely warranted because the information relates to sensitive matters or day-to-day activities as aspects of an individual’s personal, as opposed to public life.⁴⁹² Both data protection and MPI reflect Article 8 principles.

In *NT1 and NT2*,⁴⁹³ the High Court provided its first interpretation of the ‘right to be forgotten’ under UK data protection law but based on such law prior to the inception of the GDPR; the case therefore foreshadowed the inception of Art. 17. The court ordered Google to delist search results related to the spent conviction of a businessman known as ‘NT2’ but rejected a similar request from another businessman, ‘NT1,’ even though both had previous criminal convictions. In reaching these differing outcomes, the court carefully weighed the public interest against the claimants’ right to privacy, particularly in relation to the impact of the spent convictions on their personal and professional lives.⁴⁹⁴

⁴⁹⁰ [2004] UKHL 22.

⁴⁹¹ See Gavin Phillipson, ‘Privacy: The Development of Breach of Confidence – the Clearest Case of Horizontal Effect?’ [2011] In: Hoffman D, ed. *The Impact of the UK Human Rights Act on Private Law*. Cambridge University Press eBooks 136, pp 137-139.

⁴⁹² See eg *Von Hannover* [2004] EMLR 379, *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22 at §§ 17, 51, further cases *Weller v Associated Newspapers Limited* [2014] EWHC 1163 (QB) and *Copland v United Kingdom* (App 62617/00) [2007] ECHR 62617/00 under Art 8 at both Strasbourg and in the UK.

⁴⁹³ [2018] EWHC 799 (QB).

⁴⁹⁴ [2018] EWHC 799 (QB), §§ 37, 38; the Court relied both on *Google Spain* and the EU Working Party’s guidelines on its application.

The GDPR/DPA has clearly had an important impact on data protection practices in the UK. It brought about a heightened awareness of data protection responsibilities among businesses operating in the UK. Many organisations and individuals had to review and revise their data protection policies, procedures, and systems to comply with the stringent requirements of GDPR.⁴⁹⁵ Despite initial challenges, UK businesses and public bodies have adapted to DPA/GDPR requirements, recognising the importance of data protection in fostering consumer trust.⁴⁹⁶ It fosters a culture of accountability, transparency, and heightened protection of individuals' privacy rights.⁴⁹⁷ Comprehensive information on the ICO's application of their formal GDPR enforcement powers is however somewhat scarce and can be challenging to interpret consistently.⁴⁹⁸ The last four ICO annual reports cover the full-time period up to the end of 2025, but the information they provide is limited and extremely low (often single digit) enforcement figures.⁴⁹⁹ The reports document a gradual but uneven increase in the use of formal enforcement powers, including monetary penalty notices, enforcement notices, and information notices, over the four-year period, reflecting the ICO's stated commitment to a more proactive and risk-based enforcement approach articulated in its strategic framework 'ICO25'.⁵⁰⁰ However, the aggregate fines issued over this period remain modest relative to the scale of data protection violations occurring within the UK economy, and the distribution of enforcement action is heavily skewed toward particular sectors, mostly the public sector,

⁴⁹⁵ ICO, 'Essential Guide to the General Data Protection Regulation (GDPR)' [2018] Guide to the General Data Protection Regulation (GDPR) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>, p 4.

⁴⁹⁶ Ibid.

⁴⁹⁷ See Oluwatosin Reis and others, 'Privacy Law Challenges In The Digital Age: A Global Review Of Legislation And Enforcement' (2024) 6 International Journal of Applied Research in Social Sciences 73 <<https://www.fepbl.com/index.php/ijarss/article/view/733>>, pp 76, 79.

⁴⁹⁸ See David Erdos, 'Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government's Statutory Reform Plans' [2022] University of Cambridge Faculty of Law Research Paper No. 16/2022, p 8.

⁴⁹⁹ See David Erdos, 'The UK Information Commissioner's Annual Report 2024/25: Surveying a Systematic Trend Away from Adequate Enforcement', U.K. Const. L. Blog (22nd July 2025) (available at <https://ukconstitutionallaw.org/>).

⁵⁰⁰ 'ICO25 Strategic Plan' (Ico.org.uk 11 February 2025) <<https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-plan/>>.

financial services, and direct marketing, leaving significant areas of the data processing landscape, including the major technology platforms whose data processing practices pose the most systemic risks to informational privacy, comparatively underenforced.

David Erdos further argues that⁵⁰¹ a deeply entrenched internal culture of regulatory restraint, compounded by weak accountability mechanisms for data subjects, has significantly constrained the ICO's enforcement appetite. This has been reinforced by the current Information Commissioner's openly stated resistance to deploying the full range of powers available under the UK GDPR, illustrated by his decision in June 2022 to summarily reduce fines in the public sector, and by his assertion in November 2024, without clear supporting evidence, that neither high-value nor high-volume fines represent the most effective means of achieving regulatory impact. The ICO has also faced external pressure from Government, which has urged regulators to prioritise economic growth. In the ICO's case, however, rather than softening its regulatory posture in the name of growth, the ICO needs to do considerably more to fulfil its core statutory responsibility, the robust protection of personal data. The reports' own data on enforcement outcomes therefore provides empirical support for the structural critique developed in the preceding section that the current enforcement model, even as it has become more active, remains insufficiently targeted at the most consequential sources of data protection harm.

As discussed in Chapter 2, the UK accepted GDPR principles and standards in its domestic law as a member of the EU; they were supplemented by the provisions of the DPA 2018. This alignment ensured that data protection practices in the UK closely mirrored those of the EU,

⁵⁰¹ See David Erdos, 'The UK Information Commissioner's Annual Report 2024/25: Surveying a Systematic Trend Away from Adequate Enforcement', U.K. Const. L. Blog (22nd July 2025) (available at <https://ukconstitutionallaw.org/>).

facilitating seamless data flows between the UK and EU member states.⁵⁰² Post-Brexit, the UK continued to adhere to GDPR standards under the UK GDPR/DPA to maintain data adequacy. As explained in chapter 2, this meant that UK businesses handling the personal data of EU citizens needed to comply with GDPR requirements in order to ensure uninterrupted data flows between the UK and EU. Following Brexit, as mentioned in Chapter 3 previously, the UK became a ‘third country’ under the GDPR for EU purposes, impacting data transfer mechanisms. UK organisations needed to rely on mechanisms such as Standard Contractual Clauses (SCCs)⁵⁰³ or Binding Corporate Rules (BCRs)⁵⁰⁴ to transfer personal data from EU to the UK and vice versa.⁵⁰⁵ The UK ICO retained its authority to enforce GDPR standards within the UK under the UK GDPR.⁵⁰⁶ Moreover, the GDPR strengthened the rights of individuals regarding their personal data. As discussed in Chapters 2 and 3, it reminded persons as to their rights, provided an easier and clear way for individuals to safeguard their rights. This included the right to access their data, the right to erasure (or ‘right to be forgotten’, under Article 17).⁵⁰⁷ Moreover, it introduced stricter requirements for obtaining consent for data processing. Consent must be freely given, specific, informed, and unambiguous.⁵⁰⁸

The UK GDPR/the DPA have also catalysed a shift in organisational culture towards prioritising data protection and privacy, which has at times included the use of criminal law. For example, in relation to criminal law, Rachel Anderton, a former family intervention officer

⁵⁰² EU adopts ‘adequacy’ decisions allowing data to continue flowing freely to the UK, see it on <https://www.gov.uk/government/news/eu-adopts-adequacy-decisions-allowing-data-to-continue-flowing-freely-to-the-uk>.

⁵⁰³ Standard contractual clauses for data transfers between EU and non-EU countries; see *infra* pp 200-201.

⁵⁰⁴ Binding Corporate Rules (BCR) Corporate rules for data transfers within multinational companies.

⁵⁰⁵ Similarly, EU businesses transferring data to the UK had to ensure compliance with GDPR requirements.

⁵⁰⁶ Data Protection Act 2018, Chapter 3 ‘Application of the GDPR’ Sections 22; Part 5 The Information Commissioner, from the GDPR which arises under DPA; see further ICO Overview – Data Protection and the EU, on <https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/> 28 June 2021.

⁵⁰⁷ See Chapter 3, section 3.2; Chapter 4, section 4.5.1.

⁵⁰⁸ See Art. 4 GDPR Definitions Art. 6 GDPR Lawfulness of processing Art. 7 GDPR Conditions for consent, see further ICO guidance on What is valid consent 28 June 2021.

at a local council was sentenced for unlawfully accessing social services records.⁵⁰⁹ A council audit revealed that the defendant had unlawfully viewed the records of 145 individuals while employed in the social services department. The defendant pleaded guilty to one count of unlawfully obtaining personal data, in violation of s.170(1) of the DPA 2018.⁵¹⁰

This section has focused on the ICO's enforcement actions against organisations for data breaches and non-compliance with GDPR and other data protection laws in the UK. They serve as reminders of the importance of implementing robust data protection measures and the potential consequences of failing to adequately protect personal data. This section's consideration of enforcement illustrates that the GDPR/DPA has often been enforced robustly, and very high fines have often been levied, raising the profile of data protection, and encouraging individuals to vindicate their rights to data protection. However, the current regime is open to criticism, as discussed in the following section 5.3.3.

5.3.3 Examination of the challenges and loopholes in the implementation of the current personal data protection model

Rapid technological advancements, such as artificial intelligence, IoTs, and biometric data processing, present new challenges for data protection. These technologies may involve complex data processing activities, increasing the risk of privacy infringements and necessitating updates to existing regulations. The current data protection model, exemplified by frameworks like the GDPR in the EU and the UK GDPR/DPA 2018 as amended in the UK,

⁵⁰⁹ ICO Annual Report 23/24, Personal data breaches, p 41.

⁵¹⁰ See 'ICO Confirms Prosecution of Social Services Council Employee' (*Freevacy.com*2023) <<https://www.freevacy.com/news/ico/ico-confirms-prosecution-of-social-services-council-employee/4232>>.

has made relative strides in enhancing individuals' rights, as discussed.⁵¹¹ However, as indicated here, enforcement of data protection principles is usually dependent on the ICO which cannot handle all potential claims due to lack of resources. Injunctions are also not available under the GDPR/DPA, although the right of erasure is available.

Under the GDPR, individuals face higher thresholds for making claims, and in many cases, claims for violations of data protection laws and misuse of private information are often brought in the same lawsuit.⁵¹² Whether such precedents may reduce individuals' willingness to invoke the GDPR in legal action, potentially weakening the practical effectiveness of the GDPR in protecting personal data, remains a concern. In *Bekoe v Islington LBC*,⁵¹³ the court ruled that obtaining compensation for misuse of private information involves fewer obstacles than under the GDPR, explaining that claimants can receive damages for the loss or reduction of their ability to control their private information, even if no distress is caused.⁵¹⁴

On the other hand, some organisations view the risk of enforcement as relatively low compared to the potential benefits of non-compliance, leading to a lack of strong deterrence. The requirement to report data breaches promptly has highlighted challenges in identifying and assessing breaches effectively. In *Facebook and Cambridge Analytica*,⁵¹⁵ the unauthorised harvesting of personal data from millions of Facebook users by Cambridge Analytica, a political consulting firm, was found. The incident raised concerns about Facebook's data protection practices, including its failure to adequately safeguard user data and its role in

⁵¹¹ See David Erdos, 'The UK and the EU Personal Data Framework after Brexit: A New Trade and Cooperation Partnership Grounded in Council of Europe Convention 108+?' (2022) *Computer Law & Security Review* 105639, p 49.

⁵¹² For example, *Bekoe v Islington LBC* [2023] EWHC 1668 (KB).

⁵¹³ *Ibid.*

⁵¹⁴ *Ibid.*, § 65.

⁵¹⁵ [2019] EWHC 954 (Ch).

facilitating third-party access to personal information without users' explicit consent,⁵¹⁶ which illustrated the challenges of enforcing data protection regulations in the context of complex data ecosystems and highlighted the potential for exploitation of loopholes in data sharing and consent mechanisms.⁵¹⁷

To sum up, this section has considered the challenges inherent in implementing the current data protection model, including issues related to data breaches and consent mechanisms and inadequacies of enforcement. Addressing these challenges requires ongoing efforts to strengthen regulatory frameworks, especially the resourcing of the ICO, the enhancement of transparency and accountability mechanisms, which promote a deep culture of data protection and privacy compliance across industries and other data-handling bodies.

5.4 Impact of the GDPR on Protecting Private Information in the Context of the Celebrity Industry and the Privacy of 'Ordinary' People

This section considers specific cases, within the context of the current data protection model, in relation to difficulties inherent in protecting the private information of celebrities and of 'ordinary' persons where the media seeks to publish and collect such information. As discussed in Chapter 2, and above, the right to respect for private life and private correspondence is enshrined in Article 8 of the ECHR.⁵¹⁸ A legal framework is also provided by the UK GDPR/DPA 2018 for safeguarding private information, not only by commercial bodies

⁵¹⁶ Ibid, § 8, see also in Iga Kozłowska, 'Facebook and Data Privacy in the Age of Cambridge Analytica - the Henry M. Jackson School of International Studies' (*The Henry M. Jackson School of International Studies* 30 April 2018) <<https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/>>.

⁵¹⁷ See Granville, Kevin. 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens.' *The New York Times*. March 19, 2018. <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>.

⁵¹⁸ See Chapter 2, section 2.1.

generally, but in the media. These regulations establish principles for the lawful processing of personal data, which are discussed in detail in Chapter 4.⁵¹⁹ As discussed, they also grant individuals rights to access, rectify, and erase their personal data, empowering them to control how their information is used by the media.

While data protection laws aim to protect individuals' privacy, they can also pose challenges for investigative journalism. Journalists often encounter obstacles when accessing information for investigative reporting, particularly when it involves processing personal data.⁵²⁰ Balancing the public interest in investigative reporting with individuals' privacy rights requires careful consideration and adherence to legal and ethical standards.

5.4.1 Impact of the current personal data protection model on search engines, the media, including social media

In *Campbell v MGN Ltd*,⁵²¹ the issue of misuse of private information revolves around the tension between the qualified rights of Article 8 (right to respect for private life) and Article 10 (freedom of expression) of the ECHR.⁵²² The freedom of the press is closely linked to freedom of expression under Article 10. In cases involving the media, the primary focus is often on securing an injunction to prevent misuse of private information, typically aimed at stopping publication. The ECtHR has developed a sophisticated and evolving body of principles governing this balancing exercise, and their incorporation into domestic law through sections 6 and 12 of the HRA, which requires courts to have particular regard to the importance of

⁵¹⁹ See *supra* section 4.4.

⁵²⁰ See detailed in ICO Data Protection and Journalism code of practice, 07 2023, Part 4 Use personal information lawfully.

⁵²¹ [2004] UKHL 22, [2004] 2 AC 457.

⁵²² See Soumia Landi, Misuse of Private Information: A Legal Analysis of Privacy Precedent in Connection to Media Abuses in England and Wales [2023] the King's Student Law Review, Vol XIII, Issue II, p 2.

Article 10 when considering relief that might affect the exercise of that right, has directly shaped both the substantive and remedial dimensions of misuse of private information claims. The first and most foundational principle is that of proportionality, the requirement that any interference with a Convention right, whether by a public authority or through the horizontal application of Convention principles between private parties, must be proportionate to the legitimate aim pursued. In the context of misuse of private information, proportionality operates at two levels simultaneously; it governs the substantive question of whether the defendant's publication or disclosure was justified by a legitimate countervailing interest, and it governs the remedial question of whether the relief sought, particularly injunctive relief, represents a proportionate response to the privacy violation established. The ECtHR articulated this principle with particular clarity in *Axel Springer AG v Germany* and *Von Hannover v Germany (No. 2)*, where the Court identified a structured set of criteria for assessing proportionality in privacy cases involving the media, including the contribution of the publication to a debate of general public interest, the prior conduct of the person concerned, the content and form of the publication, and the severity of the sanction imposed. As the preceding analysis of these decisions has established, these criteria have been adopted and applied by UK courts in a manner that has progressively structured and disciplined the balancing exercise, though not always with the consistency and predictability that a principled framework demands.

The concept of a reasonable expectation of privacy also concerns; the threshold criterion that determines whether Article 8 is engaged at all. The Court developed this concept in *Von Hannover v Germany (No. 1)*, holding that Princess Caroline of Monaco had a reasonable expectation of privacy in respect of photographs taken of her in public spaces despite her status as a public figure, on the basis that the photographs contributed nothing to a debate of general

public interest and served only to satisfy public curiosity. It established that the reasonable expectation of privacy is not defeated merely by the public character of the location in which the information was obtained or the public status of the individual concerned, but must be assessed by reference to the specific nature of the information, the context of its acquisition, and the purpose served by its disclosure. The subsequent refinement of this principle in *Von Hannover (No. 2)*, where the Court upheld the publication of photographs of Princess Caroline on the basis that they accompanied an article on a matter of genuine public interest, confirmed that the reasonable expectation standard is contextually sensitive and fact-specific, resisting reduction to bright-line rules while demanding structured and principled analysis.

As the preceding analysis has established, this outcome reflects and deepens the remedial asymmetry between the tort and the statutory framework, and it has direct consequences not only for claimants against technology platforms but for all categories of data subject whose personal information is processed unlawfully at scale, including those whose data is mishandled by media in the course of journalistic activity. The GDPR includes exemptions for journalistic purposes to protect freedom of expression and the media's role in informing the public.⁵²³ Where the exemption does not apply, media organisations still need to balance the right to freedom of expression with individuals' right to privacy.⁵²⁴ This has led to debates and challenges around issues such as the publication of sensitive personal data, reporting on criminal proceedings, and the use of photographs and videos in news reporting.

This section extends that analysis by introducing a third legal framework, defamation, whose interaction with data protection law generates an equally significant and equally under-

⁵²³ GDPR, 'Art. 85 GDPR – Processing and Freedom of Expression and Information' (*General Data Protection Regulation (GDPR)2018*) <<https://gdpr-info.eu/art-85-gdpr/>>.

⁵²⁴ Ibid, Art. 85(2), also s. 178 of the DPA 2018 (which now codifies aspects of UK GDPR).

theorised set of overlapping rights, remedies, and causes of action. The analytical purpose of examining these three frameworks together is not to conflate them but to demonstrate that the protection of informational privacy in the current legal landscape operates across a complex, multi-framework architecture whose coherence and effectiveness cannot be assessed by examining any single regime in isolation. It is this multi-framework character of contemporary privacy protection, and the structural questions it raises about consistency, accessibility, and remedial adequacy, that provides the organising analytical thread running through the discussion that follows.

The starting point for understanding how these three frameworks interact in the media context is the constitutional and Convention framework within which all three operate. A free press is constitutionally vital, entrusted with what the ECtHR has consistently described as the function of a public watchdog,⁵²⁵ communicating information and ideas on matters of public interest in a manner that serves democratic accountability and transparency. This function is protected under Article 10 of the ECHR and reflected in the GDPR's journalistic exemptions, the qualified privilege defences available in defamation law, and the Article 10 weight accorded to press freedom in misuse of private information cases. However, as Mann J observed with analytical precision in *Cliff Richard v BBC*,⁵²⁶ a MPI case, the invocation of a press 'duty' in this context requires careful scrutiny. While the press undoubtedly performs a public function whose value the law must recognise and protect, Mann J argued that the concept of 'duty' does not automatically strengthen the media's case in the balancing exercise between Articles 8 and 10. His emphasis on the need for nuanced, fact-sensitive proportionality analysis rather than

⁵²⁵ *Axel Springer AG v Germany* (2012) 55 EHRR 6, § 79.

⁵²⁶ *Sir Cliff Richard v The BBC & The Chief Constable of South Yorkshire Police* [2018] EWHC 1837, [2018] 3 WLR 1715, § 274.

formulaic invocation⁵²⁷ of press freedom has implications that extend across all three legal frameworks under consideration, i.e. in misuse of private information cases, it structures the Article 8/10 balancing exercise; in data protection cases, it informs the assessment of whether the journalistic exemption under Schedule 2, Part 5 of the DPA 2018 is genuinely engaged; and in defamation cases, it conditions the weight to be accorded to public interest defences under s 4 of the Defamation Act 2013.

It is in this multi-framework context that *His Highness Prince Moulay Hicham Ben Abdullah Al Alaoui of Morocco v Elaph Publishing Limited*⁵²⁸ assumes its analytical significance, not merely as a case about the concurrent availability of defamation and data protection claims, but as a judicial recognition that the protection of informational integrity in the media context requires a legal architecture capable of addressing simultaneously the reputational, dignitary, and data processing dimensions of media-inflicted harm. The Prince pursued legal action both in defamation and under the DPA 1998 in relation to an article published by the defendant. At first instance, Mr Justice Dingemans held that the data protection claim was capable of constituting a real and substantial tort,⁵²⁹ meaning that the action was neither an abuse of process nor an impermissible interference with freedom of expression, thereby establishing that data protection claims arising from media publication are not inherently subordinate to, or displaced by, the defamation framework that has traditionally governed media liability for harmful publications. This holding is analytically significant because it resists the tendency, prevalent in both judicial reasoning and legal commentary, to treat data protection as a peripheral or supplementary cause of action in media cases where defamation is available,

⁵²⁷ See Soumia Landi, *Misuse of Private Information: A Legal Analysis of Privacy Precedent in Connection to Media Abuses in England and Wales*. [2023] *The King's Student Law Review*, Vol XIII, Issue II, p 5.

⁵²⁸ *HH Prince Moulay Hicham Ben Abdallah Al Alaoui of Morocco v Elaph Publishing Ltd* [2017] EWCA Civ 29.

⁵²⁹ *Ibid*, [2015] EWHC 2021 (QB), § 10.

affirming instead that the data protection framework addresses a legally distinct set of concerns whose independent vindication serves legitimate and proportionate aims.

When the case reached the Court of Appeal, Lord Justice Simon confirmed and deepened this analysis, holding that the DPA's provisions specifically seek to protect individuals from being unfairly and unlawfully subjected to distress,⁵³⁰ a formulation that connects the statutory data protection framework explicitly to the dignitary and psychological harm dimensions of privacy violation that the misuse of private information tort has developed through *Campbell* and *Gulati*. The remedial outcome in *Elaph* illustrates that the defendant agreed to correct the inaccurate personal data relating to the Prince, to erase that personal data, not to republish the article in future, and to pay damages, a package of remedies that combined the prospective protective function of erasure and non-republication undertakings with the compensatory function of damages in a manner that neither the defamation nor the misuse of private information framework alone could have achieved. The Supreme Court's subsequent refusal of permission to appeal confirmed that there is no objection in principle to claims being brought simultaneously in libel and under the DPA in respect of the same published material.⁵³¹

*Lachaux v Independent Print Ltd & Evening Standard Ltd*⁵³² illustrates with particular clarity the multi-framework character of media liability for harmful publications identified in the preceding analysis, and its significance for the present thesis extends beyond its immediate contribution to defamation law into the broader question of press responsibility for the accurate and fair processing of personal information. The claimant argued that articles published by the

⁵³⁰ Ibid, § 43; see also *Law Society v Kordowski* [2011] EWHC 3185 (QB), § 74.

⁵³¹ [2017] EWCA Civ 29; see further on Felicity McMahon, 'Supreme Court Refuses Permission in DPA/Libel Claim - 5RB Barristers' (5RB Barristers 31 July 2017) <<https://www.5rb.com/data-protection/supreme-court-refuses-permission-dpa-libel-claim/>>.

⁵³² *Lachaux v Independent Print Ltd and Evening Standard Ltd* [2019] UKSC 27.

defendants on their online platforms violated both his privacy and reputational rights, a dual framing that reflects precisely the concurrent engagement of the misuse of private information and defamation frameworks whose interaction this section has been concerned to analyse. The Supreme Court held that the articles were defamatory,⁵³³ affirming that serious harm to reputation under s 1 of the Defamation Act 2013 could be established by inference from the gravity of the defamatory meaning and the extent of publication, without the need for specific evidence of actual reputational damage in every case, a holding whose parallel with the data protection damage threshold debate examined in the preceding discussion of *Lloyd* is analytically instructive, if ultimately resolved in the opposite direction.

It is Nicklin J's judgment in *Lachaux*⁵³⁴ that provides the most analytically significant treatment of press responsibility within this context. Nicklin J engaged directly and critically with the proposition that journalists and professional publishers should be required to demonstrate not only that they held a reasonable belief that publication was in the public interest, but also how and with whom that belief was formed at the relevant time. He rejected any suggestion that this constitutes an unworkable, unreasonable, or judicially imposed standard⁵³⁵ that is beyond the realistic reach of professional publishers. Nicklin J further reasoned that, absent a clear justification for differential treatment, the law ought to strive for coherence across the publication torts.⁵³⁶ Given that the burden of establishing a public interest defence under s 4 of the Defamation Act 2013 rests with the defendant, a publisher seeking to demonstrate a reasonable belief that publication served the public interest will materially strengthen their prospects of success by producing contemporaneous records documenting the decisions taken at the time of publication. The proposition that the Court is not setting

⁵³³ Ibid, § 22.

⁵³⁴ *Lachaux v Independent Print Ltd and another* [2021] EWHC 1797 (QB).

⁵³⁵ Ibid, § 120.

⁵³⁶ Ibid, §§ 120-123.

unattainable standards is further supported by the fact that the current codes of both IPSO and IMPRESS already impose substantially equivalent requirements to those previously contained in the PCC Code of Practice.⁵³⁷ Even where a court ultimately disagrees with the journalist's assessment that publication was in the public interest, contemporaneous documentation will at least enable the publisher to demonstrate the reasoning and thought processes that informed the decision at the relevant time. Evidence of that editorial process is likely to be relevant, even if not necessarily determinative, to the court's assessment of editorial judgment under s 4(4) of the 2013 Act. Nicklin J's analysis establishes that the public interest defence is not merely a substantive legal threshold but a discipline that demands procedural rigour from professional publishers at the point of publication, not merely in retrospect.

In addition to legal requirements, adherence to ethical standards is essential for safeguarding private information in the press. Media groups often have their own codes of conduct and editorial guidelines that govern the responsible handling of personal data and sensitive information. In *Cliff Richard v BBC*,⁵³⁸ the editorial guidelines of the BBC (a form of self-regulation) provided that the BBC must consider the public interest in relation to the expectation of privacy of individuals.⁵³⁹ Self-regulatory bodies, such as the Independent Press Standards Organisation (IPSO)⁵⁴⁰ in the UK, oversee compliance with ethical standards and handle complaints from the public, but IPSO has often been criticised as a weak regulator. Cathcart has argued that the Royal Charter system offers journalists and publishers unparalleled protection against the chilling effects of legal threats from wealthy litigants, however, this level

⁵³⁷ Impress: The Independent Monitor for the Press CIC, see *infra* pp 185-186; Ibid.

⁵³⁸ [2018] EWHC 1837 (Ch).

⁵³⁹ BBC, 'BBC Editorial Guidelines' (2020) 1.3 <<https://www.bbc.co.uk/editorialguidelines/guidelinespara>>.

⁵⁴⁰ IPSO, 'Home' (Ipsos.co.uk2019) <<https://www.ipso.co.uk/>>.

of protection is not extended under IPSO.⁵⁴¹ Wragg's central contention⁵⁴² is that the binary framing of the press freedom debate, in which regulation is routinely presented as antithetical to a free press, is both intellectually impoverished and practically counterproductive. Effective press regulation, properly conceived, is not a threat to press freedom but a precondition for its legitimate exercise. A press that operates without meaningful accountability for the accuracy, fairness, and proportionality of its handling of personal information is one that abuses rather than exercises the constitutional protection that Article 10 affords.⁵⁴³ This argument resonates directly with Nicklin J's reasoning in *Lachaux*, examined above, and with Mann J's insistence in *Richard v BBC* that the invocation of a press 'duty' does not displace the need for nuanced proportionality analysis. Wragg critique of IPSO,⁵⁴⁴ established following the Leveson Inquiry as the primary self-regulatory body for the UK press, identifies it as an institution whose design reflects the press industry's interest in the appearance of accountability rather than its substance.

It is in this context of self-regulatory inadequacy that the ICO's Data Protection and Journalism Code of Practice⁵⁴⁵ assumes critical analytical significance, and it is a document whose absence from the preceding discussion represents a gap that this section now addresses directly. The Code, issued by the ICO under s 124 of the DPA 2018, provides detailed guidance on how the data protection framework applies to journalistic activity, and its content is directly relevant to the multi-framework analysis developed throughout this section. The Code makes clear that the journalistic exemption is not a blanket licence for unrestricted data processing in the name

⁵⁴¹ Brian Cathcart, 'Three Key Reasons Why the Royal Charter Is Better for Journalists than IPSO - Hacked Off' (*Hacked Off - A Campaign For A Free And Accountable Press* 13 August 2014)

<<https://hackinginquiry.org/three-key-reasons-why-the-royal-charter-is-better-for-journalists-than-ipso/>>.

⁵⁴² See Paul Wragg, *A Free and Regulated Press* (Bloomsbury Publishing 2020), pp 173-196.

⁵⁴³ *Ibid*, pp 136-168.

⁵⁴⁴ *Ibid*, pp 278-290.

⁵⁴⁵ See ICO, Data Protection and Journalism Code of Practice, [data-protection-and-journalism-code-202307.pdf](#).

of press freedom but a qualified accommodation of journalistic activity that requires, in each case, a genuine and proportionate public interest justification.

The underutilisation of the Code as an enforcement tool connects directly to the structural critique of the ICO developed in the preceding section. If the ICO's enforcement of the journalistic exemption framework is as limited and inconsistent as its broader enforcement record suggests, as the analysis of the last four annual reports has demonstrated, then the Code's practical contribution to the protection of personal information in the press context is substantially reduced, regardless of the sophistication of its substantive guidance. The Media Lawyers Association's intervention, though ultimately unsuccessful, in *Prince Moulay Hicham of Morocco*,⁵⁴⁶ arguing that the Court of Appeal's decision established a pathway to claim damages for reputational harm outside the traditional framework of libel law,⁵⁴⁷ illustrates the press industry's persistent resistance to the expansion of data protection liability in the media context.

5.4.2 *The right to be forgotten and injunctions*

Privacy injunctions are quite rare (only five out of the six proceedings for injunctions at the High Court that took place between January and June 2024 were successful and granted),⁵⁴⁸ and even if an individual has a legitimate expectation of privacy or a duty of confidence, material can still be published if there is an overriding public interest.⁵⁴⁹ This is commonly

⁵⁴⁶ [2017] EWCA Civ 29.

⁵⁴⁷ Felicity McMahon, 'Supreme Court Refuses Permission in DPA/Libel Claim - 5RB Barristers' (5RB Barristers 31 July 2017) <https://www.5rb.com/data-protection/supreme-court-refuses-permission-dpa-libel-claim/>.

⁵⁴⁸ See Accredited official statistics Civil Justice Statistics Quarterly: April to June 2024, 9.1, on <https://www.gov.uk/government/statistics/civil-justice-statistics-quarterly-april-to-june-2024/civil-justice-statistics-quarterly-april-to-june-2024#privacy-injunctions7>.

⁵⁴⁹ See the discussion of the injunction in the *PJS* case in the Supreme Court, [2016] UKSC 26, §§ 32, 33.

seen in stories concerning investigative journalists exposing corporate wrongdoing or politicians engaging in misconduct, such as breaching lockdown rules or being involved in scandals, where the public has a right to be informed. One notable instance was Financial Times journalist Madison Marriage's 2018 expose of harassment at The President's Club Charity Dinner, a men-only event at London's Dorchester Hotel.⁵⁵⁰ The public outrage that followed led to the charity's dissolution and the end of its events, highlighting the power of investigative journalism to spur accountability and reform.⁵⁵¹

Recent cases⁵⁵² concerning online privacy have highlighted the interplay between Article 17 of the GDPR, which provides for the 'right to erasure' (often referred to as the 'right to be forgotten'), and the use of injunctions to address privacy concerns.⁵⁵³ It invites reflection on whether a more innovative approach could harness the unique strengths of both mechanisms, while also questioning the extent to which their roles are truly distinct.⁵⁵⁴ A more flexible interpretation of Article 17 GDPR might allow it to function in a manner more akin to an injunction, thereby ensuring the effectiveness of the right to erasure. Such an approach could harmonise the relief available under data protection laws with that offered by tort remedies, fostering equivalence and closing gaps in the protection of privacy rights.⁵⁵⁵

When there is an overriding public interest, privacy injunctions cannot be obtained, either because liability cannot be established, or because the test for obtaining an injunction under

⁵⁵⁰ Madison Marriage, 'Men Only: Inside the Charity Fundraiser Where Hostesses Are Put on Show' (*Financial Times* 23 January 2018) <<https://www.ft.com/content/075d679e-0033-11e8-9650-9c0ad2d7c5b5>>.

⁵⁵¹ Ros Breese, 'Insurers Are Critical to Protecting Investigative Journalism' (*Tmhcc.com* 2024) <<https://www.tmhcc.com/en/news-and-articles/thought-leadership/insurers-are-critical-to-protecting-investigative-journalism>>.

⁵⁵² For example, *TU and RE v Google LLC* [2022] EUECJ C-460/20, a case concerning two claimants applying for the delisting of search results under Article 17 of the GDPR.

⁵⁵³ GDPR, 'Art. 17 GDPR – Right to Erasure ('Right to Be Forgotten') | General Data Protection Regulation (GDPR)' (*General Data Protection Regulation (GDPR)* 2013) <<https://gdpr-info.eu/art-17-gdpr/>>.

⁵⁵⁴ Fiona Brimblecombe and Helen Fenwick (note 320) p 467.

⁵⁵⁵ *Ibid.*

s.12(3) HRA is not met. A notable example is *AAA v Associated Newspapers Ltd*,⁵⁵⁶ where the Court of Appeal ruled that the story about Boris Johnson, then Mayor of London, having an adulterous affair and fathering a child was a matter of public interest, as voters were entitled to know about his conduct when assessing his suitability for high office. Similarly, many privacy injunction applications that caused a stir in the press in 2011 were unsuccessful, such as *Terry v Persons Unknown (Rev 1)*,⁵⁵⁷ where the court found that the claim was essentially a defamation claim disguised as a privacy matter and in any event enabled the media claim to prevail based on the public interest.

The remedy under data protection that most closely resembles the function of injunctions is the ‘right to be forgotten’ under Article 17 of the GDPR. However, this right is typically regarded as an *ex post facto* remedy, addressing the removal of personal data after it has been published, rather than preventing its publication in the first place.⁵⁵⁸ Consequently, its role is generally considered distinct from that of an injunction, which is inherently preventive and aimed at restraining an action before harm occurs. This distinction underscores the reactive nature of the right to erasure compared to the proactive protection afforded by injunctions.⁵⁵⁹ The right to erasure can be exercised by a data subject by directly contacting the data controller to request the deletion of their data. If the controller denies the request, the data subject can escalate the matter by challenging the refusal in court.⁵⁶⁰ This process was demonstrated under the previous legal framework in the case of *NT1 and NT2 v Google LLC*.⁵⁶¹

⁵⁵⁶ [2013] EWCA Civ 554.

⁵⁵⁷ [2010] EWHC 119 (QB).

⁵⁵⁸ Fiona Brimblecombe and Helen Fenwick (note 320) p 467.

⁵⁵⁹ Ibid, pp 467-468.

⁵⁶⁰ Ibid, p 470.

⁵⁶¹ [2019] Q.B. 344.

In *Stunt v Associated Newspapers*,⁵⁶² the Claimant unsuccessfully attempted to challenge s.32(4) of the DPA 1998, which effectively stays data subject claims related to processing for journalistic purposes if the material has not yet been published within the 24 hours before the relevant time. This provision continues under s. 176 of the DPA 2018. Although the case was referred to the CJEU, the Court of Appeal withdrew it after the Claimant failed to comply with a security for costs order, leading to the claim being struck out. As a result, the rule remains that any data subject claim brought against a journalist or publisher for a breach of data protection rights prior to publication will be stayed.⁵⁶³ Thus in effect injunctive relief is not available in data protection claims. While injunctions are often invoked for proactive removal of content, Article 17 erasures are reactive and address ongoing or imminent threats to privacy after material has become available. However, recent legal discourse suggests that there is potential to use these tools in complementary ways, maximising their effectiveness.⁵⁶⁴ For example, injunctions could provide interim relief, while disputes over erasure requests under Article 17 are resolved, or they could serve to enforce compliance with GDPR obligations where other remedies fall short.

This contrasts with the situation for MPI claims, where a claimant can apply for an interim injunction (and will be successful if s.12(3) HRA is satisfied) to prevent the publication or disclosure of private information without the claim being automatically stayed.⁵⁶⁵ When a court evaluates remedies, including injunctions, it is required to give special consideration to the significance of the Convention right to freedom of expression in cases involving ‘journalistic, literary, or artistic material.’⁵⁶⁶ This framework appears to be crafted to bolster the position of

⁵⁶² [2017] EWHC 695 (QB).

⁵⁶³ Ibid, §§ 97, 98.

⁵⁶⁴ Fiona Brimblecombe and Helen Fenwick (note 320) p 467.

⁵⁶⁵ *Stunt v Associated Newspapers Ltd* [2017] EWHC 695 (QB), §§ 46, 48.

⁵⁶⁶ See s. 12(3) HRA and Art. 85 of GDPR on journalistic material; see further Fiona Brimblecombe and Helen Fenwick, note (297) pp 478-479.

media claims in privacy disputes, reflecting a clear focus on media interests. Recent Strasbourg jurisprudence on Article 10 similarly emphasises the importance of media freedom, shaping the balance of weight given to such claims in legal proceedings.⁵⁶⁷ However, Arts 8 and 10 are to be viewed as of equal weight.

‘Reasonable expectation of privacy’ always becomes a crucial issue in dealing with celebrities’ cases. They often attract significant media attention and scrutiny, both from traditional media outlets and social media platforms. To pursue a claim for MPI, a claimant must establish a reasonable expectation of privacy in the information at issue. In *David Murray v Big Pictures UK*,⁵⁶⁸ the Court of Appeal held that: ‘the question whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case’.⁵⁶⁹ *M.L. and W.W. v Germany*⁵⁷⁰ prompted the ECtHR to deal explicitly with the right to be forgotten under Article 8. The ECtHR upheld the German courts’ decision in favour of freedom of expression, emphasising the importance of the public’s right to be informed about significant past events, which highlighted the value of historical research and the role of Internet archives in enabling access to information on these matters.⁵⁷¹ The ruling underscores the balance between privacy rights and the public interest in maintaining access to information for historical and informational purposes.⁵⁷² *Hurbain v Belgium*⁵⁷³ also conducted a balancing test (art.8, art.10 ECHR) and provided a significant clarification regarding the handling of ‘right to be forgotten’ requests directed at content providers, particularly in relation to media

⁵⁶⁷ Ibid, See further *Axel Springer AG v Germany* (2012) 55 E.H.R.R. 6; *Von Hannover v Germany* (No.2) (2012) 55 E.H.R.R. 15, §§ 38, 118.

⁵⁶⁸ *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446 (07 May 2008)

⁵⁶⁹ Ibid, § 36.

⁵⁷⁰ *Wegrzynowski and Smolczewski v Poland* App no 33846/07 (ECtHR 2013).

⁵⁷¹ Stergios Aidinlis, ‘The Right to Be Forgotten as a Fundamental Right in the UK after Brexit’ (*Ssrn.com* 9 March 2020) <<https://ssrn.com/abstract=3554625>>, p 10.

⁵⁷² Ibid, §§ 101- 115.

⁵⁷³ *Hurbain v Belgium* [2023] GC App. No(s). 57292/16.

archives.⁵⁷⁴ The Grand Chamber's approach closely mirrors the methodology applied in cases concerning the right to erasure under Article 17 of the UK GDPR.⁵⁷⁵

The Strasbourg Court⁵⁷⁶ outlined a principled framework for balancing the right to be forgotten: whether the publication contributes to a public interest debate, the applicant's public profile, their prior conduct, and the content, form, and consequences of the publication.⁵⁷⁷ Moreover, the two-part *Campbell*⁵⁷⁸ test is a key tool used in assessing the validity of privacy claims against the media in misuse of private information cases. The term 'misuse of private information' is somewhat misleading in this context, as it refers specifically to the act of taking private information and publishing it, rather than the general concept of misuse.⁵⁷⁹ The test balances the claimant's right to privacy with the freedom of expression of the media, and it is applied to determine whether the claimant's privacy has been infringed upon in a way that justifies legal protection, taking any public interest in the expression into account.⁵⁸⁰

In *Sir Cliff Richard v BBC*,⁵⁸¹ the BBC broadcast live footage of a police raid on Sir Cliff Richard's home as part of an investigation into historical sexual abuse allegations. Sir Cliff Richard sued the BBC for invasion of privacy, under MPI, arguing that the broadcast had violated his privacy rights and caused him significant distress. In 2018, the High Court ruled

⁵⁷⁴ Ibid, § 212- 254; it specified that the 7 criteria to be considered in balancing the competing interests in this case; see further in Mikel Anderez Belategi, 'The Right to Be Forgotten Concerning the Criminal Past: Developments in the Case Law of the European Court of Human Rights with Particular Reference to the Anonymisation of Digital Press Archives' [2024] Oñati Socio-legal Series, section 3.2 pp 14-17.

⁵⁷⁵ Harriet Ni Chinneide, '*Hurbain v Belgium*: Navigating the Intersection of Privacy and Press Freedom in the Digital Age - Strasbourg Observers' (*Strasbourg Observers* 3 October 2023) <<https://strasbourgothers.com/2023/10/03/hurbain-v-belgium-navigating-the-intersection-of-privacy-and-press-freedom-in-the-digital-age/>>.

⁵⁷⁶ *Satakunnan Markkinapörssi Oy v Finland* (2018) 66 EHRR 8, § 74.

⁵⁷⁷ For discussion, see Stergios Aidinlis, 'The Right to Be Forgotten as a Fundamental Right in the UK after Brexit' (Ssrn.com 9 March 2020) <<https://ssrn.com/abstract=3554625>>, p 11.

⁵⁷⁸ See the Court of Appeal in *Campbell v MGN Ltd* [2002] EWCA Civ 1373; [2003] Q.B. 633.

⁵⁷⁹ Soumia Landi, 'Misuse of Private Information: A Legal Analysis of Privacy Precedent in Connection to Media Abuses In' (2023) <<https://blogs.kcl.ac.uk/kslr/files/2023/08/Soumia-Landi-.pdf>>, p 9.

⁵⁸⁰ Ibid.

⁵⁸¹ *Richard v The British Broadcasting Corporation (BBC) & Anor* [2018] EWHC 1837 (Ch).

in Sir Cliff Richard's favour, awarding him damages and criticising the BBC for its breach of privacy. In *PJS*,⁵⁸² the Supreme Court ruled that during the balancing exercise for interim injunctions, the rights to privacy and freedom of expression should be treated as having equal importance, even in light of s. 12(4).⁵⁸³ The Court also determined that a public interest argument with minimal value, such as using privacy invasion to stimulate public debate about anti-social behaviour, was insufficient to prevent the granting of an injunction.⁵⁸⁴ Additionally, Lord Mance held that 'kiss and tell' stories hold no public interest value.⁵⁸⁵

These two cases explain 'public interest' from different perspectives. From the outcome, it appears that injunctive relief still remains effective in protecting personal privacy in the traditional media. Placing a greater burden on individual data subjects, in the context of increasing datafication and data aggregation by major internet corporations, risks undermining the 'practical' and 'effective' protection of the right to be forgotten in the UK. As large tech companies collect and combine vast amounts of personal data, expecting individuals to manage and assert their rights on their own could lead to limited or ineffective protection of their privacy. Without sufficient safeguards and support, 'the right to be forgotten' may become less accessible, particularly for individuals who lack the resources or knowledge to navigate the complexities of data protection laws.⁵⁸⁶ It may be concluded that both Art 17 and injunctions play a part in ensuring protection for private information, but in a somewhat patchy, inconsistent fashion.

⁵⁸² *PJS v News Group Newspapers Ltd* [2016] A.C. 1081 §§ 20, 33.

⁵⁸³ See s. 12(4) HRA; see also Fiona Brimblecombe and Helen Fenwick (note 320) p 479.

⁵⁸⁴ Human Rights Act 1998 c. 42 s. 12 Freedom of expression.

⁵⁸⁵ [2016] A.C. 1081, § 15, §§ 22-24.

⁵⁸⁶ See Stergios Aidinlis, 'The Right to Be Forgotten as a Fundamental Right in the UK after Brexit' (Ssrn.com9 March 2020) <<https://ssrn.com/abstract=3554625>>, p 24.

5.4.3 The legal ramifications and ethical considerations surrounding the media exploitation of private information

This sub-section examines the exploitation of private information in the celebrity media industry, analysing both the data protection framework and the tortious remedies available to those whose private information has been wrongfully disclosed or processed. In doing so, it adopts a Kantian ethical framework as an analytical lens through which the normative foundations of those remedies,⁵⁸⁷ and their structural adequacy as mechanisms for vindicating the rights of individuals whose private information has been exploited, can be most clearly evaluated. As this section argues, the Kantian perspective illuminates structural inadequacies in the current remedial architecture that purely doctrinal analysis tends to obscure, and it provides the normative vocabulary through which the gap between the law's formal commitments and its practical outcomes in the celebrity privacy context can be most precisely articulated.

Drawing on Kant, Wragg⁵⁸⁸ argues that an individual's vitality, equality, and humanity are fundamentally undermined whenever they are treated as a means to another's ends rather than as an end in themselves. On this account, unjustified invasions of privacy are not merely technical wrongs but are inherently demeaning of individuality. They threaten the formation and continuity of personal relationships, and they damage the individual's foundational sense of self, the conviction that one belongs to oneself, and is not the property of another person or of the wider community. This Kantian framing is significant precisely because it grounds privacy protection not in consequentialist calculations about harm, but in the deeper moral

⁵⁸⁷ Nick Sage, Relational Wrongs and Agency in Tort Theory [2021] *Oxford Journal of Legal Studies* Volume 41, Issue 4, p 1013, <https://doi.org/10.1093/ojls/gqab009>.

⁵⁸⁸ See Paul Wragg, 'Recognising A Privacy-Invasion Tort: The Conceptual Unity of Informational and Intrusion Claims' (2019) 78 *The Cambridge Law Journal* 409, p 426.

imperative to respect persons as autonomous agents possessed of inherent dignity. It thereby provides a principled basis for evaluating whether the law's current remedial responses adequately honour the values they purport to protect.

Kantian ethics, in their most foundational formulation, are grounded in the categorical imperative, the requirement that individuals be treated always as ends in themselves and never merely as means to an end.⁵⁸⁹ Applied to the exploitation of private information, this principle generates that where a media organisation publishes, processes, or commodifies the private information of a celebrity, or indeed of any individual, for the purpose of generating commercial profit, audience engagement, or competitive advantage, it treats that individual instrumentally, as a resource to be exploited rather than as a person whose dignity and autonomy command unconditional respect. The reasonable expectation of privacy standard that *Campbell* established, and that the ECHR's Article 8 jurisprudence underpins, is itself grounded in a conception of individual dignity and autonomy that resonates deeply with Kantian moral philosophy. The legal protection of private information is, on this reading, an expression of the law's commitment to treating individuals as ends in themselves whose informational autonomy cannot be violated without justification, accountability, and remedy.

The application of Kantian principles to tort remedies generates a specific and demanding standard against which the current remedial framework must be evaluated. Under Kantian ethics, the purpose of remediation is not merely to compensate the victim for the measurable consequences of the wrong but to restore the moral relationship between the parties that the wrongful conduct has disrupted, affirming the victim's status as an end in themselves whose

⁵⁸⁹ Ibid, pp 1015, 1017.

rights have been violated, and holding the wrongdoer accountable⁵⁹⁰ in a manner that acknowledges the intrinsic wrongfulness of their conduct rather than merely its consequences.

Assessed against this Kantian standard, the current remedial framework reveals significant structural inadequacies that the doctrinal analysis of the preceding sections has identified but not fully explained in normative terms. The compensatory damages model, whether under the tort of misuse of private information or the statutory data protection framework, focuses on the harm suffered by the claimant and seeks to restore them, so far as money can, to the position they would have occupied had the wrong not occurred. This consequentialist orientation is not without value, the recognition in *Gulati* that loss of control over private information constitutes independently compensable harm represents a significant step toward a more dignity-centred remedial approach, but it remains insufficient from a Kantian perspective because it treats the wrong as significant primarily by reference to its effects rather than its nature.

The exploitation of private information in the celebrity industry raises these concerns⁵⁹¹ with particular acuity, because it is in this context that the commercial incentives to treat individuals as means to ends are most powerful, most organised, and most resistant to the deterrent effects of the current remedial framework. The cases examined in the following analysis, drawn from both the tort and the data protection statutory context, will be evaluated through both the doctrinal lens established in the preceding chapters and the Kantian normative standard developed in this section, assessing whether the remedies awarded and the accountability imposed are adequate, in the fullest moral sense of that word, to the dignitary wrongs

⁵⁹⁰ Ibid, p 1018.

⁵⁹¹ See Gemma Horton, Celebrities' families and privacy: the need for enhanced self-regulatory protection. [2022] Communications Law: Journal of Computer, Media and Telecommunications Law, 27 (1). pp 33-35

occasioned by the systematic exploitation of celebrity private information in the current media environment.

a) Legal ramifications

As discussed in chapters 2 and 3, in jurisdictions such as the UK, individuals have a legal right to privacy that protects them from the unauthorised disclosure of private information, under MPI and data protection. Exploiting private information without consent can constitute a breach of such laws, and result in legal action including financial penalties. Since the HRA 1998 came into effect in 2000, individuals can assert these rights in UK courts under Article 8, against public authorities. MPI and data protection reflect the principles underpinning Articles 8 and 10 ECHR. However, both are qualified rights, meaning they can be restricted in certain circumstances. For instance, if a story serves the public interest, a judge might decide that a celebrity's right to privacy should be limited to further the greater purpose of public interest.⁵⁹²

Press regulation in the UK operates through two distinct self-regulatory frameworks whose coexistence reflects the fractured and contested state of press governance that has persisted since the Leveson Inquiry's recommendations were only partially implemented. The majority of national and regional press publishers are bound by the Editors' Code of Conduct ('the Code')⁵⁹³ enforced by the IPSO, while a smaller group of publishers, predominantly independent and online outlets, are regulated by IMPRESS,⁵⁹⁴ the only press regulator to have

⁵⁹² See eg *AAA v Associated Newspapers* [2013] EWCA Civ 554, the claimant was awarded £15,000 for breach of her right of privacy by repeated publication of the photograph, but no damages for publication of the private information, and no injunction.; see further Simon Carne, 'In Defence of Privacy and the Judiciary: The Fall-out from *HRH the Duchess of Sussex v Associated Newspapers* – Iain Wilson' (*Inform's Blog* 8 February 2022) <<https://inform.org/2022/02/08/in-defence-of-privacy-and-the-judiciary-the-fall-out-from-hrh-the-duchess-of-sussex-v-associated-newspapers-iaain-wilson/>>.

⁵⁹³ IPSO, 'Editors' Code of Practice' (Ipsos.co.uk 1 January 2025) <<https://www.ipso.co.uk/editors-code-of-practice/>>.

⁵⁹⁴ Impress: The Independent Monitor of the Press (Impress) <<https://www.impressorg.com/>>.

been recognised under the Royal Charter on Self-Regulation of the Press established following Leveson.

Under the IPSO framework, press publishers are bound by the Editors' Code of Conduct, a document whose drafting and revision is controlled by the Editors' Code of Practice Committee, a body dominated by senior editors from the regulated industry itself. The Code provides that interferences with privacy may be justified in the public interest, but editors are expected to demonstrate this justification and to show how they reasonably believed that publication would serve and be proportionate to the public interest,⁵⁹⁵ a requirement whose language resonates with the proportionality analysis demanded by the ECtHR in *Axel Springer and Von Hannover (No. 2)*, and with the nuanced balancing exercise that Mann J articulated in *Richard v BBC* and Nicklin J in *Lachaux*. The court is obliged to have regard to the Code under s 12(4)(b) of the HRA 1998 when considering whether to grant relief that might affect the exercise of the Convention right to freedom of expression, a provision that formally incorporates the self-regulatory framework into the judicial balancing exercise while stopping well short of making compliance with the Code determinative of the legal outcome.

The IMPRESS framework operates on a materially different basis and merits explicit comparative analysis. As the only Royal Charter recognised regulator, IMPRESS operates under a framework designed to give effect to the core Leveson recommendations, including genuine independence from the regulated industry, a robust and accessible arbitration scheme, and meaningful sanctions for serious regulatory breaches. IMPRESS's Journalism Code and accompanying guidance address the relationship between journalistic activity and individual

⁵⁹⁵ Clause 3 of the current IPSO Code; see eg *HRH the Duchess of Sussex v Associated Newspapers Ltd* [2021] EWCA Civ 1810, § 32.

rights, including privacy, in a manner that is both more prescriptive and more rights-centred than the IPSO Editors' Code. From the Kantian perspective developed in this section, the voluntary and industry-controlled character of the IPSO framework, and the major publishers' refusal to join the Royal Charter recognised IMPRESS scheme, reflects precisely the institutional resistance to meaningful accountability that the Kantian analysis identifies as morally objectionable that an industry that systematically treats individuals' private information as a commercial resource while simultaneously resisting the regulatory frameworks that would hold it genuinely accountable for doing so.

In cases involving celebrity stories or photographs, Art 8 protecting privacy and Art.10 guaranteeing freedom of expression frequently come into conflict, as discussed in Chapter 1.⁵⁹⁶ As both rights hold equal legal weight, finding a balance between them can be challenging. In jurisdictions governed by data protection laws, such as the UK GDPR, the unauthorised processing and disclosure of personal data, including information about celebrities, could result in legal consequences, subject to free speech claims. There are also instances where private information of ordinary individuals has been exposed in the media or otherwise misused without consent in breach of the GDPR, where public interest issues are not relevant. For example, *TalkTalk*,⁵⁹⁷ a telecommunications company in the UK, experienced a significant data breach in 2015, compromising the personal information of approximately 157,000 customers. The breach included names, addresses, phone numbers, and financial information. The incident resulted in a £400,000 fine imposed by the ICO for breaches of data protection laws. The judgment reinforced the limitations faced by claimants in pursuing MPI tort claims in cases

⁵⁹⁶ See *supra* p 28.

⁵⁹⁷ *Smith v TalkTalk Telecom Group Plc* [2022] EWHC 1311.

involving cyber-attacks and third-party misuse, even when a company's security failure plays a role in enabling the fraud committed by third parties.⁵⁹⁸

b) Ethical considerations

Media groups bear both a moral and legal responsibility to respect the privacy and dignity of individuals, including celebrities, a responsibility whose content is articulated in the regulatory codes examined in the preceding section and whose enforcement through both self-regulatory and statutory mechanisms has been found, throughout this analysis, to be structurally inadequate. IPSO's Editors' Code and Ofcom's Broadcasting Code each set out these responsibilities in detail,⁵⁹⁹ establishing the framework within which the public interest justification for privacy-invasive publication must be assessed. However, the adequacy of these frameworks in practice, and the normative coherence of the public interest justifications most frequently invoked in the celebrity privacy context, demands critical scrutiny that goes beyond their formal provisions.

The exploitation of private information for sensationalism or entertainment value causes harm to individuals' well-being and undermines their right to privacy in a manner that is difficult to reconcile with the proportionality requirements established by the ECtHR in *Axel Springer* and *Von Hannover*, or with the Kantian moral framework developed in the preceding section. The right to be forgotten under Article 17 of the UK GDPR provides one important mechanism through which the ongoing harm of accessible private information can be addressed, Google

⁵⁹⁸ Ibid, § 62.

⁵⁹⁹ IPSO, 'Editors' Code of Practice' (*Ipsa.co.uk* 1 January 2021) <<https://www.ipso.co.uk/editors-code-of-practice/>>, see also Ofcom, 'The Ofcom Broadcasting Code (with the Cross-Promotion Code and the on Demand Programme Service Rules)' (*www.ofcom.org.uk* 12 June 2023) <<https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-standards/broadcast-code/>>.

has faced numerous legal challenges⁶⁰⁰ regarding the implementation of this principle, as the preceding analysis of *Google Spain* and *NT1 & NT2* has established, and the challenge of balancing erasure rights against freedom of expression and access to information.⁶⁰¹

It is in this context that the role model rationale, one of the most frequently invoked and analytically problematic justifications for the publication of celebrity private information, requires careful and sustained critical examination. The argument, advanced periodically by press and their legal representatives, is that celebrities forfeit a degree of their privacy by virtue of their status as public role models,⁶⁰² and that the press therefore performs a legitimate public interest function by exposing immoral or hypocritical behaviour that contradicts the positive image such individual project. On this view, the celebrity who presents themselves as a devoted family member while conducting an extramarital affair, or who publicly advocates healthy living while privately engaging in substance abuse, has, by constructing and trading upon a false public persona, implicitly consented to scrutiny of the private conduct that contradicts it, or at least reduced their reasonable expectation of privacy in respect of that contradiction.

This rationale has been subjected to sustained and persuasive critical scrutiny⁶⁰³ in both the case law and the scholarly literature, and the weight of that scrutiny strongly favours its rejection as a general principle capable of justifying privacy-invasive publication. Hughes has identified that there is no credible evidence to suggest that a celebrity's private behaviour

⁶⁰⁰ See *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* Case [2014] C-131/12 and also *Google LLC v Commission nationale de l'informatique et des libertés* (CNIL) [2019] Case C-507/17.

⁶⁰¹ See the case of *NT1 & NT2 v Google LLC* [2018] EWHC 799 (QB), discussed *supra* pp 119-121, which arose under the previous data protection regime but illustrates the difficulties inherent in balancing Arts. 8 and 10 concerns in the context of data protection.

⁶⁰² See Gemma Horton, *Celebrities' families and privacy: the need for enhanced self-regulatory protection*. [2022] *Communications Law: Journal of Computer, Media and Telecommunications Law*, 27 (1), pp 31-32; see also *LNS v Persons Unknown* [2010] EWHC 199(QB).

⁶⁰³ For example, [2004] UKHL 22.

directly influences the conduct of those who admire them,⁶⁰⁴ rendering the public interest justification for exposure empirically unsubstantiated at its foundation. If the harm that the role model rationale purports to address, the corruption of public morals through the influence of celebrity misconduct, cannot be demonstrated to exist in any concrete or measurable form, then the privacy violation occasioned by exposure cannot be justified by reference to it.

Wragg's analysis⁶⁰⁵ extends this critique, arguing that despite superficial distinctions between the role model rationale and the broader 'freedom to criticise' doctrine, the objections applicable to the former apply with equal force to the latter. Moreover, the courts' and academics' negative treatment of the role model analysis risks foreclosing the 'freedom to criticise' doctrine from gaining a meaningful foothold in this area of law.⁶⁰⁶ While Wragg accepts that the doctrine has a legitimate function, he argues it should be confined to cases where a claimant has deliberately, rather than merely implicitly, misled the public.⁶⁰⁷ The freedom to criticise doctrine, as currently applied, is analytically distinct from the role model rationale in two important respects. It does not require proof of actual harm caused to the public by the celebrity's conduct, nor does it demand a showing of 'hypocrisy' sufficient to engage the public's right not to be misled. The doctrine therefore ostensibly extends protection to a broad range of privacy-invading expression without the limiting conditions that might otherwise constrain its reach.

This critique connects directly to the Kantian framework developed in the preceding section.

Where the role model rationale is deployed instrumentally, as a *post hoc* justification for

⁶⁰⁴ See Kirsty Hughes, 'The Public Figure Doctrine and the Right to Privacy' (2019) 78 The Cambridge Law Journal, V Conclusion.

⁶⁰⁵ Paul Wragg, 'A Freedom to Criticise? Evaluating the Public Interest in Celebrity Gossip after Mosley and Terry' (2010) 2 Journal of Media Law 295.

⁶⁰⁶ Ibid, p 317.

⁶⁰⁷ Ibid, pp 310-311.

publication decisions driven by commercial rather than genuine public interest considerations, it exemplifies precisely the treatment of individuals as means to commercial ends that Kantian ethics identifies as morally impermissible. Wragg⁶⁰⁸ further observes that courts have employed the related but equally imprecise concepts of ‘role model’ status and ‘freedom to criticise’ as devices to justify⁶⁰⁹ interferences with privacy in cases where a claimant’s private life has been judged inconsistent with their public persona, incompatible with their chosen profession, or otherwise socially or morally objectionable.⁶¹⁰ These doctrinal tools have enabled the press to mount successful public interest defences on the basis of conduct deemed morally wrong in a generalised sense, without the discipline of precise legal criteria. As Wragg pointedly notes, individuals may choose their own role models, but no one is compelled to assume that status,⁶¹¹ a consideration that fundamentally undermines the normative basis of the doctrine.

Rowbottom⁶¹² reinforces this line of criticism, observing that courts sometimes assign a *quasi*-public function to individuals in the public eye by treating them as role models, without adequately explaining why the disclosure of information about such individuals is of genuine public value beyond the vague enforcement of ill-defined behavioural expectations. The argument is both analytically strained and of limited application, extending only to that narrow class of celebrity plausibly characterised as a role model in any meaningful sense.⁶¹³ A more sceptical assessment is offered by Moosavian and Coe, who argue that Wragg overstates the practical significance of the ‘exposing hypocrisy’ ground and that the reasoning in cases such

⁶⁰⁸ Paul Wragg, ‘Protecting Private Information of Public Interest: Campbell’s Great Promise, Unfulfilled’ (2015) 7 Journal of Media Law 225.

⁶⁰⁹ Ibid, p 319.

⁶¹⁰ Ibid, p 233.

⁶¹¹ Ibid, p 244.

⁶¹² See Jacob Rowbottom, “Power and the Public Eye: Why the Limits of Acceptable Criticism Are Wider for Public Figures.” (2025) Public Law 1 Sweet & Maxwell, p 11.

⁶¹³ Ibid, pp 11, 12, 19.

as *Ferdinand* and *Hutcheson* is entirely defensible.⁶¹⁴ They contend that critiques of this doctrine tend to exaggerate its doctrinal influence. It has served as the sole or primary basis for a defendant's success in very few cases. In the majority of instances where defendants have prevailed, the 'exposing hypocrisy' ground has operated in conjunction with other Article 10-favouring factors, such as comparatively weak countervailing Article 8 rights or the engagement of the fitness for public office category, rather than as a freestanding justification. This broader critique also fails to account for the claimant's own active role in constructing the circumstances from which the information arose, and provides no satisfactory explanation for why the law of misuse of private information should operate to shield a false public image that the claimant had no legitimate entitlement to project in the first place.

5.5 Conclusion

The UK GDPR/DPA 2018 provide a significant advancement in data protection laws compared to their predecessors, the Directive 95/46/EC and the DPA 1998. This chapter set out to analyse and assess the effectiveness of the UK's current data protection regime from four key aspects with comparisons with MPI; this discussion primarily focused on analysis of the ICO's handling of cases and monetary fines, as well as the application of Article 17 of the GDPR. This evaluation not only considered the protection of ordinary individuals' private data, but also included case studies on the privacy rights of celebrities. This chapter also considered the issues arising under the HRA 1998 which provides that English courts interpret existing law (under s.3 as regards the GDPR/DPA but also s.6 in relation to indirect horizontal effect) in a way that aligns with Convention rights, including the right to respect for private life and private

⁶¹⁴ See Rebecca Moosavian and Peter Coe, *Balancing Privacy Against Free Speech: In Defence of Exposing Hypocrisy* (2025) in D. Clifford, M. Richardson, and N. Witzleb, *Research Handbook on Privacy and Confidentiality in Media Law* (Edward Elgar, 2026), p 16; *Hutcheson v News Group Newspapers Ltd* [2011] EWCA Civ 808; *Ferdinand v MGN Ltd* [2011] EWHC 2454 (QB).

correspondence under Article 8, much to the frustration of the media, who are concerned with freedom of expression. However, the Act only requires courts to do this ‘insofar as it is possible’ as regards statutes under s.3.⁶¹⁵ Additionally, decisions of the ECtHR are not binding on English courts but are merely persuasive, under s.2 HRA, giving judges some discretion in their rulings, partly due to the margin of appreciation doctrine. Thus, domestic courts do not need to adhere fully to Strasbourg rulings when balancing free expression and privacy under either data protection or MPI.⁶¹⁶

This chapter has found that the current data protection regime, which can be found to include protection for private information under MPI, in the UK is effective in a number of respects. For example, using fines as deterrent means; applying for the delisting request through Art.17 the right to be forgotten like *TU, RE v Google*.⁶¹⁷ But there still exists some of the loopholes that have been found in this chapter, such as the lack of availability of injunctions under data protection provisions and the under-resourcing of the ICO.

After considering the personal data protection regime in the UK, Chinese data protection policies will now also be analysed beginning in Chapter 6 and discussed as a comparative regime. This will provide a broader perspective on how different regulatory frameworks address data protection challenges and privacy rights. The next chapters will then turn to discuss the data protection policies in China. They will be compared with the data protection

⁶¹⁵ See Florence Powell and Stephanie Needleman, ‘How Radical an Instrument Is Section 3 of the Human Rights Act 1998?’ (UK Constitutional Law Association 24 March 2021) <<https://ukconstitutionallaw.org/2021/03/24/florence-powell-and-stephanie-needleman-how-radical-an-instrument-is-section-3-of-the-human-rights-act-1998/>>.

⁶¹⁶ For example, the tests from *Axel Springer AG v Germany* (2012) 55 E.H.R.R. 6 at Strasbourg were not adhered to in *PJS v News Group Newspapers Ltd* [2016] A.C. 1081.

⁶¹⁷ *TU, RE v Google* [2022] EUECJ C-460/20.

regime in the UK, and the possibility that China might in future adopt a regime similar to the one under the UK GDPR will be considered in Chapter 8.

CHAPTER 6 THE CURRENT CHINESE LEGAL POSITION ON PERSONAL DATA PROTECTION

6.1 Introduction

Viktor Mayer-Schönberger, in his book *Delete* states, ‘Today, over 90% of the world’s information is in digital form, making it effortless to store, process, manipulate, and transmit.’⁶¹⁸ This clearly includes a large amount of personal data, which has the potential to be misused in the modern society since 2000. In the first half of 2024, China⁶¹⁹ reported an increase of 7.4 million internet users, bringing its internet population to over one billion.⁶²⁰ With its vast internet user base and advanced technological capabilities, China’s role as a global cyber power is undeniably significant and demands recognition.⁶²¹ The information era has seen the rapid expansion of the digital economy and a growing emphasis on the value of personal data. At the same time, incidents of data breaches have become increasingly common, leading to heightened public concern over information security in China.⁶²² However, some legal concepts⁶²³ and specific provisions⁶²⁴ still lack clarification within the current data protection system in China, as discussed below.

⁶¹⁸ Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2009), pp 52,53.

⁶¹⁹ With the terms of ‘Chinese’ ‘China,’ this thesis specifically refers to the country: People’s Republic of China (‘PRC’).

⁶²⁰ China Internet Network Information Centre (CNNIC), ‘The 54th Statistical Report on China’s Internet Development’ (2024) <<https://www.cnnic.com.cn/IDR/ReportDownloads/202411/P020241101318428715781.pdf>>.

⁶²¹ See Grace Pyo, ‘An Alternate Vision: China’s Cybersecurity Law and Its Implementation in the Chinese Courts’ (2021) 60 Colum J Transnat’l L 228, pp 230-231; see also Rogier Creemers, ‘The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy’ (2023) 33 Journal of Contemporary China 1, pp 173-174.

⁶²² See Rogier Creemers, ‘China’s Emerging Data Protection Framework’ (2022) 8 Journal of Cybersecurity, pp 173-174.

⁶²³ See *infra* section 6.3.

⁶²⁴ With the specific provisions, it will mainly focus on the PIPL.

This chapter seeks to address the central argument⁶²⁵ of this thesis by dividing the research discussed in this chapter into four key steps.

Step 1 consists of analysing the development of China's personal data protection legal framework in Section 6.2. This step examines the evolution of China's personal data protection regime and applies the *Brussels Effect*⁶²⁶ to illustrate the profound influence of EU data legislation (especially the GDPR) on China, taking account of the findings in the previous chapters. By doing so, it aims to understand, explain, and compare the legal systems of both regimes, shedding light on the similarities and differences in their approaches.

Step 2 consists of exploring legal debates on the status of the *Personal Information Protection Law* (PIPL) in Section 6.3.⁶²⁷ The second step focuses on the divergent views within Chinese legal academia regarding the legal status of the PIPL and the theoretical foundations of personal information rights. Furthermore, it examines the relationship between the PIPL and other legislative instruments, such as the *Civil Code of the People's Republic of China* (hereinafter referred to as the '*Civil Code*'),⁶²⁸ to provide a comprehensive understanding of the legal framework governing personal information protection in China.

⁶²⁵ See Introduction, p 29.

⁶²⁶ With regard of *Brussels effect*, it also discussed *supra* pp 108-109 in details; see further in Anu Bradford, 'The Brussels Effect' (2012) 107(1) Northwestern University Law Review 1; Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

⁶²⁷ Personal Information Protection Law (China) (中华人民共和国个人信息保护法) [2021] ('PIPL'), available at https://en.spp.gov.cn/2021-12/29/c_948419.htm; without otherwise explained, all translation from Chinese texts was performed by author herself. The Chinese translation into English texts of direct quotes and titles of primary and secondary legal sources is accompanied by the original Chinese texts online wherever necessary.

⁶²⁸ *Civil Code* (China) (中华人民共和国民法典) [2020] ('CC'); it is necessary to clarify the system of current Chinese Civil Law system here, the *Civil Code* consists of the General Principles Part and the Specific Principles Part. The General Part, namely the *General Principles of Civil Law*, which came into effect earlier and replaced the previous *General Provisions of Civil Law*.

Step 3 consists of investigating the localisation⁶²⁹ of the right to be forgotten in China in Section 6.4. The third step specifically explores the feasibility and potential pathways for the localisation of the right to be forgotten (RTBF) in China. Since the RTBF serves as a critical remedy in personal information legal protection in the UK and EU, which constitutes a central focus of this thesis, this analysis addresses a key question raised in the Introduction of the thesis:⁶³⁰ How far can personal data be effectively protected? The discussion further evaluates whether the RTBF can be effectively implemented within China's legal framework. The academic debates over the RTBF's feasibility and localisation also remark on its importance and value.

Step 4 consists of examining the balancing test regarding protection of personal information and freedom of expression in Section 6.5. The final step examines the complex and universal legal challenge of achieving a dynamic balance between personal information protection and freedom of the media and of expression, which was also conducted above in Chapter 5.⁶³¹ This step seeks to explore how these competing interests can co-exist within a relatively robust legal framework (i.e. the EU/UK data protection model), offering insights into maintaining and developing this delicate equilibrium.

By following these four steps, this chapter aims to systematically analyse the research questions in respect of this Chinese section,⁶³² addressing both theoretical and practical dimensions of personal data protection in China.

⁶²⁹ The term 'localisation' in this context refers to the adaptation of the right to be forgotten within the Chinese legal framework, as examined by Zeng Chen in 'Chinese Localization of the Right to Be Forgotten' (2020) 9 *NAVEIN REET Nordic Journal of Law and Social Research* 253. The article critically reflects on the legislative challenges surrounding this process.

⁶³⁰ See *supra* p 29.

⁶³¹ See *supra* section 5.4.2.

⁶³² See *supra* p 29.

6.2 The Development of the Personal Data Protection Legal Framework in China

China had already established a fragmented set of data laws and regulations shaped by its unique social and cognitive context,⁶³³ with the Supreme People's Court issuing interpretations and providing guidance through landmark cases. For example, in *Jianhua Xie v Qing Ye*,⁶³⁴ the Court of Appeal upheld the judgment of the trial court that the defendant failed, finding that the defendant had breached the plaintiff's right to privacy. The decision of the trial court was grounded in multiple legal provisions, including Article 110, Paragraph 1 of the *General Principles of Civil Law*;⁶³⁵ Articles 2, 6, 15, and 20 of the *Tort Liability Law*;⁶³⁶ Articles 16 and 18 of the Supreme People's Court's Interpretation on Civil Disputes Involving Personal Rights Violations via Information Networks.⁶³⁷ However, while the decisions of the courts referenced various statutory provisions, they lacked a coherent and comprehensive framework for defining privacy violations in the context of digital media.

A key issue in this case was to distinguish between personal information that was already available to public and that information disclosed in a manner that constituted an invasion of

⁶³³ Yuxiao Duan, China's Private Law Approach to Personal Data Protection (May 26, 2019) SSRN Electronic Journal, pp 8-9, Available at SSRN: <https://ssrn.com/abstract=3484725>; see also in Wang Yi, 'Research on Personal Information Protection Legislation in the Digital Age: Based on the Comparison of Current Legislation in China, America and Europe' (2023) 7 Advances in Economics Management and Political Sciences pp 23,25..

⁶³⁴ *Xie vs. Ye – General Personality Rights Dispute* (2019) Zhe 0192 Min Chu 624 谢某、叶某一般人格权纠纷 (2019) 浙 0192 民初 6244 号; The defendant, Ye Qing, had published two articles containing the alleged defamatory statements, including direct accusations against Xie Jianhua regarding procurement activities within the residential community, which were deemed to be defamatory and damaging to personal reputation.

⁶³⁵ General Provisions of the Civil Law (China) (中华人民共和国民法通则) [2017] ('CLGP'), available at <https://www.chinalawtranslate.com/en/general-provisions-of-the-civil-law/>.

⁶³⁶ Tort Liability Law (China) (中华人民共和国侵权责任法) [2009] ('TLT').

⁶³⁷ Provisions of the Supreme People's Court on Certain Issues Concerning the Application of Law in the Hearing of Cases of Civil Disputes over the Use of Information Networks to Infringe upon Personal Rights and Interests 2014 (SPC Interpretation 11/2014) (Revised) (最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定), available at <https://law.pkulaw.com/chinalaw/2042dd6367893f26bdfb.html>.

privacy.⁶³⁸ The defendant had uploaded photos of the plaintiff on its WeChat public account, thereby exposing the plaintiff's image to an unspecified third-party.⁶³⁹ The trial court found this action to be a violation of privacy.⁶⁴⁰ However, the Court of Appeal held that the defendant's exposure of the WeChat username and profile photos of the plaintiff did not constitute a breach of privacy, as, even if it was unauthorised, these elements were already accessible to public. This reasoning reveals a persistent doctrinal ambiguity in Chinese privacy law, i.e. the extent to which online information available remains protected under the current privacy principles. The decisions of courts implicitly provide a narrow interpretation of privacy, wherein only the disclosure of non-public or sensitive information is legally actionable.

The remedial approach taken by the trial court further highlights the limitations of digital privacy jurisprudence in China, by following the Supreme Court's judicial interpretations.⁶⁴¹ Rather than awarding substantial damages, the court required the defendant to issue continuous apologies⁶⁴² on WeChat public account, deeming this an adequate remedy. Unlike the awards of *JQL v NTP*⁶⁴³ in the UK, the amount of compensation for invasion of privacy was relatively lower.⁶⁴⁴ This case shows a tendency of the Chinese courts' high reliance on a traditional tort liability framework, with a primary focus on breach of duty rather than on the broader action of data protection.

⁶³⁸ *Xie v Ye* – General Personality Rights Dispute (2019) Zhe 0192 Min Chu 624 谢某、叶某一般人格权纠纷 (2019) 浙 0192 民初 6244 号, Part 6, The Court Holds, para 1,2.

⁶³⁹ *Ibid*, Part 6, The Court Holds, para 2.

⁶⁴⁰ *Ibid*.

⁶⁴¹ To clarify the definitions and effects of judicial interpretations as follows: the legal effect of judicial interpretations refers to the authority granted to the Supreme People's Court and the Supreme People's Procuratorate to interpret the application of laws in judicial and prosecutorial cases. These interpretations have general judicial validity and are legally binding. The object of judicial interpretation is legal provisions rather than legal norms. The effect of judicial interpretations is equivalent to that of laws.

⁶⁴² From the perspectives of necessity and reasonableness, the duration of the apology was set at 30 days.

⁶⁴³ *JQL v NTP* [2020] EWHC 1349 (QB).

⁶⁴⁴ Lewis J. awarded JQL £15,000 for damages, but in *Xie*, the monetary compensation was only RMB 3000.

6.2.1 From the Brussels effect to the Beijing effect⁶⁴⁵

Building on decades of theoretical scholarship, the *Brussels Effect*, as articulated by Anu Bradford,⁶⁴⁶ stands out prominently. It refers to the EU's 'unilateral power to regulate global matters.'⁶⁴⁷ This theory suggests that the EU's regulations have a remarkable capacity to influence and shape regulatory standards globally, creating a significant regulatory pull towards EU norms.⁶⁴⁸ Wenlong Li and Jiahong Che, analysed the development of the Chinese data protection regime, in their article, combined with the *Brussels Effect*,⁶⁴⁹ which provided an effective way to explore the evolution of the Chinese data protection regime, taking account of the influence of the EU GDPR.

China began developing its data protection framework later than the EU and the U.S.. Confronted with challenges like frequent data breaches due to the absence of data regulations,⁶⁵⁰ China had the valuable opportunity to look into existing models that addressed similar issues and then incorporate their rules into its domestic law. This process, known as legal transplantation,⁶⁵¹ the transfer of a legal rule or system from one country to another, is a

⁶⁴⁵ See Matthew Erie and Thomas Streinz, 'The Beijing Effect: China's Digital Silk Road as Transnational Data Governance', (2021) 54 NYU Journal of International Law and Politics, pp 1–92, see also further in Rogier Creemers, 'The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy' (2023) 33 Journal of Contemporary China 1, p 188.

⁶⁴⁶ Anu Bradford, 'The Brussels Effect' (2012) 107(1) Northwestern University Law Review 1.

⁶⁴⁷ Ibid.

⁶⁴⁸ Wenlong Li and Jiahong Chen, 'From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China' (2024) 54 Computer law & security report 105994, p 2.

⁶⁴⁹ With regard of *Brussels effect*, it also discussed *supra* in Chapter 4, pp 108-109, 195 in details.

⁶⁵⁰ Emmanuel Pernot-Leplay, China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.? 2020, 8 PENN. ST. J.L. & INT'L AFF. 49, pp 64-65, Available at: <https://elibrary.law.psu.edu/jlia/vol8/iss1/6>; Anja Geller, 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective' (2020) 69 GRUR International, pp 1191-1192; see also further in Wenlong Li and Jiahong Chen, 'From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China' (2024) 54 Computer law and security report/Computer law & security report 105994, pp 2-3.

⁶⁵¹ See Alan Watson, Legal Transplants: An Approach to Comparative Law 21 (1 ed. 1974).

well-established concept in comparative law studies.⁶⁵² China has chosen the EU legal approaches to data protection. The PIPL is a typical example of this process, because it largely mirrors the provisions of the EU GDPR in essence. The detailed statutory comparison with the GDPR will also be discussed in the following Chapter 7.

This chapter will now primarily focus on analysing the statutory provisions *per se* as China follows a civil law system.

a) Fragmented data protection: exploration

Prior to the enactment of the PIPL, China's legislative approach to personal information protection exhibited two main characteristics: first, relevant principles, rules, and mechanisms were scattered across various normative legal documents; second, regional legislative initiatives preceded and outnumbered those at the central level.

As personal data legislation has become increasingly systematic in Europe,⁶⁵³ China has also been learning from and absorbing, to an extent, the European legislative experiences as discussed below and in Chapter 7. With the continuous development of its society and the improvement of public awareness, China's legislative approaches to digital privacy and private data online are gradually aligning with European methods (e.g. the enactment of the PIPL),⁶⁵⁴ although the regulatory capabilities of China still lag significantly behind those of the EU system, especially the regulatory ability of the Standard Contractual Clauses (SCCs), which

⁶⁵² See Emmanuel Pernot-Leplay (note 650) p 53.

⁶⁵³ Followed by a set of data regulations and policies established in the EU, such as Directive 95/46 and EU GDPR etc...

⁶⁵⁴ See Wenlong Li and Jiahong Chen, 'From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China' (2024) 54 Computer law and security report/Computer law & security report 105994, pp 2-3.

are pre-approved contractual arrangements between data exporters and data importers that impose binding data protection obligations on the receiving party, providing a legal basis for transfers to third countries that lack an adequacy decision. Their significance within the EU framework was reaffirmed, and simultaneously complicated, by the CJEU's decision in *Schrems II*, which required that SCCs be supplemented by transfer impact assessments capable of verifying that the legal order of the destination country does not undermine the protections they purport to guarantee. Chinese legislators demonstrate a clear inclination toward stronger personal data protection, increasingly incorporating personal data protection provisions into general laws such as the *Tort Liability Law*, the *Consumer Protection Law*, the *Criminal Law*,⁶⁵⁵ and the *Civil Code*. However, it is regrettable that data protection legislative efforts in China have remained primarily focused on trade, market and economic concerns,⁶⁵⁶ with insufficient attention being given to building legal principles, rights and remedies regarding individuals' private information. Thus, clear differences between the EU and the Chinese approach are still apparent.

Due to China's expanding international market and influence, under the framework of the Belt and Road Initiative,⁶⁵⁷ and other international collaborations, China's legal regulations and data legislation framework have garnered wide international attention.⁶⁵⁸ China's legislative experience has also been widely referenced by some developing countries, which can be

⁶⁵⁵ Criminal Law (2021 Edition) (China Law Translate 28 December 2020) <https://www.chinalawtranslate.com/en/criminal-law-2021/>, the Seventh Amendment to the Criminal Law, adopted on February 28, 2009, was the first legal provision to incorporate personal information into the realm of criminal law protection.

⁶⁵⁶ See Rogier Creemers, 'The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy' (2023) 33 *Journal of Contemporary China* p 180; see also in Mark Jia, 'Authoritarian Privacy' (2023) 91 *The University of Chicago Law Review*, p 753.

⁶⁵⁷ China's Belt and Road Initiative (BRI) (一带一路), take a glance at European Bank, 'Belt and Road Initiative (BRI)' (European Bank for Reconstruction and Development 2023) <<https://www.ebrd.com/what-we-do/belt-and-road/overview.html>>.

⁶⁵⁸ See Matthew Erie and Thomas Streinz, 'The Beijing Effect: China's Digital Silk Road as Transnational Data Governance', (2021) 54 *NYU Journal of International Law and Politics*, pp 3, 6.

described as the *Beijing Effect*.⁶⁵⁹ For example, China provides AI surveillance technology to some governments⁶⁶⁰ to use it for mass surveillance purposes.⁶⁶¹ Clearly, this influence does not follow the logic of the *Brussels Effect*. After all, the *de facto Brussels effects* occurs when companies from non-EU Member states voluntarily extend EU rules across their global businesses.⁶⁶²

b) Pillars of the legal framework for personal data protection in China

Although it cannot be directly applied in judicial cases, Art. 40 of the Chinese Constitution provides at the constitutional level protections for the freedom of communications for individuals. Bearing this in mind, the legal pillars of the framework for data protection could be considered as follows. Building upon the basic legal principles and regulations of the *Civil Code*,⁶⁶³ the current legal framework in China for personal data protection is primarily established through the *Cybersecurity Law*,⁶⁶⁴ the *Data Security Law*⁶⁶⁵ and the PIPL.

⁶⁵⁹ See Richard Heeks and others, 'China's Digital Expansion in the Global South: Systematic Literature Review and Future Research Agenda' (2024) 40 *The Information Society* 1; see also in Rogier Creemers, 'China's Emerging Data Protection Framework' (2022) 8 *Journal of Cybersecurity*, pp 8, 9.

⁶⁶⁰ In exporting AI surveillance technologies internationally to approx. 63 recipient countries; Uganda, for example, acquired a nationwide system of surveillance cameras with facial recognition capabilities from Huawei in 2019, and state authorities in Zimbabwe have acquired facial recognition technologies for border security and mass surveillance.

⁶⁶¹ See Kaan Sahin, 'The West, China, and AI Surveillance' (Atlantic Council 18 December 2020) <<https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance/>>.

⁶⁶² Maria Niestadt and Jasmin Reichert, *The global reach of the EU's approach to digital transformation*, 2024 EPRS European Parliamentary Research Service, p 2, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757632/EPRS_BRI\(2024\)757632_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757632/EPRS_BRI(2024)757632_EN.pdf).

⁶⁶³ *Civil Code* of the People's Republic of China (english.www.gov.cn 31 December 2020) <https://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html>

⁶⁶⁴ *Cybersecurity Law of the People's Republic of China* [Effective] 中华人民共和国网络安全法 (Lawinfochina.com 2016) <<https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3>>.

⁶⁶⁵ *Data Security Law (China)* (中华人民共和国数据安全法) [2021] ('DSL').

Certain provisions of the PIPL remain ambiguous, as its language is relatively vague and broad.⁶⁶⁶ For instance, the right to be forgotten under Article 17 of the UK GDPR explicitly delineates both applicable and non-applicable scenarios across three sections, providing clear guidance as to when erasure of personal data requests from data subjects can be granted or denied. By contrast, Article 47 of the PIPL grants individuals the right to request the deletion of their personal data but does not specify any exceptions or limitations. While the five sub-sections listed under Article 47 provide the grounds for individuals to request data deletion, they fail to clarify the categories of data that cannot be deleted. Therefore, in comparison to the framework of the GDPR, the PIPL's approach to data de-listing and the right to be forgotten still remains underdeveloped, leaving significant room for interpretative uncertainty, as discussed above.

This chapter will now analyse three legal pillars i.e. the *Cybersecurity Law*, the *Data Security Law* and the PIPL as the legal basis for personal data protection and further analyse personal data protection in China in the following sections within Chapter 6.

6.2.2 The cultural approach to the development of Chinese data protection policy

When examining the Chinese cultural context for privacy and data protection through a broad historical lens, the primary distinction appears to lie in the perception of personal data in relation to the cultural community. In Western cultures,⁶⁶⁷ privacy is often viewed as an individual asset,⁶⁶⁸ linked to preserving personal dignity and autonomy, and protected by law

⁶⁶⁶ See Lu Zhang, 'Personal Information of Privacy Nature' under Chinese *Civil Code* (2021) 43 Computer Law & Security Review 105637, pp 2, 3.

⁶⁶⁷ In relation to Western cultures, it refers to a broad term as social and legal norms, customs, values... in Europe or based on the European culture.

⁶⁶⁸ See Henrik Skaug Sætra, 'Privacy as an Aggregate Public Good' (2020) 63 Technology in Society 101422, p 2.

even against state interference, as discussed in the previous chapters.⁶⁶⁹ In contrast, privacy concerning the relationship between the individual and the state is far less prominent in Chinese traditional cultural values.⁶⁷⁰ In China, privacy is more of a moral concept⁶⁷¹ tied to proper private behaviour, maintained through self-regulated balance rather than via formal legal protections.⁶⁷² Much space is left for local courts and Judges to decide on the nature, scope and impact of these rights of individuals on a case-by-case basis.⁶⁷³

Given the legal and political differences between Western countries and China, directly adopting Western data protection models⁶⁷⁴ would face significant challenges.⁶⁷⁵ Instead, China follows its own reasoning and creates distinct characteristics, similar to how the divergent foundational philosophies of the EU and the U.S. trigger their unique approaches.⁶⁷⁶ However, as discussed above, the current legislative framework for data protection is fragmented and offers insufficient protection for the rights of individuals in China.⁶⁷⁷ Moreover, in the scope of the processing of personal data, Chinese personal data protection law remains

⁶⁶⁹ See Kunbei Zhang and Aernout Schmidt, 'Looking at China's Facebook (RenRen) through the Lens of European Data Protection Principles' [2013] SSRN Electronic Journal, p 2, Available SSRN: <https://ssrn.com/abstract=2257907> or <http://dx.doi.org/10.2139/ssrn.2257907>; see also chapters 2 and 4 *supra*.

⁶⁷⁰ Emmanuel Pernot-Leplay (note 650) pp 65-66.

⁶⁷¹ With the specific moral concept, it refers to Confucianism; see further in Daniel A Bell, *China's New Confucianism: Politics and Everyday Life in a Changing Society* (Princeton University Press 2010).

⁶⁷² *Ibid*, see also Kunbei Zhang and Aernout Schmidt, 'Looking at China's Facebook (RenRen) through the Lens of European Data Protection Principles' [2013] SSRN Electronic Journal, p 2, Available at SSRN: <https://ssrn.com/abstract=2257907> or <http://dx.doi.org/10.2139/ssrn.2257907>.

⁶⁷³ *Ibid*.

⁶⁷⁴ Such as EU GDPR, DPA 2018 in the UK.

⁶⁷⁵ See Wenlong Li and Jiahong Chen, 'From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China' (2024) 54 *Computer law & security report* 105994, pp 5,9,13; see also in Gao, Henry S., *Data Regulation with Chinese Characteristics* (August 1, 2019). SMU Centre for AI & Data Governance Research Paper No. 2019/04, Singapore Management University School of Law Research Paper No. 28/2019, In M. Burri (Ed.), *Big Data and Global Trade Law* (pp. 245-267). Cambridge: Cambridge University Press. doi:10.1017/9781108919234.017, Available at SSRN: <https://ssrn.com/abstract=3430284> or <http://dx.doi.org/10.2139/ssrn.3430284>

⁶⁷⁶ See Emmanuel Pernot-Leplay (note 650) p 54.

⁶⁷⁷ Morgana Mo Zhou and others, 'Understanding Chinese Internet Users' Perceptions Of, and Online Platforms' Compliance With, the Personal Information Protection Law (PIPL)' (2024) 8 *Proceedings of the ACM on human-computer interaction* 1, 138:2; see also Xuanbo Chen, *Personal Information Protection and Improvement of Information Disclosure System for Network Service Providers* (in Chinese). *Journal of South-Central Minzu University (Humanities and Social Sciences)* 40, 1 (2020), pp 174-180.

largely territorial in nature,⁶⁷⁸ though there are still exceptions that exist. For instance, the protection permits courts to assert jurisdiction over a non-resident defendant based solely on the physical location of a server.⁶⁷⁹

Just as Deng Xiaoping introduced the concept of ‘socialism with Chinese characteristics,’⁶⁸⁰ there is also a new notion of ‘data protection with Chinese characteristics.’⁶⁸¹ This framework is influenced by the principle of cyber-sovereignty and the differentiation between privacy protected from intrusion by private individuals and privacy protected from the government. It reflects China’s distinctive sociopolitical context and geopolitical notions, defining the country’s unique approach to data protection.⁶⁸² In particular, if data collection is ‘necessary and proportionate,’ the EU GDPR allows Member States to collect personal information in the public interest.⁶⁸³ The recognition of personal information protection as a *de jure* protectable interest within the legal framework in China is not a priority within the legal hierarchy and its legal position, affected by its distinctive socio-political stance has significantly affected how personal information protection is balanced against other rights and interests.⁶⁸⁴ For instance,

⁶⁷⁸ Anja Geller, ‘How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective’ (2020) 69 GRUR International, p 1193.

⁶⁷⁹ Jie (Jeanne) Huang, Chinese Private International Law and Online Data Protection (July 9, 2018). Journal of Private International Law, p 4, Available at SSRN: <http://dx.doi.org/10.2139/ssrn.3646640>.

⁶⁸⁰ Xiaoping Deng, ‘Deng Xiaoping: Socialism with Chinese Characteristics - New Learning Online’ (newlearningonline.com1984) <<https://newlearningonline.com/new-learning/chapter-4/neoliberalism-more-recent-times/deng-xiaoping-socialism-with-chinese-characteristics>>.

⁶⁸¹ See Roberts, Huw, Informational Privacy with Chinese Characteristics (December 18, 2021). Digital Ethics Lab Yearbook 2021, Available at SSRN: <https://ssrn.com/abstract=3988745>; see also in Gao, Henry S., Data Regulation with Chinese Characteristics (August 1, 2019). SMU Centre for AI & Data Governance Research Paper No. 2019/04, Singapore Management University School of Law Research Paper No. 28/2019, In M. Burri (Ed.), Big Data and Global Trade Law (pp 245-267). Cambridge: Cambridge University Press. doi:10.1017/9781108919234.017, Available at SSRN: <https://ssrn.com/abstract=3430284> or <http://dx.doi.org/10.2139/ssrn.3430284>.

⁶⁸² See Emmanuel Pernot-Leplay (note 650) p 54.

⁶⁸³ Art.9 of GDPR, ‘General Data Protection Regulation (GDPR) – Final Text Neatly Arranged’ (General Data Protection Regulation (GDPR)2013) <<https://gdpr-info.eu/art-9-gdpr/>>.

⁶⁸⁴ See Wenlong Li and Jiahong Chen, ‘From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China’ (2024) 54 Computer law & security report 105994, p 12.

domestic courts depart from the explicit provisions of the tort laws in order to compensate data subjects where the personal information has been misused.⁶⁸⁵

6.2.3 The annotation method within legislative responses in China

In 2018, during the China Development Forum, Baidu CEO Robin Li sparked a wave of controversy on social media with his remark that ‘Chinese people are willing to trade privacy for convenience or efficiency.’⁶⁸⁶ This statement drew widespread criticism and highlighted the inherent tension between convenience/efficiency and privacy in the era of big data.⁶⁸⁷ The protection of personal information online is a critical component of the broader personal information protection framework in China. It is also an urgent necessity in China’s judicial practice.⁶⁸⁸ Legislative responses from China to these evolutions were however slow in coming, with basic and broad frameworks only put in place at the end of the 2000s.⁶⁸⁹

a) Definitions of data protection

According to Article 4 of *the Provisions on Protecting the Personal Information of Telecommunications and Internet Users* issued by the Ministry of Industry and Information Technology in 2013,⁶⁹⁰ personal information is defined as ‘a user’s name, date of birth, identity

⁶⁸⁵ Benjamin L Liebman, ‘Ordinary Tort Litigation in China: Law versus Practical Justice?’ (2020) 13(2) *Journal of Tort Law*, pp 200, 208.

⁶⁸⁶ Sixth Tone, ‘Are Chinese People ‘Less Sensitive’ about Privacy?’ (#SixthToneMarch 2018) <<https://www.sixthtone.com/news/1001996>>.

⁶⁸⁷ Wang Zhihao and Lei Yuxi, ‘The Boundaries and Reexamination of the ‘Right to Be Forgotten’ in social media’ (2024) 5 *Southeast Communication*, p 98.

⁶⁸⁸ Anja Geller, ‘How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective’ (2020) 69 *GRUR International*, p 1202.

⁶⁸⁹ *Ibid.*

⁶⁹⁰ ‘Provisions on Protecting the Personal Information of Telecommunications and Internet Users’ (2016) 48 *Chinese Law & Government* 147, available at <https://www.tandfonline.com/doi/full/10.1080/00094609.2015.1048162#d1e56>.

card number, address, telephone number, account number, passwords, and other information that can distinguish the user's identity either independently or in combination with other data.'⁶⁹¹ After that, Article 111 of the *General Provisions of Civil Law*⁶⁹² (replaced by the *Civil Code*) emphasised the importance of information protection and outlined potential legal liabilities for misusing of personal information.⁶⁹³

However, at the legislative level, only the *Cybersecurity Law* explicitly addresses 'data' from the perspectives of network construction, operation and service provision, network operation security, and network infrastructure.⁶⁹⁴ The term 'data' is used, for the first time, and defines key elements of data network security, such as integrity, confidentiality, and availability.⁶⁹⁵ Nevertheless, the *Cybersecurity Law* does not differentiate between 'information' and 'data.' Even in Article 1, which sets out the legislative purpose, the law employs the term 'information' instead of 'data.'⁶⁹⁶ The lack of strict differentiation between these terms suggests that in existing laws, judicial interpretations, and regulatory documents, 'information' and 'data' are implicitly regarded as equivalent or, at the very least, are used interchangeably in conceptual terms.⁶⁹⁷

b) The scope of application

⁶⁹¹ Yuxiao Duan, China's Private Law Approach to Personal Data Protection (May 26, 2019) SSRN Electronic Journal, p 5, Available at SSRN: <https://ssrn.com/abstract=3484725>.

⁶⁹² General Provisions of the Civil Law (China) (中华人民共和国民法通则) [2017] ('CLGP'), available at <https://www.chinalawtranslate.com/en/general-provisions-of-the-civil-law/>.

⁶⁹³ Yufan He, 'On the Construction of Chinese Legislation Path Concerning Data Protection - the Introduction of the Right of Data Portability' [2022] 2021 2nd International Conference on World Economy and Project Management (WEPM 2021), p 41, DOI: 10.23977/wepm2021.006.

⁶⁹⁴ Art 10 of Cybersecurity Law (China) (中华人民共和国网络安全法) [2016] ('CL').

⁶⁹⁵ Chapters 3 and 4 of Cybersecurity Law (China) (中华人民共和国网络安全法) [2016] ('CL').

⁶⁹⁶ See Art.1 of the CSL: This Law is formulated in order to: ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the informatization of the economy and society.

⁶⁹⁷ See Lu Zhang, 'Personal Information of Privacy Nature' under Chinese *Civil Code* (2021) 43 Computer Law & Security Review 105637, pp 3,4.

The CSL and the *Data Security Law*⁶⁹⁸ provide limited extraterritorial application.⁶⁹⁹ The *Laws* mainly applies to the construction, operation, maintenance, and use of networks within China, as well as the supervision and management of cybersecurity and data security.⁷⁰⁰ Unlike the CSL and the DSL, the PIPL⁷⁰¹ applies to the processing of natural persons' personal information within China, as well as covering certain circumstances where personal information of individuals in China is processed outside the country. Its regulatory scope includes rules for personal information processing, regulations on cross-border transfer of personal information and individuals' rights in processing of personal information.

c) Legal remedies

After the issue of the CSL in 2017, some of the provisions establish rights related to privacy and data security, providing a potential basis for plaintiffs to pursue civil litigation.⁷⁰² Articles 42, 43, and 44 of the CSL concern personal information, requiring network operators to take steps to '*...ensure the security of personal information they gather*' and prohibiting unlawful use of personal information.⁷⁰³

⁶⁹⁸ Art. 2 of the Data Security Law (China) (中华人民共和国数据安全法) [2021] ('DSL').

⁶⁹⁹ Art. 2 and 5 of the CSL; see also in Grace Pyo, 'An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts' (2021) 60 Colum J Transnat'l L pp 240-241.

⁷⁰⁰ Art. 2 of the Cybersecurity Law (China) (中华人民共和国网络安全法) [2016] ('CL').

⁷⁰¹ Art. 3 of the Personal Information Protection Law (China) (中华人民共和国个人信息保护法) [2021] ('PIPL'), available at https://en.spp.gov.cn/2021-12/29/c_948419.htm.

⁷⁰² See Grace Pyo, 'An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts' (2021) 60 Colum J Transnat'l L pp 241,242.

⁷⁰³ Articles 42, 43, and 44 of the CSL; Rogier Creemers, Graham Webster and Paul Triolo, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' (DigiChina29 June 2018) <<https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>>.

The Supreme People's Court also provides practical guidance. Article 12, Paragraph 1, Items (4) and (5) of the *Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Disputes Involving Personal Rights Infringed by the Use of Information Networks*,⁷⁰⁴ reflects a nuanced approach to the protection of personal information, suggesting that individuals who have voluntarily posted their information online have limited legal recourse in cases of further dissemination. However, the inclusion of broad and undefined concepts such as 'public interest' and 'social ethics' introduces interpretative challenges, granting courts considerable discretion in determining whether a claim is actionable. This contrasts with more structured frameworks, such as the GDPR, which explicitly outlines data subjects' rights and the circumstances under which personal data can be lawfully processed or erased.

6.2.4 Overview: understanding the Personal Information Protection Law and the Chinese data protection framework

Subsequent laws, such as the *Data Security Law* and the PIPL, both passed in 2021, have further expanded China's data regulations. As discussed above, the Personal Information Protection Law is largely similar in some respects to the EU GDPR.⁷⁰⁵ Through comparison, it is evident that, compared to certain judicial interpretations and the *Civil Code*, the PIPL defines the scope

⁷⁰⁴ Provisions of the Supreme People's Court on Certain Issues Concerning the Application of Law in the Hearing of Cases of Civil Disputes over the Use of Information Networks to Infringe upon Personal Rights and Interests 2014 (SPC Interpretation 11/2014) (Revised), which came into effect on October 10, 2014, regulates that 'if personal information voluntarily disclosed by a natural person online, or other legally disclosed personal information, is published on the internet, even if it causes adverse effects, the data subject cannot seek remedies from the people's court on the grounds of infringement as long as the act of disclosing the information does not violate public interest, social ethics, or harm the significant interests of the data subject that deserve protection.' (最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定), available at <https://law.pkulaw.com/chinalaw/2042dd6367893f26bdfb.html>.

⁷⁰⁵ Natasha Lomas, China Passes Data Protection Law, (Aug. 20, 2021) TECH CRUNCH, <https://techcrunch.com/2021/08/20/china-passes-data-protection-law> [<https://perma.cc/8J48-38WG>].

of personal information in a general manner, rather than through a specific list.⁷⁰⁶ Where the PIPL is primarily concerned with the relationship between a data subject and a data controller/processor, the DSL basically focuses on national security.⁷⁰⁷ Regulatory bodies such as the Cyberspace Administration of China (CAC)⁷⁰⁸ dominate enforcement. However, sectoral overlaps, particularly between the CAC, the Ministry of Public Security, and local public security bureaus, frequently lead to delays, unclear mandates, and insufficient coordination, all of which impair swift and unified enforcement.⁷⁰⁹

Furthermore, the PIPL establishes a relatively plausible regime for legal liabilities in the case of misusing of personal information in China. It emphasises tort liabilities for the misuse of personal data, holding data controllers accountable for any harm caused by violations of the law. However, the effectiveness of these provisions in practice remains contingent upon the proper enforcement of these rights and the development of a robust regulatory and judicial framework to address such violations.

6.3 Doctrinal Debates on Legal Concepts and the Status of the Personal Information Protection Law

The legislative conceptions captured in the current Chinese data protection model are built on two fundamental pillars, as Creemers observes: personal information protection and data

⁷⁰⁶ Art.3 of the Personal Information Protection Law (China) (中华人民共和国个人信息保护法) [2021] ('PIPL'), available at https://en.spp.gov.cn/2021-12/29/c_948419.htm.

⁷⁰⁷ Ibid, p 6.

⁷⁰⁸ CyberspaceAdministrationofChinaLaunchestheInitiativeonChina-AfricaJointlyBuildingaCommunitywithaSharedFutureinCyberspace_中央网络安全和信息化委员会办公室 (www.cac.gov.cn) <https://www.cac.gov.cn/2021-08/25/c_1631480920680924.htm>.

⁷⁰⁹ See Liping Yang, Yiling Lin and Bing Chen, 'Practice and Prospect of Regulating Personal Data Protection in China' (2024) 13 Laws 78, pp 4, 5 of 17; see also on 'Regulators, Enforcement Priorities and Penalties | China | Global Data and Cyber Handbook | Baker McKenzie Resource Hub' (Bakermckenzie.com2025) <<https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/asia-pacific/china/topics/regulators-enforcement-priorities-and-penalties>> accessed 6 August 2025.

security.⁷¹⁰ This dual framework reflects China's approach to managing the complexities of data governance, whereby the legal protection of personal information of individuals is balanced with broader concerns about national security. The two pillars form the foundation of the evolving legal and regulatory landscape for data protection in China, but they also raise important questions regarding the tension between individuals' rights and state interests in China, particularly in an era of high-tech and digital surveillance.

6.3.1 *The fundamental legal position and protective functions of the PIPL*

During the drafting of the PIPL, there was no consensus among the drafting experts.⁷¹¹ To thoroughly understand the PIPL, it is necessary to first examine its fundamental legal positioning and protective functions, followed by a comparison of its convergence with and divergence from the GDPR. In the legislative explanations for the PIPL's draft, the legislature highlighted its dual nature as a fundamental law encompassing both public and private law attributes, stating that the PIPL 'originates from the Constitution and is derived from the *Civil Code*.'⁷¹² Therefore, the PIPL constitutes a fundamental law of personal information protection, with equal status to *Criminal law* and the *Civil Code*.⁷¹³ However, in terms of its specific content, particularly its protection systems and enforcement mechanisms, the PIPL demonstrates significant cross-disciplinary features.⁷¹⁴ The *Civil Code* establishes the basic

⁷¹⁰ See Rogier Creemers, 'China's Emerging Data Protection Framework' (2022) 8 *Journal of Cybersecurity*, p 8.

⁷¹¹ Zhou Hanhua, 'The Legal Positioning of Personal Information Protection' (2020) 3 *Studies in Law and Business*, p 71.

⁷¹² 'Article 1 of the Personal Information Protection Law (Legislative Purpose and Basis): Text and Explanation' (Ahdhf.com, 2024) <http://www.ahdhf.com/law/twsy/15059.html>.

⁷¹³ Zhou Hanhua, 'The Legal Positioning of Personal Information Protection' (2020) 3 *Studies in Law and Business*, p 73; see also Long Weiqiu, 'The Basic Legal Positioning and Protective Function of the Personal Information Protection Law: An Analysis Based on the Formation and Expansion of the New Legal System' (2021) 43 *Modern Jurisprudence* 5 <https://doi.org/10.3969/j.issn.1001-2397.2021.05.06>, pp 87-91.

⁷¹⁴ See Lu Zhang, 'Personal Information of Privacy Nature' under Chinese *Civil Code*' (2021) 43 *Computer Law & Security Review* 105637 pp 5-7; see also in Igor Calzada, 'Citizens' Data Privacy in China: The State of

framework for personal information rights, while the PIPL further elaborates on these rights by specifying their subjects, legal effects, and remedies.⁷¹⁵

Shi Jiayou, in his article, described the *Civil Code* as the ‘sun,’ while the PIPL acts as a ‘planet’ orbiting around it.⁷¹⁶ As a specialised law, the PIPL should be interpreted in accordance with the ‘sunlight’, emitted by the foundational principles of the *Civil Code*. He argued that the PIPL should be drafted with the characteristics of administrative law, as preventive measures for personal information protection require the establishment of a detailed governmental regulatory system.⁷¹⁷ Consequently, from this perspective, such legislation would fall within the realm of administrative law rather than civil law. Wang Liming contended that, due to the unique nature of personal information *per se*, it is difficult to fully achieve protection within a single branch of law.⁷¹⁸ Thus, a combination of civil and administrative law has arisen, resulting in the PIPL as a form of sector-specific legislation that inherently combines the attributes of both branches.⁷¹⁹

This thesis argues that the relationship between the PIPL and the *Civil Code* cannot be processed through the traditional framework of general and specialist laws or regulations.⁷²⁰

the Art of the Personal Information Protection Law (PIPL)’ (2022) 5 Smart Cities 1129

<https://www.mdpi.com/2624-6511/5/3/57>, p 1136.

⁷¹⁵ Shen Weixing, ‘On the Construction and Systematization of Personal Information Rights’ (2021) 5 *Journal of Comparative Law*, pp 1-3.

⁷¹⁶ See Shi Jiayou, ‘How to Connect and Coordinate the Personal Information Protection Law and the *Civil Code*’ (2021) 2 *People’s Forum*, pp 92-93; see also in Shi Jiayou, ‘The Private Law Dimension of Personal Information Protection: On the Relationship between *Civil Code* and Personal Information Protection Law’ (2021) 5 *Journal of Comparative Law* pp 31–32.

⁷¹⁷ See Xianzhong Sun, ‘Recommendations for Amendments to the Draft Personal Information Protection Law 关于《个人信息保护法》(草案)的修改建议’ (Ccssn.cn, 2020) http://iolaw.cssn.cn/zxzp/202104/t20210408_5325166.shtml, section 3.

⁷¹⁸ Wang Liming, ‘Harmony in Diversity: The Rule Differentiation and Application of Privacy Rights and Personal Information’ (2021) 2 *Law Review* <https://doi.org/10.13415/j.cnki.fxpl.2021.02.002>, pp 23-24.

⁷¹⁹ Ibid.

⁷²⁰ Cheng Xiao, ‘On the Relationship Between the *Civil Code* and the Personal Information Protection Law’ (2022) 3 *Science of Law (Journal of Northwest University of Political Science and Law)* <https://doi.org/10.16290/j.cnki.1674-5205.2022.03.015>, pp 23-24.

Instead, it should be addressed through mutual referral clauses to ensure proper alignment and integration. However, in terms of practical application, the PIPL still plays a supplementary role⁷²¹ rather than acting as the primary legal instrument in cases involving personal data protection. In this respect, as in others, it presents a contrast to the GDPR. While it establishes essential rights for individuals and obligations for data controllers/processors, the judicial decisions often intersect with other legal areas, such as the tort or cybersecurity regulations, which continue to hold significant weight in resolving cases. Despite its importance, the PIPL is not fully integrated into the broader legal system as the primary regulatory framework for personal data protection.

6.3.2 *The rights to personal information in China*

Neither the *Civil Code* nor the PIPL explicitly establishes the concept of a *right to personal information*,⁷²² meaning that they do not directly define the fundamental legal interests of data subjects. Instead, this fundamental legal interest is embedded within the broader framework of ‘personal information processing rules.’⁷²³ These rules govern the collection, use, and transfer of personal data, serving as foundational norms within the legal system. By framing personal information protection in this way, the *Civil Code* and the PIPL provide a regulatory structure that focuses primarily on the lawful processing of personal data rather than directly articulating personal information as a distinct right.

⁷²¹ See *Qin Moule and Others* (2021) Personal Information Infringement Case (2021) Jing 0105 Xing Chu 2759 秦某乐等人侵犯公民个人信息案, 京 0105 刑初 2759 号; *Guo Mou, Lü Mou and Others* (2020) Personal Information Infringement Case, Gan 0123 Xing Chu 53 郭某、吕某等侵犯公民个人信息案(2020)赣 0123 刑初 53 号.

⁷²² Individuals have a number of rights over the way organisations use their personal information in the UK GDPR/ DPA 2018. These are set out in the General Data Protection Regulation (GDPR).

⁷²³ See Chapter 4 of the PIPL.

For purposes of comparison with the PIPL, to specifically understand the examination of the rights granted to data subjects under the GDPR, as discussed in Chapter 4,⁷²⁴ it is helpful to categorise online data into two broad categories: visible and invisible data. The right to be forgotten primarily addresses visible personal data that has been accessible to public, such as private information shared on social media, websites, or other online platforms. This right allows individuals to request the erasure of such public visible data from data controllers/processors, in order to restore control over personal information that has been disseminated online.⁷²⁵

This distinction between visible and invisible data helps to clarify how the GDPR/DPA 2018 applies its various rights and principles, with the right to be forgotten targeting data that is actively visible and available to others, while other principles such as data minimisation focus on the processing of personal data at the backstage.⁷²⁶ By addressing these two types of personal data separately, the GDPR provides an approach to data protection: balancing individual's private information with the need for businesses and governments to process data for legitimate purposes. In contrast, the PIPL did not provide the practical approaches to that. State organs are exempt from their notification duties where other laws or regulations require 'confidentiality,' or where 'notification will impede State organs' fulfilment of their statutory duties and responsibilities.'⁷²⁷

⁷²⁴ See *supra* section 4.5.1.

⁷²⁵ See Li Wenlong, 'Privacy Protection and the Right to Be Forgotten in the Era of Big Data' (2015) 30(2) Graduate Law Review (CUPL), p 48. See also discussion in Chapter 2, p 48.

⁷²⁶ In this context, 'backstages' refers to the operations conducted within internal computer systems of certain entities, such as states and corporations, activities that remain largely hidden from public.

⁷²⁷ Mark Jia (note 656) p 751.

Cheng Xiao's perspectives focus on the differences between the *Civil Code* and the PIPL in their approaches to personal information protection.⁷²⁸ The *Civil Code* emphasises tort liabilities for invasion of personal information rights, providing *ex post facto* protection and remedies.⁷²⁹ In contrast, the PIPL regulates personal information processing activities, particularly through numerous public law provisions that establish the legal obligations of data controllers and processors.⁷³⁰ This instance helps to understand the functions of PIPL in terms of preventing illegal processing of personal data and digital invasions on the rights to personal information for data subjects through strict duties *ex ante* imposed on data controllers and processors.

The case of *Zhu Ye v Baidu*⁷³¹ could be a significant example here: the Nanjing Court ruled that Baidu Company's personalised ad online did not constitute a breach of Zhu Ye's privacy.⁷³² The Judges of Appeal held that the Baidu collected and used data that could not be linked to an identifiable individual, meaning that the anonymous nature of such data did not meet the identifiability requirement for personal information.⁷³³ The court emphasised the anonymised nature of the data, arguing that it did not have the necessary identifiability to be classified as personal information under Chinese law.⁷³⁴ However, this section argues that this ruling confuses the concepts of personal information and privacy, bearing in mind that misuse of non-personal information can still constitute privacy invasion.

⁷²⁸ Cheng Xiao, 'On the Relationship Between the *Civil Code* and the Personal Information Protection Law' (2022) 3 Science of Law (Journal of Northwest University of Political Science and Law) <https://doi.org/10.16290/j.cnki.1674-5205.2022.03.015>, pp 20-24.

⁷²⁹ Ibid, pp 20-21.

⁷³⁰ Ibid.

⁷³¹ *Zhu Ye v Baidu Company* (2014) Ning Min Zhong Zi No 5028; *Zhu Ye v Beijing Baidu Wangxun Technology Co., Ltd* (2013) Gu Min Xia Chu Zi No 2, 朱烨与北京百度网讯科技有限公司一审民事裁定书 (2013) 鼓民辖初字第2号; Zhu Ye discovered that while browsing websites at home and at work, using the Baidu search engine to look up specific keywords resulted in related advertisements appearing on certain websites. On May 6, 2013, Zhu Ye filed a lawsuit against Baidu Online Network Technology Co., Ltd..

⁷³² Ibid, section of the Judgment conclusion.

⁷³³ Ibid, p 9.

⁷³⁴ Ibid.

Although the EU does not entirely distinguish between personal information and privacy, it views personal data protection as a critical element of a broader right to privacy for individuals.⁷³⁵ This approach is reinforced by the GDPR, which treats the processing of personal data as an integral aspect of privacy protection, ensuring that individuals have control over their personal information in various contexts, including in electronic communications, as stated in the preamble of its E-Privacy Directive.⁷³⁶

‘Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms.’

This section aligns more with stances in the judgment of the trial court in *Ye*, which stated:⁷³⁷

Since Baidu’s website defaults to users consenting to the use of cookie technology to collect and utilise their BGI data, users may not even be aware that their private information is being collected and used, making it impossible for them to provide informed consent. Therefore, when setting default consent, Baidu should bear greater responsibility for providing clear explanations and reminders so that users can fully understand Baidu’s practices and make rational choices.

The conceptual confusion between personal information and privacy therefore lead to judicial uncertainty and inconsistencies in practical adjudication. While drafting the PIPL, Wang

⁷³⁵ See Chapters 2 and 4 *supra*.

⁷³⁶ See (24) of ‘Directive - 2002/58 - EN – E-privacy Directive - EUR-Lex’ (Europa.eu2024) <<https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng>>.

⁷³⁷ (2013) Gu Min Xia Chu Zi No 2.

Liming suggested that the legislation should be based on the distinction between the concepts of personal information and privacy in the *Civil Code*.⁷³⁸ This section agrees with such an approach: legislation should first clarify these concepts, similar to the interpretation provided in Part 1, Section 3 of the DPA 2018.⁷³⁹ However, the PIPL avoids addressing these academic debates and opts for the term ‘*personal information interests*,’⁷⁴⁰ revealing the legislature’s cautious stance. By framing the issue in terms of ‘interests’ rather than rights, the PIPL sidesteps the complexity of defining personal information as based on an unequivocal legal entitlement. The current version of the PIPL suggests a reluctance to fully embrace the notion of personal data as a standalone fundamental right, requiring the balancing of the rights to individuals with the demands of national security.

6.3.3 Lessons from the UK model: working on the Chinese data protection framework

To establish a solid data protection legal system that complements and potentially replaces the synergy between the *Civil Code*, lessons can be drawn from the UK model. Currently, the *Civil Code* and the PIPL are intertwined in terms of concept interpretation and the practical application of personal information. In broader data protection matters, the DSL and the PIPL then complement each other.⁷⁴¹ However, in practical cases, Chinese judges tend to favour

⁷³⁸ See Wang Liming, ‘Harmony in Diversity: The Rule Differentiation and Application of Privacy Rights and Personal Information’ (2021) 2 *Law Review* <https://doi.org/10.13415/j.cnki.fxpl.2021.02.002>, p 22.

⁷³⁹ [legislation.gov.uk](https://www.legislation.gov.uk), ‘Data Protection Act 2018’ (Legislation.gov.uk2018) <<https://www.legislation.gov.uk/ukpga/2018/12/section/3>>.

⁷⁴⁰ See Chapter 1 Art. 2 of the PIPL.

⁷⁴¹ See *supra* section 4.2 and section 5.3.

invoking the Art. 253 of the Criminal Law⁷⁴² for punitive measures and interpreting the PIPL for explanatory purposes.⁷⁴³

The UK organised its current data protection framework based on the DPA 2018 and the UK GDPR, as discussed and analysed in the previous Chapter 4.⁷⁴⁴ The current data protection framework in the UK entered a new phase of enhanced iteration with the adoption of the EU GDPR in 2016.⁷⁴⁵ Following Brexit, this regulation was retained in domestic law as the UK GDPR and is also reflected in the DPA 2018.⁷⁴⁶ This specialised legislation provides China with some legislative methods that could be emulated, namely that a special Data Protection Act could be drafted to support and complement the current PIPL. Further discussion and analysis of the comparison between the UK and China will be addressed in the following Chapter 7.

The UK model is a valuable reference for China's data protection legislation. Unlike the specialised nature of the UK's data protection system, which combines the DPA 2018 and the GDPR, the data protection framework in China interestingly exhibits a fragmented nature with a decentralised approach, as discussed above.⁷⁴⁷ Further, as mentioned, it is deployed in courts in an explanatory mode, rather than enabling individuals whose data has been misused with an avenue to be relied on to obtain remedies directly.

⁷⁴² Article 253 of the Chinese Criminal Law: Any postal worker who opens without authorisation or conceals or destroys mail or telegrams shall be sentenced to fixed-term imprisonment of not more than two years or criminal detention.

⁷⁴³ 'Part 4 of 5: Penalties and Liabilities under China's Data Protection Laws' (BCLP - Bryan Cave Leighton Paisner laws2022) <<https://www.bclplaw.com/en-US/events-insights-news/part-4-of-5-penalties-and-liabilities-under-chinas-data-protection-laws.html>>.

⁷⁴⁴ See *supra* pp 94-97.

⁷⁴⁵ See DLA Piper, 'Data Protection Laws in the United Kingdom - Data Protection Laws of the World' (Dlapiperdataprotection.com2024) <<https://www.dlapiperdataprotection.com/?c=GB>>.

⁷⁴⁶ Ibid.

⁷⁴⁷ Xinzhaio Pang, 'Civil Law Protection of Personal Information in the Era of Big Data' (2021) 08 OALib 1, pp 5-6.

6.4 The Right to Be Forgotten in the EU and Its Controversy in its Introduction to the Chinese Legal System

Viviane Reding, former Vice-President of the European Commission, first proposed in 2010 that people should be granted the right to control their online identity. This proposal was based on the recognition of the internet's powerful search and memory capabilities and was aimed at protecting online privacy, particularly in relation to the rights of children.⁷⁴⁸ The right to be forgotten was formally proposed in the EU in 2012, aiming to protect the privacy rights of data subjects by allowing individuals to request the deletion of their publicly available information on the internet to prevent it from adversely affecting their personal life in specific situations. This right was later incorporated into Article 17 of the GDPR, as discussed in Chapter 4.

Article 17(1) of the GDPR provides five other scenarios in which the right to erasure applies. Such erasure is requested when the data subject withdraws consent, consent expires, or when there is no legal basis for processing. Although Chinese law does not explicitly define a right to erasure, it grants the data subject a relatively narrow right to delete information online. For example, Article 47 of the PIPL provides that data subjects can request the deletion of their personal information from data controllers or a third party if they unlawfully collect or use their personal data.⁷⁴⁹

⁷⁴⁸ Viviane Reding, 'Privacy matters – Why the EU needs new personal data protection rules' (*The European Data Protection and Privacy Conference* 30 November 2010) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_10_700>.

⁷⁴⁹ Article 36 of the Tort Liability Law also provides that data controllers are liable for the unlawful collection or use of personal information. Deleting information is essentially one of the seven ways to assume liability for a tort, specifically the method of 'restoring the original state.'

The PIPL adopts a more limited approach, confining the right to data deletion strictly to instances where the original purpose for data collection has been fulfilled or the legal grounds for processing no longer exist. Despite the formal recognition of the right, the avenues available for individuals to autonomously enforce such protections remain markedly constrained, especially when directed against dominant digital platforms or actors with governmental affiliations. In practice, enforcement is largely contingent upon local regulatory authorities or judicial mechanisms, both of which may present significant procedural and structural barriers, thereby rendering effective redress challenging and, in many cases, impracticable.⁷⁵⁰

Although the PIPL establishes a framework for remedies, pursuing civil litigation remains fraught with significant obstacles, including prohibitive legal costs, limited relief, challenges in gathering sufficient evidence, and an overall lack of effective mechanisms for damage compensation.⁷⁵¹ While public interest litigation may result in substantial financial penalties for defendants, such penalties are often absorbed by the state treasury rather than being directed toward compensating the individuals whose personal data rights were infringed.⁷⁵²

6.4.1 Scholarly hypotheses on the right to be forgotten in China

Notice and Take Down Rule

Zhu Wei, in his research, put forward that the ‘notice and take down rule’ in Article 36, Paragraph 2 of China’s *Tort Liability Law* can provide the legal basis for the right to be

⁷⁵⁰ For example, the *Ren Jiayu* below.

⁷⁵¹ See Xinbao Zhang, ‘On the Exercise of the Right to Request Protection of Personal Information’ (2023) 2 *Tribune of Political Science and Law* 29 (in Chinese).

⁷⁵² Guosong Shao and others, ‘Assessing the Implementation of China’s Personal Information Protection Law: A Two-Year Review’ [2025] *International Data Privacy Law*, p 13<<https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipae022/8100448>>.

forgotten.⁷⁵³ This rule grants individuals the ability to notify the internet service provider to remove infringing content, which aligns closely with the concept of the right to be forgotten. Yang Lixin further argues that instead of introducing the right to be forgotten through legislation, it should be directly included in the protection of privacy rights in the *Civil Code*, which would be more feasible in Chinese judicial practice.⁷⁵⁴ This refers to Article 2, Paragraph 2 of the *Tort Liability Law* regarding privacy protection; courts could recognise the right to be forgotten as part of privacy rights and make rulings accordingly. Xue Li points out that as a specific personality right, the localisation of the right to be forgotten is constrained by the progress of China's personal information protection legal system. A feasible approach at present is to expand the interpretation of Article 111 of the *General Principles of Civil Law*, which has already come into effect, incorporating the interests protected by the right to be forgotten within its scope in judicial practice.⁷⁵⁵

This thesis argues, however, that such a right could conflict with the fundamental principle of freedom of expression.⁷⁵⁶ The implementation of this right could potentially undermine the protection of media freedom, as it would tend to be interpreted in court as limiting the ability of the media to access and disseminate information to public. It could be used in an overly restrictive manner since China's record on protection for media freedom is not in any event

⁷⁵³ Zhu Wei, 'The 'Right to Be Forgotten' Forgotten in the Era of Big Data' (China Social Sciences Network, 2014) http://www.cssn.cn/xwcbx/xwcbx_gcsy/201411/t20141125_1414903.shtml.

⁷⁵⁴ Yang Lixin and Du Zexia, 'Commentary on the Judicial Reasoning in China's First Case on the 'Right to Be Forgotten': *Ren Jiayu v Baidu* Company Reputation Dispute' (2017) 16 *Application of Law: Judicial Cases*, section 2 and 3; see also in Yang Lixin and Han Xu, 'Localisation and Legal Application of the Right to Be Forgotten in China' (2015) 2 *Journal of Law Application*, pp 28-30.

⁷⁵⁵ See online, Li Xue, 'Research on the Establishment of the Right to Be Forgotten in China under the Background of GDPR Implementation' (Ccssn.cn, 2018) http://iolaw.cssn.cn/fxyjdt/201906/t20190625_4923815.shtml.

⁷⁵⁶ Article 35 of the Chinese Constitution guarantees citizens' rights to freedom of speech, press, assembly, association, procession, and demonstration. However, in practice, these rights are heavily restricted by the government, often justified by concerns related to national security. The authorities employ extensive surveillance and censorship mechanisms to control the flow of information.

strong.⁷⁵⁷ This concern highlights a key tension in the debate over personal data protection: balancing individuals' privacy with broader societal interests. However, the right to be forgotten under the GDPR, as discussed in Chapter 5,⁷⁵⁸ is balanced against the protection for media freedom; it is not exercised successfully without due regard being paid to such freedom.⁷⁵⁹ Such a balance could also, in theory, be achieved in China.

The academic and legal debates surrounding the localisation of the right to be forgotten in China remain ongoing. Proponents of its introduction argue that it would help individuals reclaim control over their personal data online, particularly in the digital age. However, critics argue that its application could lead to censorship or excessive restrictions on the free flow of information. This tension between private life and freedom of expression has led to a careful and context-sensitive approach to the localisation of the right to be forgotten, discussed below.

6.4.2 *The quasi-foundational regulations for the right to be forgotten*

Beyond the traditional action of tort liability, the *Civil Code* establishes a new pathway for personal information protection, through the injunction framework affecting the protection of personality rights. Specifically, Article 997⁷⁶⁰ of the *Civil Code* introduces the personality rights injunction system, which allows individuals to plead to the court to cease violations if

⁷⁵⁷ See Amnesty International, 'Everything You Need to Know about Human Rights in China 2020' (Amnesty International 2023) Part of Freedom of expression, association and assembly <<https://www.amnesty.org/en/location/asia-and-the-pacific/east-asia/china/report-china/>>; see further on Harriet Moynihan and Champa Patel, 'Restrictions on Online Freedom of Expression in China the Domestic, Regional and International Implications of China's Policies and Practices International Law Programme Asia-Pacific Programme' (2021) <<https://www.chathamhouse.org/sites/default/files/2021-03/2021-03-17-restrictions-online-freedom-expression-china-moynihan-patel.pdf>>.

⁷⁵⁸ See *supra* section 5.4.2.

⁷⁵⁹ *NT1 & NT2 v Google LLC* [2018] EWHC 799 (QB); [2018] EMLR 18; [2018] HRLR 13; see discussion *supra* in pp 119-121, fn 601 and associated text.

⁷⁶⁰ Article 997 of 'Civil Code of the People's Republic of China' (2020) <https://regional.chinadaily.com.cn/pdf/CivilCodeofthePeople%27sRepublicofChina.pdf>, regulated as *..the person has the right, in accordance with law, to request the people's court to order the actor to stop the act.*

they have evidence proving that the defendant is committing or is about to commit an unlawful act invading their personality rights.⁷⁶¹

Section 5.1 of the *Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems*⁷⁶² also defines ‘deletion’ as ‘making personal information no longer usable in the information system.’ According to these guidelines, when a data subject has a legitimate reason to request the deletion of their personal information, the data controllers are obligated to promptly delete the relevant information online. This provision provides that personal data is not retained unnecessarily and should be removed when it no longer serves a legitimate purpose, reflecting the broader principles of the rights in relation to privacy of individuals.

Based on the above laws and regulations, there are three potential theoretical frameworks for the right to be forgotten that are already embedded within the Chinese legal system. These frameworks provide a foundation for integrating the right to be forgotten into Chinese law in a way that aligns with both existing legal principles and emerging trends in data protection; therefore, this section argues that the right to be forgotten could be appropriately incorporated into the Chinese legal system in the near future. The next section will analyse these bases and evaluate the effectiveness of the localisation of the RTBF through a landmark case in China, *Ren Jiayu v Baidu*.

⁷⁶¹ Article 1034 declares that ‘the personal information of natural persons is protected by law,’ provides a definition of personal information, and distinguishes between private and non-private information; Article 1035 sets out basic behavioural norms for personal information processing. The subsequent provisions address liability exemptions (Article 1036), three claims of personal information subjects (access and copying, correcting inaccuracies, and deleting unlawful processing), and prohibitions and obligations for personal information processors (Articles 1037–1039).

⁷⁶² *Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems*, (第 24 号) (*Wwww.gov.cn*2025) <https://www.gov.cn/gongbao/content/2013/content_2473881.htm>; This ‘guideline’ is not a law but falls under the category of soft law.

6.4.3 Case study (the first case): *Ren Jiayu v Baidu*

In 2015, China's first 'right to be forgotten' case draws attention; *Ren Jiayu v Baidu*,⁷⁶³ involved a request for Baidu to delete information about the plaintiff no longer working at a certain educational institution. The court did not support the request, citing the lack of legal interest justification and the lack of necessity for the protection of his personal data online.⁷⁶⁴ The courts held that the right to privacy protects personal information that has not been disclosed to the public. Since Ren's employment history had already been made public, it was not protected under the right to privacy.⁷⁶⁵ The information in question, Ren's recent professional experience, remains directly relevant and timely, as he is still active in the field of corporate education. This employment information constitutes a core component of his professional background and is directly related to his current personal credibility within the industry.⁷⁶⁶

*Google Spain*⁷⁶⁷ and the *Ren Jiayu*⁷⁶⁸ case are typical examples of disputes related to the right to be forgotten in the EU and China, illustrating the differences between the approaches to the two frameworks. Despite the highly similar circumstances in the facts of the two cases, the rulings of the cases were completely different. In *Google Spain*,⁷⁶⁹ the plaintiff requested the

⁷⁶³ *Ren Jiayu v Baidu* (2015) Beijing Haidian District People's Court, 21 July 2015 Hai Min Chu Zi No 17417; 09558.

⁷⁶⁴ See Xue Li, 'Research on the Establishment of the Right to Be Forgotten in China under the Background of the GDPR's Implementation' (2019) 2 *Legal Forum* (Online).

⁷⁶⁵ Such information serves as a crucial reference point for potential clients or students in evaluating his qualifications and reflects the integrity expected of someone in a teaching role. Thus, retaining and disclosing such information is objectively necessary for public awareness, including for individuals who may consider engaging with her services.

⁷⁶⁶ (2015) Hai Min Chu Zi No 17417; 09558; section of judgment reasons.

⁷⁶⁷ Case C-131/12.

⁷⁶⁸ (2015) Hai Min Chu Zi No 17417; 09558.

⁷⁶⁹ Case C-131/12.

removal of links related to personal information that was ‘incomplete, irrelevant (no longer relevant), or excessive (beyond the original purpose of processing),’ especially historical information, such as details about unpaid social security contributions and a forced home auction several years ago.⁷⁷⁰ On the other hand, in *Ren Jiayu*,⁷⁷¹ Ren claimed the right to delete the suggested search keywords displayed by the search engine through a specific algorithm.⁷⁷² In both cases, the personal information was uploaded and published through legal means. After that, the continued existence of this information became outdated and then brought negative comments that were detrimental to the individuals involved.

In *Ren Jiayu*, Ren’s main request was to remove outdated information to prevent its continued existence from negatively impacting his personal life, employment, and daily activities. Both judges of the trial and appeal court held that the right to be forgotten fell under the category of personality interests and should be protected accordingly under personality rights,⁷⁷³ which happens to show a judicial decision to agree with Yang Lixin’s view on the localisation of the right to be forgotten, indicating a broader judicial trend towards recognising the RTBF and the remedial needs for misusing of personal data in the digital era. However, in *Ren* itself, a ‘right’ of deletion did *not* overcome the other interests deemed to be at stake, in contrast to the outcome in *Google Spain*. This raises the question of whether, even if the RTBF was recognised more clearly in China, it would in practice lead to deletions of information, bearing *Ren* in mind.

6.5 Dynamic Balance? China’s Approaches to balancing Protection of Personal Information and Freedom of Expression

⁷⁷⁰ Ibid, § 15.

⁷⁷¹ (2015) Hai Min Chu Zi No 17417.

⁷⁷² Ibid, section: Plaintiff request.

⁷⁷³ Ibid, section: Reasons of Judgment.

6.5.1 The legal approach to the balancing test

Introducing the right to be forgotten could challenge press freedom and the public interest. Press/media freedom is a constitutional right in the Chinese legal system,⁷⁷⁴ although such protection is not fully established in practice, but the dynamic balancing mechanism between privacy and press freedom has not been fully established. The potential for the right to be forgotten to limit the accessibility of personal information and restrict media reporting has raised concerns about its impact on journalistic freedom. The state's position on freedom of expression can be discerned through its regulatory actions and enforcement practices.⁷⁷⁵ Chinese regulatory bodies have often cited Article 35 of the Chinese Constitution as a rationale for imposing restrictions on media reporting or data access, particularly when the content is deemed sensitive or conflicting with state-approved narratives.⁷⁷⁶ For example, in instances of online defamation or critiques of government officials, authorities have frequently justified these actions by invoking the need to safeguard national security or public order, thereby prioritising these concerns over individual media freedoms.⁷⁷⁷

In practice, Article 35 can be viewed as a tool that enables the state to limit media freedom when a perceived conflict arises between safeguarding personal data and fulfilling broader public policy or security objectives. This creates a precarious situation for journalists,

⁷⁷⁴ Article 35 of the Chinese Constitution guarantees freedoms of speech, assembly, association, and publication; In practice, Article 35 can be interpreted in a way that restricts media freedom, as the government may invoke national security or public order concerns to limit or regulate media access to personal data or restrict journalistic activities that challenge state policies.

⁷⁷⁵ See Karen M Markin, 'Discovering China's Free Expression Values' (DigitalCommons@ONU2024), p 6 <<https://digitalcommons.onu.edu/ilj/vol2/iss1/5>>; see case studies on Foreign & Commonwealth Office, 'Freedom of Expression in China' (GOV.UK12 March 2015) <<https://www.gov.uk/government/case-studies/freedom-of-expression-in-china>>.

⁷⁷⁶ Ibid, Markin (note 775) p 7.

⁷⁷⁷ Ibid, Markin (note 775) pp 11, 20-21.

especially those engaged in sensitive or investigative reporting, as the state could justify interference in their work under the pretext of protecting national security.

Thus far, judicial oversight on this matter has been insufficient, with regulatory bodies and courts largely deferring to the state's interpretation of public interest and national security.⁷⁷⁸ This raises crucial questions about the role of the judiciary in balancing privacy rights with media freedoms, ensuring that the latter are not excessively compromised for the sake of state control. The absence of established case law and precedent suggests that the application and interpretation of Article 35 will remain an evolving legal issue in China, particularly as international scrutiny on these matters intensifies.

The Chinese legal system has not developed a dynamic mechanism for creating a balance between personal information and press freedom. In this context, the challenge lies in striking an appropriate balance between protecting individuals' privacy rights and preserving the freedom of the press. A robust legal framework would need to carefully consider when and on what basis the right to privacy should outweigh the public interests, and vice versa, as discussed in Chapter 4 in relation to the GDPR. The establishment of a clear and transparent balancing mechanism would be essential to avoid arbitrarily broad applications of the right to be forgotten, while ensuring that it does not unduly restrict press freedom or the free flow of information. But it would also need to be able to ensure that where the information in question was of little public interest, as found in the case of *NT2*, the RTBF would prevail.⁷⁷⁹

⁷⁷⁸ See Yuxia Zhang and Zhuang Liu, 'The Rise of the Chinese Judiciary and Its Limits: Administrative Litigation in the Reform Period' [2024] SSRN Electronic Journal p 3.

⁷⁷⁹ See Fiona Brimblecombe and Helen Fenwick (note 320) p 471.

As debates continue in China regarding the potential introduction of the right to be forgotten, it is crucial for its legal system to develop guidelines that recognise the complexities of balancing privacy with public interests, including press freedom and national security. Before the *Civil Code* came into effect, the *Tort Liability Law* provided a broad provision for distinguishing between freedom of the press and the protection of private information.⁷⁸⁰ The *Civil Code* then established claims related to personal information, laying out the fundamental structure for its protection through principled provisions while leaving room for future legislation in this field.⁷⁸¹ Moreover, the PIPL provides a more abstract framework for establishing the legitimacy of personal information processing activities. It sets out both protective and restrictive measures for journalism and public oversight based on ‘public interest’ and ‘reasonable scope.’⁷⁸² While Chinese legislators have provided above laws for balancing protection of personal information with other interests closely tied to public interest, the existing laws and regulations lack clear guidelines as to the specific responsibilities, behavioural norms, and operational boundaries for the media in collecting and using personal information.

6.5.2 *Creating a flexible balancing mechanism in China?*

If the media is the battlefield for the conflicts between the public interest and privacy, where individuals often have a strong sense of self-rights in response to news reports, then the rapid development of social media has led people to become accustomed to disclosing personal

⁷⁸⁰ Arts. 1, 2, 36 of the *Tort Liability Law* 侵权责任法.

⁷⁸¹ See Jihong Chen and Yun Luo, ‘How China’s First-Ever *Civil Code* Protects Personal Information’ (Ibanet.org2020) <<https://www.ibanet.org/article/28ED74A0-4A46-4EC6-B786-796AA66061A8>> accessed 31 January 2025.

⁷⁸² ‘Article 13’ (PIPL2 March 2022) (V) where such acts as news reporting and supervision by public opinions are carried out for the public interest, and the processing of personal information is within a reasonable scope; <<https://personalinformationprotectionlaw.com/PIPL/article-13/>>.

information within these platforms,⁷⁸³ but in a number of more recent instances persons have challenged such disclosure, including in *Google Spain*, but also at Strasbourg. In the older case of *Egeland and Hanseid v Norway*,⁷⁸⁴ the Strasbourg Court ruled that prohibiting the media from publishing a photograph of a woman displaying intense emotional distress after receiving a 21-year prison sentence did not constitute a violation of press freedom. The Court held that Norway's prohibition on photographing individuals charged or convicted in the context of court proceedings was not anomalous within Europe, and thus there was no established European consensus against such restrictions. As a result, the Court afforded Norwegian authorities a broad margin of appreciation in reconciling the competing interests at stake. It concluded that the restriction served a legitimate aim, protecting the individual's right to privacy, and that this aim outweighed the press's interest in reporting on matters of public concern. The Court particularly noted that the photographs captured the woman in a moment of vulnerability and diminished self-control, which heightened the imperative to safeguard her personal dignity over the media's right.

The significant recent decision in *Hurbain v Belgium* in 2023 arose,⁷⁸⁵ in which the Article 8 right to be forgotten was invoked in relation to electronically archived material held by a media body and readily available for search purposes. The material did not concern someone in the public eye; it was also found domestically and at Strasbourg, to have limited public interest value since it lacked topicality. It concerned reporting on traffic accidents which included the

⁷⁸³ Raffael Heiss, Andreas Nanz and Jörg Matthes, 'Social Media Information Literacy: Conceptualization and Associations with Information Overload, News Avoidance and Conspiracy Mentality' (2023) 148 *Computers in Human Behavior* 107908 <https://www.sciencedirect.com/science/article/pii/S0747563223002595>, pp 2, 3.

⁷⁸⁴ *Egeland and Hanseid v Norway*, April 16, 2009, App. No. 34438/04.

⁷⁸⁵ App. no 57292/16 (ECHR, 4 July 2023). For discussion, see Hugh Tomlinson, '*Hurbain v Belgium*, Grand Chamber upholds decision that order anonymising newspaper archive did not violate Article 10' (26 July 2023) INFORRMBlog<<https://inform.org/2023/07/26/case-law-strasbourg-hurbain-v-belgium-grand-chamber-upholds-decision-that-order-anonymising-newspaper-archive-did-not-violate-article-10-hugh-tomlinson-kc>> accessed 28 February 2024.

applicant's involvement in a car crash some years previously and, as between a 'right to remember' and to be forgotten, the majority judges favoured the latter in the circumstances.

In the previous judicial practice, balancing privacy with the public interests and press freedom becomes a major challenge when introducing the right to be forgotten in China. To address online celebrities/influencers and the potential virality of information on public social media, the Supreme People's Court established criminal liability and possible imprisonment for publishing false information online if it is retweeted 500 times or viewed 5,000 times.⁷⁸⁶ In *Jianhua Xie v Qing Ye*,⁷⁸⁷ the defendant depicted the plaintiff as leading a criminal gang, engaging in manipulative practices for commercial gain, and harassing others, but failed to provide adequate evidence to support these allegations. The court further determined that the actions of the defendant damaged the plaintiff's reputation,⁷⁸⁸ and therefore, it ruled that the defendant should compensate the plaintiff for damages, despite the relatively low number of retweets, in the amount of 3,000 RMB and it also awarded an injunction (i.e. to immediately delete and remove the texts and photos concerning Xie from the original articles online and cannot publish them again).⁷⁸⁹

⁷⁸⁶ Rogier Creemers, 'The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy' (2023) 33 *Journal of Contemporary China* p 182; see cases in Supreme People's Court and Supreme People's Procuratorate, 最高人民法院最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释 (Interpretation concerning Some Questions of Applicable Law When Handling Uses of Information Networks to Commit Defamation and Other Such Criminal Cases, September 6, 2013, <http://chinacopyrightandmedia.wordpress.com/2013/09/06/interpretation-concerning-some-questions-of-applicable-law-when-handling-uses-of-informationnetworks-to-commit-defamation-and-other-such-criminal-cases/>).

⁷⁸⁷ *Xie vs. Ye* (2019) General Personality Rights Dispute, Zhe 0192 Min Chu 624 谢某、叶某一般人格权纠纷 (2019) 浙 0192 民初 6244 号, section of reasons.

⁷⁸⁸ *Ibid*, section: reasons of judgment.

⁷⁸⁹ With further decisions: the defendant must publish an apology statement for 30 consecutive days to restore the plaintiff's reputation. If the defendant fails to fulfil the obligations within the stipulated time or does not comply for the full duration, the court, upon the plaintiff's request, will select a newspaper in Hangzhou to publish the main content of the judgment at the defendant's expense.

Political and institutional factors have resulted in most media outlets possessing official backgrounds and receiving implicit governmental support in China.⁷⁹⁰ The Chinese government and legislative bodies place a strong emphasis on public power, a perspective that quite strongly contrasts with the Western focus on privacy rights.⁷⁹¹ Consequently, the *de jure* concept of individual rights, particularly privacy, whether online or offline, has not been afforded substantial *de facto* space in China. There are scholars who assert that, in order to safeguard the integrity of journalistic practices and prevent potential abuses in China, it is necessary to strictly limit the scope of those eligible to invoke the press/media exception.⁷⁹² As the practical efforts in defining the identity and role of the media and journalists within the legal framework remain apparently fairly minimal, the difficulties arising in establishing a flexible balancing mechanism in China are clear.

6.6 Conclusion

This chapter has analysed the personal data protection legal framework of China in four steps. It has discussed the advantages and weaknesses of the current data legal system and further conducted a case study on the right to be forgotten. The third section focused on the academic debates in the legal field regarding several concepts, such as personal information rights, highlighting the urgent need to clarify and accord further protection to fundamental concepts of privacy within the personal data legal framework of China.

By examining the fragmented Chinese legal system, four substantive pillars of personal information protection are identified: the *Civil Code*, the *Cybersecurity Law*, the *Personal*

⁷⁹⁰ See Zhang Wenliang and Liu Yuqi, 'On the News Exception in Personal Information Protection' (2024) 1 Human Rights CN.

⁷⁹¹ See Mark Jia (note 656) p 737.

⁷⁹² See Zhang Wenliang and Liu Yuqi (note 790).

Information Protection Law, and the *Data Security Law*, with a particular focus on the PIPL for detailed analysis. Comparing China's system with the European and UK data protection frameworks, this chapter argues that the PIPL still requires improvements, particularly in its broad and vague wording and its limited coverage of personal information protection. Enforcement and creating a balance with free expression remain a problem.

In Chapter 6, the focus was on presenting the foundational legal frameworks, principles, and regulations surrounding data protection and privacy rights, with a special emphasis on established legislations like the GDPR or PIPL. This chapter has covered how these laws intersect with media freedom, privacy concerns, and the mechanisms that exist for individuals to safeguard their personal information. Topics such as the right to erasure, consent, and data processing have been explored in depth, along with the challenges that individuals face in enforcing these rights, particularly when dealing with powerful corporate entities or government-linked bodies.

In contrast, Chapter 7 will delve into a more practical analysis of how these legal frameworks in China are applied and enforced in real-world scenarios. While Chapter 6 focused on the theoretical and regulatory aspects, Chapter 7 examines concrete examples and case studies illustrating how privacy violations and data protection laws play out within the media and online spaces in China. It will explore the delicate balance between privacy and freedom of expression, created in China, particularly in journalistic contexts, and investigate how media outlets or journalists navigate the complexities of privacy law while exercising their rights. Furthermore, Chapter 7 will look at the challenges in enforcement, the role of judicial oversight, and the practical difficulties faced when applying these laws across different jurisdictions. The chapter will come to conclusions as to the efficacy of data protection in China. Through this

lens, Chapters 7-8 combined will provide a more nuanced understanding of the implications of data protection laws, showing the tensions between safeguarding privacy and ensuring freedom of speech and expression in the digital era in China and in chapter 8 some comparisons will be drawn with the UK. Conclusions will be reached in relation to the research questions.

CHAPTER 7 CONCLUSIONS AS TO THE EFFICACY OF THE CHINESE PERSONAL DATA PROTECTION FRAMEWORK⁷⁹³

7.1 Introduction

Personal information is no longer understood merely as a matter of personal dignity or individual autonomy; increasingly, it is regarded as a critical economic asset.⁷⁹⁴ In the digital age, data fuels algorithmic systems, targeted advertising, and predictive analytics, making personal information one of the most valuable commodities in the global economy.⁷⁹⁵ In China, many cases of personal data violations occur, not from malice or ideological motives, but for commercial gain.⁷⁹⁶ Companies harvest, trade, and exploit user data to enhance profits, often with minimal user consent or transparency. This economic treatment of personal information brings into sharper focus Professor Alan Westin's long-standing concern about 'the preservation of privacy under the new pressures from surveillance technology.'⁷⁹⁷ While his original commentary centred on Western democracies, it is particularly resonant in the Chinese context, where state and corporate surveillance overlap in complex ways. China has been frequently criticised for its pervasive surveillance architecture, ranging from facial recognition

⁷⁹³ See for comparisons with the UK GDPR Chapters 2-4; Fiona Brimblecombe and Helen Fenwick, 'Protecting Private Information in the Digital Era' (2022) 73 Northern Ireland Legal Quarterly 26.

⁷⁹⁴ See Raymond Yang Gao, 'A Battle of the Big Three? —Competing Conceptualizations of Personal Data Shaping Transnational Data Flows' (2023) 22 Chinese journal of international law p 708.

⁷⁹⁵ See Hamid Mattiello, 'Exposing the Hidden Costs of "Free": Personal Data Commodification in the Digital Economy via X.0 Theory, Fuzzy Delphi, Thematic Analysis, and Problem-Solving Frameworks' (2025) 2 Journal of Policy and Society 2330, pp 2-4; see news on: The Economist, 'The World's Most Valuable Resource Is No Longer Oil, but Data' (The Economist 6 May 2017) <<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>>.

⁷⁹⁶ See Chi Zhang, 'China's Privacy Protection Strategy and Its Geopolitical Implications' (2024) 3 Asian Review of Political Economy, p 8; Rogier Creemers, China's Emerging Data Protection Framework (2022) Journal of Cybersecurity 8 (1): tyac011. <https://doi.org/10.1093/cybsec/tyac011>.

⁷⁹⁷ Alan Westin, 'Privacy and Freedom' (1968) 25 Washington and Lee Law Review 166 <<https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20>>.

in public spaces to social credit systems,⁷⁹⁸ that allow public authorities to monitor citizens on unprecedented scales.

Legal systems across jurisdictions tend to regulate privacy and personal data protection through distinct legislative frameworks. As this thesis has discussed, the EU provides a notable example: the GDPR is primarily concerned with the processing and safeguarding of personal data, whereas issues more traditionally associated with privacy, such as intrusions upon seclusion or reputation, are addressed within broader civil or tort law areas.⁷⁹⁹ Privacy and data protection can be viewed as grounded in differing normative foundations and tend to serve distinct legal functions. The EU explicitly recognises the protection of personal data as an autonomous constitutional right. Article 8 of the EU Charter of Fundamental Rights declares: ‘*Everyone has the right to the protection of personal data concerning him or her.*’⁸⁰⁰ This recognition elevates data protection to the status of a new-generation fundamental right, one that is conceptually and functionally distinct from the right to privacy in the Charter.⁸⁰¹ The values it seeks to uphold, the risks it seeks to mitigate (e.g., algorithmic discrimination, surveillance capitalism), and the mechanisms of enforcement (e.g., data subject rights, regulatory authorities) all indicate a unique legal identity.⁸⁰²

⁷⁹⁸ See Xiongbiao Ye and others, ‘Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective’ (2024) 48 Telecommunications Policy 102851, p 3.

⁷⁹⁹ See van Ooijen and Helena U Vrabec, ‘Does the GDPR Enhance Consumers’ Control over Personal Data? An Analysis from a Behavioural Perspective’ (2018) 42 Journal of Consumer Policy 91 <<https://link.springer.com/article/10.1007/s10603-018-9399-7>>.

⁸⁰⁰ Article 8 of the EU Charter of Fundamental Rights.

⁸⁰¹ See Maria Tzanou, ‘Data Protection as a Fundamental Right next to Privacy? “Reconstructing” a Not so New Right’ (2013) 3 International Data Privacy Law p 89, and the section of Dancing together apart: Privacy and data protection.

⁸⁰² See Xiongbiao Ye and others (note 798) p 3.

China's legal landscape further illustrates the divergence between these two domains. Traditionally, Chinese law conceptualises privacy as an absolute right,⁸⁰³ emphasising a categorical protection of private life against infringement. However, personal data in the digital age transcends the private sphere, often encompassing commercial interests, public administrative functions, and national security considerations. This multidimensional nature of personal data necessitates a governance model that balances competing values and interests, something privacy law alone cannot adequately achieve.

Reflecting this complexity, Chinese legal doctrine increasingly regards personal information as a *sui generis* personality right, distinct from the right to privacy.⁸⁰⁴ This view has been codified in the Civil Code of China, which separately recognises the right to privacy (Article 1032) and the rights and interests associated with personal information (Article 1034). Importantly, the Civil Code anticipates areas of intersection and potential conflict between these two domains by providing that, in instances where personal information overlaps with privacy interests, either the provisions on the right to privacy or, where lacking, those on data protection shall apply.⁸⁰⁵ This interpretive flexibility affirms the conceptual independence of the two rights while also offering a framework for managing their overlap.⁸⁰⁶

⁸⁰³ See Jingchun Cao, "Protecting the Right to Privacy in China" [2005] 36(3) Victoria University of Wellington Law Review 645, p 645.

⁸⁰⁴ See Cheng Xiao, On nature of the right and interest of personal information in the Civil Code of China, (2020) Political Science and Law, p 8.

⁸⁰⁵ See Igor Calzada, 'Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)' (2022) 5 Smart Cities 1129, pp 1133-1135; Liming Liu, 'Governing Data in China | New College of Interdisciplinary Arts and Sciences' (Asu.edu2025) <<https://newcollege.asu.edu/global-human-rights-hub/fellows-program/ghr-fellows-blog/liming>>.

⁸⁰⁶ See Xiongbiao Ye and others, 'Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective' (2024) 48 Telecommunications Policy 102851, p 3.

If it approaches the concepts of personal information and the related concepts of privacy from a more philosophical and comparative perspective, the narrative becomes less straightforward. Privacy is not a universally fixed concept.⁸⁰⁷ Instead, it is a socially constructed and culturally contingent value, its significance shaped by historical, political, and normative understandings. In most democracies, privacy is often seen as a shield against state intrusion and a foundation for individual liberty.⁸⁰⁸ In China, by contrast, the concept of privacy has traditionally taken a collectivist orientation,⁸⁰⁹ whereby the public interest and social harmony are frequently prioritised over individual rights.⁸¹⁰ This cultural orientation helps explain why certain practices that might be seen as privacy violations in the West are more tolerated, or even accepted, in China, especially when they are framed in terms of the interests in economic development, public safety, or national security.⁸¹¹ The philosophical dilemma, then, is whether privacy can be meaningfully asserted as a universal human right,⁸¹² or whether it must be understood in relation to the political and social norms of each society.

A prominent case illustrating the urgency of data protection in China is that of *Xu Yuyu*,⁸¹³ in which the victim, a high school graduate, committed suicide from shock after falling prey to a

⁸⁰⁷ See Deirdre K Mulligan, Colin Koopman and Nick Doty, 'Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy' (2016) 374 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20160118 <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5124066/>>; Daniel J Solove, *Conceptualizing Privacy*. (2002) 90 *California Law Review* 1087 Available at SSRN: <https://ssrn.com/abstract=313103>; Sharon Mason, 'Exploring Privacy from a Philosophical Perspective: Conceptual and Normative Dimensions' [2024] *Technology, work and globalization* 23.

⁸⁰⁸ See discussion section 2.1 *supra*.

⁸⁰⁹ Chi Zhang, 'China's Privacy Protection Strategy and Its Geopolitical Implications' (2024) 3 *Asian Review of Political Economy*, p 2.

⁸¹⁰ See Randall Peerenboom, 'China's Long March toward Rule of Law' [2002] Cambridge University Press, pp 61, 62.

⁸¹¹ See Zhen Troy Chen and Ming Cheung, 'Privacy Perception and Protection on Chinese Social Media: A Case Study of WeChat' (2018) 20 *Ethics and Information Technology* 279, pp 2-3.

⁸¹² See Karen M Markin, "Discovering China's Free Expression Values," [2024] *Ohio Northern University International Law Journal*: Vol. 2, Article 5. Available at: <https://digitalcommons.onu.edu/ilj/vol2/iss1/5>, p 14.

⁸¹³ See 'Girl's Death Raises Public Concerns about Personal Information Leakage | Chinlingo' (Chinlingo.com2016) <<https://www.chinlingo.com/articles/801773/>>.

targeted telecom scam enabled by the illicit acquisition of her university admission data. The *Xu* case triggered nationwide concern regarding the risks of personal data breaches and catalysed the legislative momentum for data protection. Although the existing Criminal Law provides for criminal liability in cases involving the unlawful acquisition of personal data, practical enforcement remains hindered by difficulties in evidence collection, lenient sentencing, and the clandestine nature of the illegal data trade.⁸¹⁴ More critically, victims often struggle to pursue civil remedies, indicating that personal information has yet to be widely recognised as an independent civil right, and that although the PIPL has filled certain regulatory gaps, its implementation in civil redress mechanisms remains underdeveloped.

Accordingly, this Chapter will be divided into three sections to examine China's current stance on data protection and critically assess the effectiveness of the PIPL through relevant case studies. The first section (7.2) explores how personal data is increasingly treated as a commercial asset in China's digital economy and considers the resulting implications for individual personal data rights. The second section (7.3) traces the progression of China's data protection framework and compares its regulatory mechanisms and remedies to those found in other jurisdictions. The third section (7.4) examines how China balances personal information protections with freedom of expression, particularly comparing the protections to those of the GDPR and the DPA 2018, as discussed in Chapters 3-5. The Chapter concludes by evaluating the current Chinese legislative framework and identifying existing gaps.

This Chapter draws on the discussions from Chapter 6 as regards the Chinese situation, in order to come to conclusions as to the level of protection offered, and the political and cultural

⁸¹⁴ See discussion in Chapter 6, p 195.

context affecting that level. Throughout this chapter, it introduces a comparative element with the GDPR/DPA 2018 by examining China's legal framework regarding the misuse of personal data online. Building on the comparative approach, the seventh chapter deepens the analysis of China's legal system by evaluating its foundational principles, enforcement mechanisms, and institutional capacity in protecting personal information online. It considers the roles of various actors including the CAC, courts, and private litigants.

7.2 The Commodification of Privacy: Rethinking Data Protection in the Chinese Context

7.2.1 The socio-historical concepts of privacy in China

While PIPL introduces personal information protections, as discussed in Chapter 6, it does so within a framework that remains sensitive to the imperatives of state control, economic growth, and technological innovation. The Chinese legal framework concerning privacy and personal information cannot be fully understood without considering the broader historical, cultural, and ideological context. The subordination of individual rights to collective welfare is not simply a legislative feature but reflects enduring societal values shaped by long-standing institutional and philosophical legacies.⁸¹⁵ As China continues to engage with the challenges of digital modernity and global integration, its approach to data governance will be likely to remain anchored in this distinctive normative context. The growing commodification of personal information, combined with state surveillance capabilities, demands a more practical

⁸¹⁵ See Christopher McCrudden, 'Human Dignity and Judicial Interpretation of Human Rights' (2008) 19 *European Journal of International Law* 655, pp 710, 722 <<https://academic.oup.com/ejil/article/19/4/655/349356>>; Richard Arneson, 'Egalitarianism' (Stanford Encyclopedia of Philosophy 2013) <<https://plato.stanford.edu/entries/egalitarianism/>>.

understanding of modern privacy online: one that recognises both the material value of data and the moral-political dimensions of its protection.⁸¹⁶ The Chinese experience invites this Chapter to reflect on how personal information is interpreted and instrumentalised differently across societies, and whether digital governance can, or should, attempt to reconcile these divergent perspectives.

To understand the Chinese traditional approach to privacy, one must consider the socio-historical contexts that have shaped its societal values and legal norms. Privacy, as a concept, has not been traditionally emphasised in Chinese society at governmental, legal, or societal levels.⁸¹⁷ This lack of focus on privacy is not merely the result of policy decisions but is deeply rooted in the nation's historical experiences. The scars of World War II and the subsequent struggles for survival and national rejuvenation left an indelible mark on Chinese society, necessitating a focus on survival and rebuilding that left little room for cultivating societal notions such as privacy. Moreover, Chinese society has historically prioritised substantive needs such as security and economic needs over psychological or philosophical concerns such as freedom of expression and privacy.⁸¹⁸

Chinese philosophical traditions, rooted in Confucianism, placed greater emphasis on collective harmony, familial obligations, and societal order rather than individual rights, as discussed in Chapter 6.⁸¹⁹ Unlike Western philosophical traditions that foreground individual

⁸¹⁶ See Matthew Crain, 'The Limits of Transparency: Data Brokers and Commodification' (2016) 20 *New Media & Society* 88, pp 97-99.

⁸¹⁷ Kenneth Neil Farrall, *Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S.*, (2008) 2 *International Journal of Communication* 993, p 995, <<https://ijoc.org/index.php/ijoc/article/viewFile/370/228>>.

⁸¹⁸ Karen M Markin, 'Discovering China's Free Expression Values' (DigitalCommons@ONU2024) <<https://digitalcommons.onu.edu/ilj/vol2/iss1/5>>, p 8.

⁸¹⁹ See *supra* section 6.2.2.

liberties, classical Chinese philosophy seldom addressed privacy as a distinct legal or moral category.⁸²⁰ For example, in *Yang Lijuan*,⁸²¹ a young woman from Gansu province, was a fan of Liu Dehua, a Hong Kong movie star. Yang's parents suffered not only financial pressure but also huge psychological stress because of her long-term adulatory activities, and in March 2007, Yang's father jumped to his death in the sea in Hong Kong. Southern Weekly, a social media site in Guangdong province, published a lengthy article on Yang's adulation of the actor and the death of her father. Shortly after the publication of this article, Yang and her mother brought a lawsuit in the local court against the Southern Weekly for invasion of their privacy.

However, the results were that none of the court rulings supported the claims of the plaintiffs. The decisions in this case indicate that when faced with direct conflicts between individual privacy and collectivist values, those above being marital loyalty, expectations of good behaviour and filial piety respectively, Chinese courts tread carefully and frequently choose to take a stand with the latter. The plaintiffs did not obtain the support of the courts because their previous 'immoral' behaviour (in the view of the court) challenged the common values of the collective, which is rooted in traditional Confucian heritage and socialist ideologies.⁸²² It could be argued that the parents did exemplify the collectivist value of family loyalty by aiding their daughter in her adulation, which encourages societal stability, but clearly the court did not take that view or it considered that the other collectivist values were more significant.

⁸²⁰ Karen M Markin, 'Discovering China's Free Expression Values' (DigitalCommons@ONU2024) <<https://digitalcommons.onu.edu/ilj/vol2/iss1/5>>, p 17.

⁸²¹ *Yang Lijuan v Southern Weekly* (2008) Guangdong Guangzhou Intermediary People's Court, Civil Second Instance, No. 3871.

⁸²² See Snejina Michailova and Kate Hutchings, "National Cultural Influences on Knowledge Sharing: A Comparison of China and Russia" (2006) *Journal of Management Studies* 43, pp 392-394.

This philosophical orientation has translated into a legal framework whereby collective interests often take precedence over individual privacy. Given these historical and philosophical echoes, it is not surprising that Chinese legislators tend to prioritise economic development in the early stages of policymaking. The enactment of laws related to personal information (such as the PIPL) reflects this pragmatic orientation, which seeks to balance modernisation and economic growth with emerging concerns about privacy. However, this approach may create friction in relation to trading partners, particularly with partners such as the EU, which upholds stringent data protection standards under the GDPR. If China's data governance is perceived as insufficiently protective of individual rights, trading partners may hesitate to transfer personal data across borders. The EU's adequacy framework restricts data flow to countries that fail to provide 'essentially equivalent' protection. The collectivist emphasis on economic development could therefore conflict with the expectations of trading partners, making it more difficult to conclude comprehensive trade agreements or data transfer mechanisms.

7.2.2 The evolution of data protection in China: Statutory developments and practical challenges

While China lacks explicit constitutional protection for the right to privacy, its statutory framework has evolved to include an increasingly sophisticated set of legal safeguards,⁸²³ as discussed in Chapter 6.⁸²⁴ The introduction of an explicit 'right to privacy' in the Civil Code

⁸²³ See Kenneth Neil Farrall, *Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S.*, (2008) 2 *International Journal of Communication* 993, pp 1005-1006, <<https://ijoc.org/index.php/ijoc/article/viewFile/370/228>>.

⁸²⁴ *supra* section 6.3.

marked a significant milestone in this evolution. This development was not merely a response to shifting domestic public sentiment or reactive policymaking; rather, it was shaped by a combination of internal and external pressures.⁸²⁵ As McDougall observes, the legal context suggests that the Civil Code was drafted within the parameters of an international legal framework shaped by free-market ideologies, particularly those endorsed by the World Trade Organisation and the U.S. government.⁸²⁶

Under the Civil Code, Article 1032(1) affirms that ‘a natural person enjoys the right to privacy.’⁸²⁷ Paragraph 2 of the same article further defines ‘privacy’ as referring to ‘a natural person’s private peace of life and the private space, private activities, and private information that he or she does not wish to be known to others.’⁸²⁸ This definition incorporates a modern understanding of informational privacy, and the accompanying provisions introduce data processing standards similar to those found in prior regulatory instruments; which include rights to access, correct, and delete personal information, paralleling key principles found in data protection frameworks.⁸²⁹ The definition of personal information is based on the comparative law principle of identifiability, meaning that any information which can directly or indirectly identify a specific natural person should be regarded as personal information. Recognising that certain personal information may also contain private content, Article 1034(3)⁸³⁰ provides that *for confidential information within personal information, the provisions relating to the right to privacy shall apply; in the absence of such provisions, the provisions on the protection of personal information shall apply.* Although this legislative

⁸²⁵ See Kenneth Neil Farrall (note 823) pp 1005-1006.

⁸²⁶ See Bonnie S McDougall, ‘Privacy in Modern China’ (2004) 2 History Compass, p 6.

⁸²⁷ See Mark Jia (note 656) p 750; Civil Code, arts. 1032–1039.

⁸²⁸ Civil Code of the People’s Republic of China, art. 1032.

⁸²⁹ Ibid.

⁸³⁰ Ibid, art. 1034.

design attempts to bridge the conceptual and procedural gap between privacy and personal information, it also reflects the fact that personal information rights have not yet achieved full independence as a distinct legal interest, and the boundary between relevant data protection laws remains blurred in judicial practice.⁸³¹

This legislative progress gives rise to a deeper re-evaluation of the concept of privacy itself. Traditionally conceived as a deeply personal and subjective experience, privacy is often associated with autonomy, the capacity of individuals to control access to their private lives and information.⁸³² It is not solely a legal entitlement but also a psychological and social condition that depends on one's perception of personal boundaries and the ability to maintain them free from unwanted interference.⁸³³ Moreover, the rapid advancement of technology has prompted the Chinese government to increasingly rely on legal instruments to navigate and manage competing privacy interests.⁸³⁴ While these legal developments represent significant steps toward formal privacy protection, they also reflect the ongoing tension between state authority, societal control, and individual autonomy.

Despite the fact that the PIPL defines personal information as *various kinds of information that can identify a natural person either independently or in combination with other information* and establishes specific processing rules and associated rights and obligations, ambiguity persists in judicial practice regarding applicable standards. For example, the law does not offer a categorical classification of non-traditional identifiers such as geolocation data, device

⁸³¹ See relevant discussion in Chapter 6 at pp 182-186.

⁸³² See discussion in Chapter 2, section 2.1.

⁸³³ Ibid.

⁸³⁴ See Mark Jia (note 656) p 748.

fingerprints, or behavioural tracking information. This issue is particularly evident in the previous case of *Zhu Ye v Baidu Inc.*,⁸³⁵ where the court held that ‘online behavioural traces’ did not fall within the scope of personal information, and thus Baidu was not held liable.⁸³⁶ The court’s conservative interpretation of identifiability of personal information online and its failure to accommodate emerging concepts such as weak or indirect identifiability reflect a disconnect between the law and the technological realities it is meant to regulate, and indicate the insufficiency of the current legal definition of personal information in China in responding to the intricacies of modern data protection.

7.3 China’s Evolution Toward Data Protection Law: A Comparative Analysis of Regulatory and Remedial Schemes

7.3.1 Disclosing/facilitating online actors; threats to private information and its remedies

China, often viewed as the world’s most famous autocracy and the architect of a sophisticated surveillance state, has often been labelled as Orwellian, techno-totalitarian, and the ‘perfect police state.’⁸³⁷ Given this context, it may seem paradoxical that China would sponsor privacy protections, either online or offline.⁸³⁸ However, in recent years, several laws have been introduced that, on the surface,⁸³⁹ were aimed at safeguarding personal information. Some

⁸³⁵ (2014) Ning Min Zhong Zi No. 5028.

⁸³⁶ Ibid, judgment of reason; see discussion in Chapter 6, section 6.4.3.

⁸³⁷ See Mark Jia (note 656) pp 735-736.

⁸³⁸ See Jin Li, Yulan Zhang and Jian Mou, ‘Understanding Information Disclosures and Privacy Sensitivity on Short-Form Video Platforms: An Empirical Investigation’ (2023) 72 Journal of Retailing and Consumer Services 103292 pp 9-10; Mark Jia (note 656) pp 735-736.

⁸³⁹ *supra* chapter 6, section 6.2.

aspects of these laws are said to resemble the GDPR, which is seen as providing a global standard for data protection.⁸⁴⁰

When personal data is unlawfully disclosed or misused, legal remedies in China remain relatively limited.⁸⁴¹ Defendants are typically subject to injunctive relief, public apologies, and monetary compensation. However, there is no standardised framework for calculating damages in China (except under the Criminal Law), and courts tend to determine monetary compensation on a case-by-case basis, resulting in inconsistencies and uncertainty. Given that China does not follow a common law system, prior judgments do not carry binding authority, complicating the establishment of a coherent and predictable framework for monetary damages.

Although the PIPL stipulates liability in the form of both economic damages and administrative penalties, it provides little guidance on the expected quantum of damages. This lack of uniformity results in significant variations in compensation, which diminishes the law's deterrent effect and fails to provide meaningful redress for victims. Moreover, the notion of a public apology in the media may be seen as a second harm to victims, as it could cause additional damage to their reputation or privacy. However, its significance in the legal landscape lies in how such an apology serves to acknowledge wrongdoing and hold parties accountable. The legal system must balance the need for privacy protection with the potential consequences of publicly acknowledging harm.

⁸⁴⁰ See discussion in Chapters 4 and 5; especially “*Brussels effect*” in pp 101-102.

⁸⁴¹ See Yang Feng, ‘The Future of China’s Personal Data Protection Law: Challenges and Prospects’ (2019) 27 Asia Pacific Law Review 62, Part III. Safety-oriented Legislation: Features and Problems.

As discussed in Chapter 6,⁸⁴² China's personal data protection regime is characterised by legislative fragmentation, with relevant provisions scattered across the Civil Code, Cybersecurity Law, Data Security Law, and the PIPL. This scattered structure complicates the application of law in judicial proceedings, particularly in complex cases where courts struggle to base decisions on a unified legal framework. At present, the judicial protection of personal information in China largely relies on the traditional legal frameworks of the right to privacy and defamation.⁸⁴³ Due to the absence of 'personal information' as an independent right within the legal system, courts often face a lack of clear and unified legal grounds in adjudication, resulting in limited protection for individuals.⁸⁴⁴ Against this backdrop, the PIPL undoubtedly provides a more systematic and *ex ante* legal framework for the protection of personal data in China. However, its practical application continues to encounter numerous challenges and difficulties.

Despite certain surface-level similarities, China's data protection laws do not align with those in western nations.⁸⁴⁵ These statutes include broad, unreviewable exceptions that enable state surveillance, and their enforcement also reflects the irregularities and opacity of Chinese legal practice.⁸⁴⁶ Rather than limiting the state's power, these laws function as mechanisms that support and legitimise surveillance.⁸⁴⁷ As Rogier Creemers has noted, this framework enables the government to regulate specific entities while ensuring that law enforcement and security

⁸⁴² *supra* pp 200-202.

⁸⁴³ See Anja Geller, 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective' (2020) 69 GRUR International, p 1198; Lu Zhang, "'Personal Information of Privacy Nature" under Chinese Civil Code' (2021) 43 Computer Law & Security Review 105637, pp 2-3.

⁸⁴⁴ *Ibid*, Lu Zhang, p 2.

⁸⁴⁵ *Ibid*, Mark Jia (note 656) p 736.

⁸⁴⁶ See Rogier Creemers, 'China's Emerging Data Protection Framework' (2022) 8 Journal of Cybersecurity, p 6.

⁸⁴⁷ *Ibid*, Mark Jia (note 656) p 737.

agencies retain unfettered access to personal data.⁸⁴⁸ Nevertheless, these laws are treated as formal legal statutes within the country, functioning arguably in the same way as tort or contract law.⁸⁴⁹

a) evidentiary chain: burden of proof

This situation generates a systemic tension: while privacy is promoted as a legal value, it is ultimately subordinated to the imperatives of state security.⁸⁵⁰ In practice, privacy is frequently sacrificed on the altar of national security in China,⁸⁵¹ a social value often invoked to justify governmental overreach. Alarming, much of this sacrifice occurs in the name of ‘security theatre:’⁸⁵² measures that provide the illusion of safety without genuinely improving security. The case of *Pang Lipeng v China Eastern Airlines & QuNar*⁸⁵³ offers a compelling illustration of these issues within the Chinese legal framework. Mr. Pang purchased a ticket via QuNar.com, a third-party online travel agency, for a flight operated by China Eastern Airlines. Shortly thereafter, he received a fraudulent SMS suggesting flight cancellation, which he identified as a scam. Claiming that the leak of his personal information: specifically, his name, phone number, and travel itinerary, facilitated the fraud, Mr. Pang brought a privacy claim against both the airline and the platform operator. The trial court dismissed the claim due to insufficient

⁸⁴⁸ Rogier Creemers, ‘China’s Emerging Data Protection Framework’ (2022) 8 Journal of Cybersecurity, p 6.

⁸⁴⁹ See discussion about “legal status of the PIPL” in section 6.3.

⁸⁵⁰ See Jamie P. Horsley, How Will China’s Privacy Law Apply to the Chinese State? (2021) Brookings Inst. <https://perma.cc/4UGA-CWQK>.

⁸⁵¹ See Robert Weatherley, ‘The Right to Privacy, the Right of National Security and the Challenges Posed by New Technology in the UK A...’ (Lexology 8 September 2011)

<<https://www.lexology.com/library/detail.aspx?g=8f33dbaf-9272-4818-82db-d86284ea5313>.

⁸⁵² See Daniel J Solove, ‘Why is Privacy Important?’ On Privacy and Technology (New York, NY, 2025; online edn, Oxford Academic, 3 Jan. 2025), p 10, <https://doi.org/10.1093/9780197771716.003.0004>; further on Bruce Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World 38–39 (2003).

⁸⁵³ *Pang v Beijing Qunar Information Technology Co., Ltd. et al.* (2017) Jing 01 Min Zhong No. 509.

evidence of direct causation between the scam and the leak of the personal information.⁸⁵⁴ On appeal, however, the Court of Appeal held that there existed a high degree of probability⁸⁵⁵ that the personal data was leaked by either China Eastern or QuNar,⁸⁵⁶ thus permitting liability under tort of the privacy violations under the Civil Code.

In contrast to the approach seen in *Lloyd v Google LLC*,⁸⁵⁷ where the courts emphasised the need to prove actual damage or distress,⁸⁵⁸ the Chinese courts appear more flexible about this, at least where the risk of harm is deemed substantial. This suggests that Chinese courts are increasingly adopting a risk-based approach to personal data protection, echoing trends seen in the EU,⁸⁵⁹ where the existence of a duty to safeguard user data and the foreseeability of harm may establish a *prima facie* liability even in the absence of direct causation. However, unlike the UK data protection regime, Chinese courts have not yet developed a clear distinction between data controllers and processors, nor do they impose corresponding regulatory obligations.⁸⁶⁰ This leads to broader, and potentially more discretionary, judicial assessments of liability. From *Pang*, it is clear to see that, in the Chinese jurisprudence, the appellate court did not explicitly invoke the concept of joint data control, but it analogously assigned potential liability to both parties based on probabilistic reasoning.

⁸⁵⁴ *Pang v Beijing Qunar Information Technology Co., Ltd. et al.* (2015) Hai Min Chu No. 10634.

⁸⁵⁵ (2017) Jing 01 Min Zhong No. 509, section of judgment reasons.

⁸⁵⁶ In the UK, where multiple data controllers or joint controllers are involved, Article 26 of the GDPR imposes a duty to transparently delineate responsibilities. If QuNar and China Eastern were joint controllers, each would be liable for any processing that infringes upon a data subject's rights unless they can prove they were not responsible for the event causing the damage (Article 82(3)).

⁸⁵⁷ [2021] UKSC 50.

⁸⁵⁸ *Ibid.*, §§ 90 - 143.

⁸⁵⁹ See C-101/01 *Bodil Lindqvist* (2003) and C-131/12 *Google Spain SL* (2014) para 36; see comments on Tuulia Karjalainen, 'All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm' (2022) 8 European Data Protection Law Review 19; Gabriel Maldoff and Westin Fellow, 'The Risk-Based Approach in the GDPR: Interpretation and Implications' (2016) <https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf>.

⁸⁶⁰ See Anja Geller, 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective' (2020) 69 GRUR International, pp 1193-1194.

This Chapter contends that such a conclusion suffers from certain logical flaws and arguably lacks sufficient analytical rigor. Substantively, what Mr. Pang demonstrated at the trial level was merely the state of data breach concerning his personal information and the fact that such information had been held by the respondents, namely Qunar (a subsidiary of QuNa Company) and China Eastern Airlines. On this basis, the court's characterisation of the evidence as forming a 'complete evidentiary chain' appears overly expansive and lacks strict doctrinal support.

In the appellate judgment of *Pang*, the Court of Appeal held that the evidence submitted by Pang at the trial court met the basic requirements in both formal and substantive terms, thereby establishing a complete evidentiary chain.⁸⁶¹ In reality, Mr. Pang did not discharge the evidentiary burden of proving that the respondents committed the act of disclosing his personal information; in other words, he failed to directly identify the tortfeasor responsible for the alleged information leak.⁸⁶² What he established was a factual inference of infringement, the existence of a compromised privacy interest, rather than direct evidence of the infringing act itself. Such a structure of proof aligns more closely with the notion of *prima facie* factual self-proving in civil law systems, particularly in regard to foundational facts, rather than with the traditional model of a closed and coherent evidentiary chain. From the standpoint of traditional evidentiary rules, the plaintiff arguably failed to substantiate the act element of tort liability and thus ran the risk of having his claim dismissed for failure to meet the burden of production.

⁸⁶¹ See *Pang v Beijing Qunar Information Technology Co., Ltd. et al.* (2017) Jing 01 Min Zhong No. 509, section of judgment reasons.

⁸⁶² *Ibid*, section of case fact.

Nevertheless, what merits closer scrutiny is the fact that the appellate court did not confine itself to the traditional framework of evidentiary assessment. Instead, it adopted a public-policy-oriented approach, asserting the proposition that entities exercising control over personal data bear an enhanced duty of care with respect to information security.⁸⁶³ In doing so, the court effectively introduced an evidentiary framework analogous to the rebuttable presumption under English law. Specifically, once the plaintiff had established the following test: (i) the occurrence of a privacy breach; (ii) that the defendants had control over the relevant data; and (iii) that the leaked information was not publicly known or readily accessible, the evidentiary burden shifted to the defendants to rebut the presumption of wrongdoing. Failing such rebuttal, the defendants were deemed to bear the adverse consequences of their inability to adduce exonerating evidence. This inversion of the burden of proof marks a notable departure from the classical *Actori incumbit onus probandi* principle and reflects a redistribution of evidentiary duties favouring the data subject, premised on the asymmetry of information control.

Crucially, this case illustrates an instance in which the Chinese judiciary prioritised privacy interests, suggesting that the common perception of China as largely indifferent to personal data protection may not fully capture the complexities involved. While the broader legislative and policy framework often places societal concerns such as national security and economic development above individual privacy, this judicial approach reveals a more nuanced reality.⁸⁶⁴ It demonstrates that privacy protection can, at times, be robustly upheld in Chinese courts,

⁸⁶³ Ibid, section of judgment reasons.

⁸⁶⁴ See Igor Calzada, 'Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)' (2022) 5 Smart Cities 1129 <<https://www.mdpi.com/2624-6511/5/3/57>>; Jonna Nyman, 'Towards a Global Security Studies: What Can Looking at China Tell Us about the Concept of Security?' (2023) 29 European Journal of International Relations 673.

showing the evolving nature of data privacy jurisprudence within the country and highlighting that privacy is not uniformly subordinated to collective interests.

Moreover, personal information disputes often involve emerging technologies and cross-sectoral issues, complicating factual determinations. The processes of data collection, storage, transmission, and usage typically involve multiple parties, making it difficult to pinpoint a specific defendant and establish liability. While the trial court dismissed Pang's claim for lack of direct evidence,⁸⁶⁵ the appellate court adopted a more flexible approach, emphasising the concept of 'reasonable probability' in establishing a data breach.⁸⁶⁶

The appeal judgment is significant for several reasons. First, it affirmed that certain categories of information, such as a person's name, phone number, and travel itinerary, are considered private data under Chinese law and protected under the right to privacy. This is an important step forward in clarifying the scope of what qualifies as private information in the digital age, where such data is routinely collected and shared by online platforms and airlines. *Pang*, therefore, has broader implications for the development of tort-based data protection enforcement in China. It illustrates how courts may be moving toward a more substantive understanding of privacy harms, one that goes beyond the mere existence of damage and looks at systemic vulnerabilities in the way personal information is handled. Although the court did not go so far as to issue a final finding of liability against either defendant, its willingness to entertain the probability of misconduct, and its rejection of weak defensive arguments, points to a maturing legal attitude toward digital privacy and consumer protection.

⁸⁶⁵ (2015) Hai Min Chu No. 10634, section of judgment reasons.

⁸⁶⁶ (2017) Jing 01 Min Zhong No. 509, section of judgment reasons.

While the outcome reached by the appellate court may be defensible in substantive justice terms, in that it seeks to enhance the justiciability of personal data protection claims, the court's reasoning process conflates distinct legal concepts. The invocation of a 'complete evidentiary chain' as a basis for decision-making elides the critical distinction between (i) the closure of an evidentiary chain and (ii) the construction of a presumptive inference from a set of high-probability facts. This conflation renders the doctrinal analysis logically tenuous. Therefore, it indicates that greater conceptual clarity is needed in distinguishing between proof of a high probability of a factual link and the identification of a tortfeasor in civil proceedings involving informational privacy. Additionally, it advocates for legislative clarification concerning the use of presumptions and reverse burden mechanisms in data breach cases, so as to avoid reliance on vague or improvised reasoning in judicial practice: a tendency that may, paradoxically, undermine legal certainty and the coherence of evidentiary doctrine.

While judicial efforts to advance personal data protection are evident, as reflected in the court's willingness to adopt progressive evidentiary frameworks, there remains a lack of consistent doctrinal clarity and legislative guidance. This ambiguity mirrors the broader national context, where the prioritisation of societal interests, such as national security and economic development, sometimes complicates the establishment of clear and robust privacy protections. Thus, China's approach to privacy law is marked by a dynamic but uneven development, balancing between emerging privacy concerns and longstanding collective priorities.

In a manner similar to that of *Pang*, the court in *Lin Nianping v Sichuan Airlines Co., Ltd.*⁸⁶⁷ held that the plaintiff had met the standard of a high degree of probability merely by proving the factual link between the act of ticket purchase and the subsequent receipt of fraudulent messages.⁸⁶⁸ The court further acknowledged that the plaintiff was not in a position to provide more specific evidence regarding the point of data leakage, whereas the defendant, Sichuan Airlines, held a superior evidentiary position.⁸⁶⁹ As the airline failed to produce contrary evidence, the burden of further proof did not rest on the plaintiff. In *Lin*, the court's reasoning was instructive. By accepting that the plaintiff's provision of a factual sequence, purchasing a ticket and subsequently receiving fraudulent messages, was sufficient to meet the evidentiary threshold, the judgment recognised the asymmetry of information between data subjects and data controllers. The court emphasised that once a plausible factual link is established, the burden subtly shifts to the defendant to explain why the alleged breach did not occur within their systems.⁸⁷⁰ Again this case shows that there is some determination in the Chinese courts to ensure effective privacy protection, on occasion.

This reasoning, however, is far from uniformly applied in Chinese courts. Some have adhered to a stricter evidentiary stance, especially in similar cases like *Ma Chunyan v China Southern Airlines*⁸⁷¹ and *Zhao Junyan v China Southern Airlines*,⁸⁷² where the absence of definitive causation led to the rejection of plaintiffs' claims. These decisions reflect a more conservative and formalist approach, whereby the inability to conclusively isolate a breach within a single platform or provider, especially in the absence of law enforcement findings, results in judicial

⁸⁶⁷ *Lin Nianping v Sichuan Airlines Co., Ltd.* (2015) 成民终字第 1634 号.

⁸⁶⁸ *Ibid*, section of judgment reasons.

⁸⁶⁹ *Ibid*, section of judgment results.

⁸⁷⁰ *Ibid*, section of judgment reasons.

⁸⁷¹ *Ma Chunyan v China Southern Airlines Co., Ltd.* (2016) Su 01 Min Zhong 3947.

⁸⁷² *Zhao Junyan v China Southern Airlines Co., Ltd.* (2017) Yue 71 Min Zhong 11.

reluctance to assign liability. The divergence in outcomes raises a broader doctrinal tension; how to balance the evolving need for effective remedies in a digital realm with traditional principles of tort law.

Without strong regulatory backing or an empowered data protection authority, courts are often the only available avenue for redress, but they remain fragmented in their approach. In the absence of an equivalent institutional mechanism in China, judicial innovation, such as the ‘high probability’ test, would provide a partial path forward, although obviously it does not affect the remedial situation. However, without consistent jurisprudential application, its utility remains limited. The decisions in *Pang* and *Lin Nianping* reflect a promising shift toward a more victim-sensitive approach to data protection, but as long as other courts continue to demand strict causation, plaintiffs will remain disadvantaged. Thus, the real tension lies not merely in how courts interpret causation, but in the broader architecture of personal data protection. The key question is whether China’s legal system will move toward empowering individuals and holding data controllers/processors to higher accountability standards or will continue to rely on patchwork remedies as discussed in Chapter 6 that offer little certainty or consistency in enforcement.

b) ‘substantial’ breach of privacy

For robust data protection laws to take effect, there must be a comprehensive and balanced conception of privacy, one that recognises personal data as a powerful tool capable of

influencing decisions, behaviours, and potentially causing significant harm if misused.⁸⁷³ However, legal interpretations of privacy and personal data in China remain narrowly defined.⁸⁷⁴ Courts typically extend legal protection only to those cases where the disclosure of personal information causes substantial harm, a high threshold that leaves many forms of abuse unaddressed. For example, actions like forced bundling of software, tracking across applications, or unauthorised sharing and storing of user data are often excluded from legal protection, where they do not result in immediate or quantifiable harm. Even though these actions involve personal information, they are not deemed to constitute a *substantial* breach of privacy.⁸⁷⁵

As technological advancements continue and personal data breaches become more frequent, the need to clearly define the scope of online data protection in Chinese courts has become an urgent issue. In tort cases involving online data violations, the burden of proof remains disproportionately high. Plaintiffs are often required to prove that data leakage not only occurred, but also that it directly caused tangible economic loss or psychological distress.⁸⁷⁶ This is particularly challenging given the informational and technical imbalance between ordinary users and intermediaries. Without access to technical evidence, many victims are unable to meet these evidentiary standards. It undoubtedly increases the difficulty of meeting the burden of proof placed on the plaintiff, making it difficult for them to obtain adequate relief, even if they have suffered in fact. This explains why, in some cases,⁸⁷⁷ the court ultimately did

⁸⁷³ See Daniel J Solove, ‘Why is Privacy Important?’ On Privacy and Technology (2025) online edn, Oxford Academic), p 10, <https://doi.org/10.1093/9780197771716.003.0004>.

⁸⁷⁴ See discussion in Chapter 6, section 6.2.3.

⁸⁷⁵ The recognition of breaches typically involves only “personal information” that has privacy attributes, and legal protection is granted only when the disclosure of information results in a substantial infringement of privacy rights.

⁸⁷⁶ See *Lin Nianping v Sichuan Airlines Co., Ltd.* (2015) 成民终字第 1634 号, for example.

⁸⁷⁷ For example, *Xu Linlin v Bank of China Liaoning Branch* (2023) Liao 03 Min Zhong No.1358.

not support claims for psychological damages. It further gives rise to the limited number of successful lawsuits and the broader phenomenon of ‘widespread breach, low success rates, and weak litigation incentives’ in Chinese Courts.⁸⁷⁸

A case that illustrates the legal boundaries of personal data use is *Xu Linlin v Bank of China, Liaoning Branch*.⁸⁷⁹ In this case, the court determined that the bank had improperly obtained and used the plaintiff Xu Linlin’s phone number without her consent. Specifically, the bank repeatedly contacted Xu in an attempt to collect a credit card debt owed by her mother. This unsolicited and unauthorised use of her contact information constituted a breach of Xu’s privacy rights under Chinese civil law, which safeguards individuals from non-consensual access to and misuse of their personal data.

Despite acknowledging the violation itself, the court ultimately declined to hold the bank liable for any damages or to mandate a public apology. The reasoning was that Xu failed to prove the bank acted with malicious intent or that she suffered substantial harm as a result of the privacy breach. Therefore, while the court affirmed that privacy had been infringed, the absence of demonstrable intent or measurable injury meant that civil liability was not imposed. As a result, courts frequently dismiss these cases as outside the scope of enforceable privacy rights, emphasising a reactive rather than preventative approach to harm. This judicial trend, to some extent, limits the scope of traditional privacy rights disputes, protecting only those actions that

⁸⁷⁸ See Chinese Supreme People’s Procuratorate Report on 佟海晴, ‘准确理解大规模侵害个人信息民事公益诉讼_中华人民共和国最高人民检察院’ (Spp.gov.cn2022)

<https://www.spp.gov.cn/spp/llyj/202206/t20220609_559264.shtml>.

⁸⁷⁹ *Xu Linlin v Bank of China Liaoning Branch* (2023) Liao 03 Min Zhong No.1358.

have already caused actual harm, while leaving other actions that do not constitute substantial harm without intervention.

c) public awareness and legal literacy

Furthermore, public awareness and legal literacy remain low. Many citizens are unaware of their privacy rights or are deterred by the complexity and cost of litigation. Even when legal recourse is pursued, inconsistent judicial interpretations further frustrate attempts to enforce privacy protections. Courts diverge on issues such as the legal meaning of ‘consent.’⁸⁸⁰ Some judges interpret the mere act of publishing personal data online as according implied consent for any subsequent use: regardless of whether users understand the full implications or scope of that use, which serves as an exemption from liability, assuming that when an individual publishes personal information online, that is equivalent to consenting to the collection and use of that information by others.⁸⁸¹ However, the problem arises with whether the individual fully understands or is aware of how their published information will be used. If consent is presumed, is it limited to the purpose of publishing the information? Are there restrictions on the purposes and methods of collection by the collector? These issues have not formed a unified understanding in judicial practice, leading to different standards in different courts when handling similar cases, which in turn results in inconsistency in the protection of personal data.

⁸⁸⁰ See Samm Sacks, ‘China’s Emerging Data Privacy System and GDPR’ (Csis.org2018), section of ‘consent’ <<https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr>>.

⁸⁸¹ See *supra* section 4.4 and 5.2.1 for comparison with the UK position; see Fan Jinghe and Tang Wenhan, ‘China Law Update a Balance Between Social Media Users’ Personal Information Protection and Combating (Mis) And (Dis)Information in China’ (2022) Tsinghua China Law Review, p 347.

In practice, criminal protection is often given precedence in China, while civil remedies are placed lower on the agenda.⁸⁸² This situation arises from both objective reasons, such as the covert nature of personal information incidents in the digital age and the imbalance of information between the defendant and the victim, as well as subjective reasons, such as deficiencies in the legal system that lead to varying interpretations among different judicial personnel and judicial bodies. This variation in understanding, especially regarding whether ‘personal information rights are civil rights,’⁸⁸³ directly affects the strength of judicial protection of personal data. Different courts’ approaches to protection scope, enforcement, and evidentiary requirements have resulted in a significant gap between civil judicial protection of personal information and public expectations.

Civil remedies, when available, are also overshadowed by a judicial system that prioritises criminal enforcement over private rights. Although privacy infringements frequently originate from private-sector behaviour, such as unauthorised data sharing, profiling, or commercial exploitation, the current legal system tends to approach them through the lens of public order and criminal liability, rather than treating them as violations of individual rights. This results in a justice framework that is underdeveloped and difficult to access, especially for ordinary users who often lack legal literacy or the financial resources necessary to pursue claims. Furthermore, the relative weakness of the data protection system contributes to a widespread low expectation among the population that effective data privacy safeguards can be achieved. This diminished public confidence can undermine both the demand for stronger protections

⁸⁸² Yang Feng, ‘The Future of China’s Personal Data Protection Law: Challenges and Prospects’ (2019) 27 Asia Pacific Law Review 62, pp 11-13 in its own page.

⁸⁸³ See Lu Zhang, “‘Personal Information of Privacy Nature’ under Chinese Civil Code’ (2021) 43 Computer Law & Security Review 105637, p 2.

and the accountability of data controllers, perpetuating a cycle where individual privacy rights remain insufficiently protected.

7.3.2 Contrasts between remedial relief and regulatory aspects of the two schemes: influence on design

China's evolution towards formal data protection law reflects an interplay between two hybrid 'schemes' in theory: the regulatory scheme, which imposes obligations on data controllers and processors, and the remedial scheme, which offers individuals paths to enforcing their rights and securing relief when those obligations are breached. A thorough understanding of the contrast between these dimensions, and their influence on the design of China's data protection regime, necessitates an examination of both the legal instruments and their practical impact.⁸⁸⁴

The most prevalent cases on individual rights in China revolve around violations of the right to know and the right to decide.⁸⁸⁵ These violations are often driven by a variety of factors, including economic pressure, geopolitical considerations, and national security concerns.⁸⁸⁶ Violations of these rights, core elements of informational self-determination, expose the tension within China's legal and regulatory framework, which is both expansive and intrinsically conflicted.

⁸⁸⁴ See *supra* section 6.2.2 and 6.3.

⁸⁸⁵ See Guosong Shao and others, 'Assessing the Implementation of China's Personal Information Protection Law: A Two-Year Review' [2025] *International Data Privacy Law*, p 9 <<https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipae022/8100448>>.

⁸⁸⁶ Mark Jia (note 656) p 753.

Despite the existence of some statutory frameworks, such as the PIPL, discussed in Chapter 6, the ability of individuals to seek and obtain effective redress remains significantly constrained.⁸⁸⁷ The legal structure tends to emphasise regulatory compliance over individual remedies, treating personal information or digital privacy largely as the matter of market discipline rather than of civil empowerment. While these laws impose obligations on data controllers/processors to limit, secure, and justify their collection and use of personal information, they do not equally equip individuals with the means to enforce their rights or seek compensation for violations of their data protection rights.⁸⁸⁸ One of the primary challenges for Chinese data protection law is that of balancing the need for personal data to fuel digital innovation with the desire to maintain stringent state control. The key difficulty lies in enabling the free flow of data necessary for technological and economic growth, without undermining the state's overarching authority⁸⁸⁹ and without enabling constant data breaches.

The remedial mechanisms available to individuals in China are conspicuously underdeveloped. Whereas the GDPR grants individuals extensive enforceable rights, including the right to compensation, the right to erasure, and the ability to lodge complaints with independent supervisory authorities,⁸⁹⁰ China's model does not meaningfully empower citizens to assert claims or seek redress when their data rights are violated, which is to be managed by regulators rather than defended by individuals. Legal standing for individuals is weak, the evidentiary

⁸⁸⁷ Ibid.

⁸⁸⁸ See Shao Yi, 'Personal Information Protection: China's Path Choice' (2021) 18 US-China Law Review, pp 241-243.

⁸⁸⁹ Emmanuel Pernot-Leplay (note 650) p 110.

⁸⁹⁰ See *supra* section 4.5.1.

burden is often insurmountable, and courts frequently defer to administrative discretion or public interest exemptions when resolving disputes.⁸⁹¹

The consequences of this divergence are not merely theoretical. Consider the types of harms that dominate Chinese cases: unauthorised profiling, medical records leaks, or large-scale data disclosures in academic settings, as in the case where a graduate student, Ma,⁸⁹² accessed and compiled sensitive personal information from fellow students. The data, including names, student IDs, birthdates, and photographs, was used to create a website that rated students' physical appearances, particularly targeting female students. The website, active since 2020, allowed users to view profiles containing personal information alongside ratings of the students' facial attractiveness.

The handling of this case reveals both progress and limitations in China's approach to privacy protection. Authorities eventually intervened to shut down the website and arrested Ma for violating data privacy norms. There is no further disclosure from official authority regarding this case. The relatively delayed response, limited transparency and scope of sanctions proved that ongoing challenges arise in terms of promptly addressing such infringements and providing effective remedies for victims. Moreover, the incident sparked public debate about the boundaries of personal data use and the protection of individual dignity in digital spaces. It also reflects the broader tension between emerging privacy concerns and the prioritisation of collective or social order interests that characterises much of Chinese data governance.

⁸⁹¹ See Guosong Shao and others, 'Assessing the Implementation of China's Personal Information Protection Law: A Two-Year Review' [2025] *International Data Privacy Law*, <<https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipae022/8100448>>, p 13.

⁸⁹² See police report on official account: <https://weibo.com/1710175603>.

In each instance of such misuse of personal data, individual recourse is either absent or deeply limited. While criminal charges may be pursued against offenders, and administrative penalties may be levied, individuals, even those demonstrably harmed, are rarely made whole. The civil dimension of data protection is not a genuine pillar of the regime, but rather a footnote to its regulatory enforcement and compliance. What emerges from this system is not a genuine ‘data protection law’ in the rights-based sense, as exemplified by the GDPR, but rather a compliance code for managing information flows within an authoritarian governance model. In the case of *Ye v Shi et al.*,⁸⁹³ the plaintiff, Ye, and the defendant, Shi, were involved in a residential lease agreement. A dispute subsequently arose concerning the return of the rental deposit. In response to the disagreement, Shi published a post on the social media platform Douban, in which they described the events surrounding the conflict and disclosed Ye’s phone number, as well as information regarding Ye’s involvement in other rental-related legal disputes.⁸⁹⁴ After reviewing the facts, the court held that the defendant did not act with intent to infringe on the plaintiff’s right to privacy.⁸⁹⁵ The court found that the disclosure did not result in any demonstrable or substantial harm. As a result, the plaintiff’s claim for infringement of privacy rights was dismissed.

Both the *Ye* and *Ma* cases reveal, not only the vulnerabilities in China’s data protection framework, but also the profound consequences of unauthorised access and misuse of personal information. These cases demonstrate how breaches of personal data, whether in healthcare or educational settings, can have severe legal, social, and reputational consequences. They

⁸⁹³ *Ye v Shi et al.* (2014) Chaoyang District People’s Court of Beijing, Chaominchu No. 00008.

⁸⁹⁴ *Ibid*, section of case facts.

⁸⁹⁵ *Ibid*, section of judgment reasons.

illustrate the importance of improving data protection mechanisms, ensuring accountability for violations, and reinforcing privacy rights as part of a broader cultural and regulatory shift toward stronger safeguards for personal information.

The Chinese current model therefore raises a critical question: can data protection be meaningful in the absence of enforceable individual rights? The honest answer, developed throughout the preceding chapters of this thesis and crystallised in the analysis that follows, is that the GDPR is significantly less effective than its formal architecture suggests, and that the gap between its normative ambitions and its practical outcomes is sufficiently large to require serious qualification of any claim that it represents a genuinely successful model of data protection against which other frameworks should be measured. The evidence for this conclusion is substantial and has been developed across multiple dimensions of the preceding analysis. The consent fatigue generated by cookie banner proliferation, the complexity and inaccessibility of privacy notices, the evidential burdens imposed by the *Lloyd* damage threshold, and the transaction costs of individual litigation collectively ensure that the GDPR's promise of individual empowerment remains, for most data subjects in most circumstances, a theoretical entitlement rather than a practically exercisable right. China's answer, for now, seems to be that data protection is valuable only insofar as it aligns with state priorities, and individuals are protected only to the extent they do not challenge the logic of centralised control. This divergence is not just a matter of design, but of ideology. Nevertheless, given the sheer scale of China's large population and the administrative burden associated with comprehensive enforcement, the existing framework for personal data protection appears, at present, to be the most pragmatic approach.

However, the critical question that this thesis must confront directly is whether this ideological divergence is as absolute as the binary framing of GDPR *versus* Chinese model suggests, or whether the tensions identified in China's framework are, in attenuated but analytically significant form, visible within the UK's own post-Brexit data protection regime. The compelling and concrete illustration of this tension in the UK context is the government's persistent deployment and endorsement of facial recognition technology, a processing activity whose compatibility with the UK GDPR's requirements of necessity, proportionality, and lawful basis for the processing of biometric data under Article 9 is deeply contested, and whose continued expansion in the face of clear resistance from EU regulators and civil liberties organisations raises profound questions about the UK government's genuine commitment to the data protection values it formally espouses. Facial recognition technology deployed by police forces and, increasingly, by private actors in public spaces involves the large-scale, indiscriminate processing of biometric data, special category data attracting the highest level of protection under Article 9 of the UK GDPR, of individuals who have neither consented to that processing nor been informed of it, and who have no practical means of objecting to or opting out of it.

The UK government has persisted in its support for facial recognition technology, framing it as an essential tool of public safety and law enforcement whose benefits justify the data protection risks it generates. This framing is itself revealing that it subordinates the individual data subject's right to informational autonomy and freedom from mass biometric surveillance to the state's competing interest in security and crime prevention in a manner that structurally resembles the logic of China's prioritisation of state interests over individual data protection rights.

The deeper issue that facial recognition illustrates, and that connects the UK's experience analytically to the Chinese model examined in this section, is the question of what data protection law is ultimately for. If it exists primarily to empower individuals with enforceable rights over their personal information, then a framework that permits the mass processing of biometric data without individual consent, knowledge, or effective remedy is one that has failed in its most fundamental purpose. If, on the other hand, data protection law is understood primarily as a regulatory instrument for managing the data economy in a manner broadly consistent with public values, but ultimately subordinate to competing state priorities when those priorities are sufficiently weighty, then facial recognition's continued expansion is not a failure of the framework but a feature of a manifestation of the political choices about the relative weight of individual rights and collective security that the framework reflects. This thesis's answer, grounded in the Kantian moral framework developed in the preceding section and in the conception of informational autonomy as a foundational value that the GDPR's architecture embodies, is that the former understanding is the correct one, and that the UK's accommodation of facial recognition technology therefore represents a failure to treat data subjects as ends in themselves whose right to informational autonomy cannot be overridden by the state's interest in the convenience and efficiency of mass biometric surveillance.

This issue was particularly evident during the COVID-19 pandemic, when public health measures often intersected with personal data rights. In *Jiang v Binzhou Magic Pharmacy Co., Ltd.*,⁸⁹⁶ the plaintiff, Jiang, went to the defendant Binzhou Magic Pharmacy to purchase medicine. Jiang was asked by the store clerk to scan a QR code and input personal information

⁸⁹⁶ *Jiang v Binzhou Magic Pharmacy Co., Ltd.*, (2022) Lu 1602 Minchu No. 976.

before being allowed to enter. However, Jiang did not end up purchasing any medication. Since the personal information was considered private and Jiang did not make a purchase, Jiang requested that the defendant delete all personal information stored. The defendant refused to delete the information. Despite multiple attempts by Jiang to resolve the issue and even contacting the police twice, the defendant continued to refuse the deletion. Jiang then filed a lawsuit seeking compensation for economic and reputational damages.

The court held that the personal information stored in the *Binzhou Epidemic Prevention and Control Drug Traceability System*, including Jiang's name, contact number, drug names, quantities, and purchase time, was considered personal information.⁸⁹⁷ The focus of the case was whether the defendant had committed an infringement, whether they should be held liable for damages, and whether the defendant was obligated to delete Jiang's personal information from the system. According to Article 13 of the PIPL, during the COVID-19 pandemic, in response to the public health emergency, the defendant followed government market supervision departments' instructions and activated the *Binzhou Epidemic Prevention and Control Drug Traceability System* for the registration of medicine purchases related to epidemic control. The system required real-name registration for medicine purchases for symptoms like fever, cough, and diarrhoea. The court found that this action was not inappropriate and did not constitute a breach; therefore, the court did not support Jiang's claim for deletion of his personal information.⁸⁹⁸

⁸⁹⁷ Ibid, section of the court held.

⁸⁹⁸ Ibid, section of judgment: reasons.

Based on Article 1035, Paragraph 2 of the Civil Code and Paragraph 2, Article 4 of the PIPL, the court ruled that while the pharmacy was responsible for verifying the registered information in the system, it was not authorised to store, modify, or delete personal information.⁸⁹⁹ Furthermore, once the defendant logged into the system, Jiang's personal information no longer appeared in the sales records. During the epidemic, the defendant's actions were in accordance with the market supervision department's instructions and the emergency notice regarding the activation of the epidemic prevention drug traceability system. The real-name registration requirement for medicine purchases related to epidemic prevention was found to be in compliance with the law and did not constitute an infringement of personal information.

The contrasts between regulatory control and remedial relief in China's personal data protection regime reveal a fundamental design tension. The architecture of these laws is heavily influenced by the state's need to promote economic modernisation and global digital leadership. This has led to a paradoxical model wherein the state enacts laws that mimic global practices in form, but whose function is often to legitimise data centralisation. In other words, in reality, the state and corporations need to deploy personal data in a variety of ways tends to take priority over safeguarding that data from misuse or protecting individual privacy. Consequently, regulatory frameworks serve not only as instruments of data protection, but also as mechanisms to consolidate control over data flows, reflecting broader political and economic objectives rather than purely privacy-driven concerns.

7.3.3 Enforcement in China, comparing it with the GDPR

⁸⁹⁹ Ibid, section of judgment: results.

The limited enforcement power in the PIPL is exacerbated by systemic barriers faced by individuals attempting to exercise their rights under the law. Although the PIPL acknowledges the rights of individuals to access, correct, and delete their data, as does the GDPR,⁹⁰⁰ these rights are difficult to enforce. Victims of data misuse face challenges such as high evidentiary burdens, a lack of transparency, and a judiciary that is often more concerned with state interests and stability than with individual redress. Compared to the GDPR, which provides clear recourse mechanisms,⁹⁰¹ the PIPL's remedial pathways are fragmented and largely ineffective, making it difficult for individuals to seek meaningful compensation or correction for data abuses.

The challenge with the PIPL lies in its relatively mild penalties and limited enforcement mechanisms, which have hindered meaningful progress in safeguarding personal information. While the law aligns in many ways with the GDPR, particularly in its focus on consent, data minimisation, and user rights, it ultimately falls short in crucial areas like enforcement, penalties, and the creation of a data rights culture. This inadequacy in enforcement has allowed companies to largely disregard the regulatory requirements,⁹⁰² contributing to the continued prevalence of personal information violations. As a result, the lack of a robust deterrent effect undermines the law's potential to significantly improve personal information protection in the country. The case involving the unauthorised disclosure of actress Kathy Chow Hoi-mei's⁹⁰³

⁹⁰⁰ See *supra* pp 114-119.

⁹⁰¹ See *supra* section 4.5.1.

⁹⁰² Ibid, Guosong Shao and others, 'Assessing the Implementation of China's Personal Information Protection Law: A Two-Year Review' [2025] International Data Privacy Law, p 9 <<https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipae022/8100448>>.

⁹⁰³ Kathy Chow, a well-known Hong Kong actress, passed away on December 11, 2023, after a prolonged illness. Shortly after her death, a screenshot of her electronic medical record, containing sensitive personal information and details about her treatment, was leaked online.

medical records, after her death, has drawn significant attention and concern over personal data protection in China. The breach originated at a hospital in Beijing, where a hospital employee, Fu, had accessed and photographed Chow's medical records, later sharing them in WeChat groups, claiming to be 'showing off.'⁹⁰⁴

In response, Beijing police placed Fu under administrative detention,⁹⁰⁵ and the Beijing Shunyi District Health Commission launched an investigation into the breach. While Fu faced personal punishment, publicly available information does not clearly indicate whether the hospital itself was fined or if any medical staff members had their licenses revoked. This lack of transparency regarding institutional accountability has sparked debate about the effectiveness of enforcement mechanisms against organisations responsible for safeguarding personal data.

Although Fu's sanction demonstrates that individual violations are recognised and punishable under Chinese law, the apparent absence of significant penalties for the hospital supports the argument that the regulatory focus tends to target individuals rather than systemic issues within institutions. This case thus exemplifies the broader challenge in China's data protection framework, where misuse of personal data is addressed unevenly, and institutional responsibilities for preventing such breaches remain insufficiently enforced.

One of the most critical distinctions between the PIPL and the GDPR lies in their underlying enforcement philosophies. The GDPR is structured around accountability and deterrence. It

⁹⁰⁴ See Yan Maoqiang, 'Beijing Police Detain Man Responsible for Leaking Personal Medical Records' (Chinadaily.com.cn2023) <<https://www.chinadaily.com.cn/a/202312/14/WS657a6e12a31040ac301a7c3f.html>>.

⁹⁰⁵ See police report on official account <https://weibo.com/1710175603>.

empowers independent supervisory authorities to impose substantial fines and mandates transparency from both public and private sector actors.⁹⁰⁶ These elements serve as a deterrent, encouraging companies to comply with the law. In contrast, the PIPL lacks robust enforcement measures and independent bodies to oversee its implementation. Its penalties are often mild, and violations are not publicly scrutinised, which diminishes its deterrent effect. This has resulted in widespread noncompliance, especially among powerful tech companies and state-affiliated platforms that are able to sidestep regulation.⁹⁰⁷

7.3.4 'Personal data' under the GDPR/DPA and the PIPL

While both legal frameworks claim to safeguard personal data, the scope, enforcement, and underlying principles of each reflect markedly different approaches to privacy, shaped by distinct political, legal, and philosophical contexts. The GDPR defines 'personal data' in broad terms, including not only basic identifiers like names and addresses but also digital identifiers, online behaviour, biometric data, and more.⁹⁰⁸ The GDPR treats personal data as a civil right, rooted in European legal traditions that emphasise individual dignity and autonomy.⁹⁰⁹ This framework imposes stringent requirements on the collection, processing, storage, and transfer of personal data, ensuring that individuals have comprehensive rights, including the right to access, correct, erasure, and transfer their data. In contrast, while the PIPL similarly defines personal data in broad terms, its implementation falls short of offering the same level of

⁹⁰⁶ See *supra* section 4.5.1.

⁹⁰⁷ See Fan Jinghe and Tang Wenhan, 'China Law Update a Balance Between Social Media Users' Personal Information Protection and Combating (Mis) And (Dis)Information in China' (2022) *Tsinghua China Law Review*, pp 335-338.

⁹⁰⁸ See *supra* p 27.

⁹⁰⁹ See Raymond Yang Gao, 'A Battle of the Big Three? —Competing Conceptualizations of Personal Data Shaping Transnational Data Flows' (2023) 22 *Chinese journal of international law* 707, pp 718-721.

protection, with a particular focus on personal information of privacy nature, in other words, *private information which is unwilling to be known to others*.⁹¹⁰

There is an argument that the enactment of the PIPL aligns with the broader ‘global trend’⁹¹¹ toward stronger privacy legislation, aiming to foster international trust and therefore aid trading opportunities.⁹¹² However, it is overly simplistic to assert that internal stability in economic terms⁹¹³ while providing protection for personal data, is the sole or even primary motivator behind this legislation. While stability certainly plays an important role in Chinese policymaking, it is not the only factor shaping policy. The political philosophy in China is diverse, and it impacts policy decisions in various ways, reflecting a broader range of considerations beyond merely safeguarding internal stability. Therefore, the driving forces behind the PIPL clearly differ from those driving the GDPR, despite superficial similarities in their legislative frameworks.

The effectiveness of the PIPL in advancing personal information protection in China has not met initial expectations.⁹¹⁴ A key challenge lies in the PIPL’s inability to distinguish itself from other related frameworks, particularly concerning their practical application and the assignment of administrative responsibilities. This lack of clarity has contributed to the absence

⁹¹⁰ See Lu Zhang, “‘Personal Information of Privacy Nature’ under Chinese Civil Code’ (2021) 43 Computer Law & Security Review 105637, introduction.

⁹¹¹ See Graham Greenleaf, “The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108”, *International Data Privacy Law* 2(2012), pp 68-69.

⁹¹² Mark Jia (note 656) p 759; see further in Yu Xiaoyang (于晓洋) & He Bo (何波), Woguo “Geren Xinxi Baohu Fa” Lifa Beijing Yu Zhidu Xiangjie (我国《个人信息保护法》立法背景与制度详解) [A Detailed Explanation of the Legislative Background and Institutions of Our Country’s “Personal Information Protection Law”], 8 DASHUJU (大数据) [BIG DATA RSCH.] 168, 171 (2022) (citing the 128 countries that have enacted such laws).

⁹¹³ See Mark Jia (note 656) p 761.

⁹¹⁴ Ibid, Guosong Shao and others, ‘Assessing the Implementation of China’s Personal Information Protection Law: A Two-Year Review’ [2025] *International Data Privacy Law*, <<https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipae022/8100448>>, p 12.

of a coherent and unified standard for determining the legal basis for penalties, leading to inconsistent and discretionary interpretations of the law.⁹¹⁵ Consequently, the PIPL has evolved into a hybrid framework, merging elements of both public and private law, thereby enabling arbitrary enforcement practices that compromise the law's intended regulatory impact.⁹¹⁶ A central concern in contemporary privacy law is the treatment of personal information, how it is defined, regulated, and protected. At the heart of this issue lies a stark contrast between China's PIPL and the GDPR, which is the conceptualisation and treatment of personal data.

In conclusion, the PIPL's resemblance to the GDPR is more cosmetic than functional. While it adopts similar terminology and structure, such as data subject rights, data minimisation, and consent requirements, it lacks the institutional backing, legal coherence, and rights-based philosophy that underpin the GDPR.⁹¹⁷ Personal information under the GDPR is framed as belonging to the individual; under the PIPL, it is governed, supervised, and conditionally protected. This distinction reveals two fundamentally different views of privacy: one as an intrinsic right, the other as a regulated privilege. As digital technologies continue to reshape societies, the ability to regulate personal information becomes ever more critical. The GDPR offers a rights-based model that recognises personal information as central to identity, autonomy, and democracy. The PIPL, while a step forward in the Chinese context, remains limited by its state-centric approach and uneven enforcement. Until these structural and philosophical gaps are addressed, the protection of personal information in China will remain limited, and privacy will continue to function more as a tool of governance than a shield for the individual.

⁹¹⁵ Ibid, p 12.

⁹¹⁶ Ibid.

⁹¹⁷ See *supra* section 4.2.1.

7.4 The Speech/Privacy Balancing Act: A Comparison Between the GDPR/DPA Framework and the Chinese Model

7.4.1 The protective framework for freedom of expression and information

The intersection of personal information protection with media freedom and freedom of expression further illustrates the differences between the GDPR and the PIPL. The GDPR explicitly acknowledges that data protection must be balanced with freedom of expression and access to information.⁹¹⁸ Article 85 of the GDPR, for instance, requires member states to reconcile the right to data protection with freedom of the press, academic freedom, and artistic expression. This sought-after balance ensures that data protection laws are not misused to stifle investigative journalism or restrict the free flow of public-interest information.⁹¹⁹ While the PIPL contains references to balancing personal information with public interest, these provisions of freedom of journalism are applied inconsistently and often serve as legal justification for controlling narratives and limiting journalistic freedom.⁹²⁰ Instead of fostering an open media environment, as discussed in Chapter 5,⁹²¹ China's legal system potentially

⁹¹⁸ Article 85 of the GDPR; see *supra* section 4.4.

⁹¹⁹ See Melinda Rucz, 'SLAPPED by the GDPR: Protecting Public Interest Journalism in the Face of GDPR-Based Strategic Litigation against Public Participation' (2022) 14 *Journal of Media Law*, pp 379-380.

⁹²⁰ See Harriet Moynihan and Champa Patel, 'Restrictions on Online Freedom of Expression in China the Domestic, Regional and International Implications of China's Policies and Practices International Law Programme Asia-Pacific Programme' (2021) pp 3-4 <<https://www.chathamhouse.org/sites/default/files/2021-03/2021-03-17-restrictions-online-freedom-expression-china-moynihan-patel.pdf>>; Maria Repnikova, 'Restrictions on Critical Journalism' [2017] *Media Politics in China, Improvising Power under Authoritarianism* Cambridge University Press, pp 76-108; see disagreement on Fang Kecheng, 'Quality Journalism in China Is Not Dead; It's Just More Dispersed than Ever' (Made in China Journal 28 January 2025) <<https://madeinchinajournal.com/2025/01/28/quality-journalism-in-china-is-not-dead-its-just-more-dispersed-than-ever/>>.

⁹²¹ *supra* section 5.4.

allows state actors to claim personal data or privacy protection as a pretext for silencing critics or suppressing politically sensitive material.⁹²² The result is a paradox in which privacy, intended to shield individuals from unwarranted intrusion, becomes a tool of censorship. This gap is reflected in China's approach to digital media and information control. The Chinese government has used privacy and data protection regulations to tighten its grip on digital expression, often invoking national security or public order concerns as justification for curbing free speech.⁹²³

The tension between the right to privacy and the freedom of expression exists across all legal systems but is approached very differently across different countries. Under the GDPR/DPA, the right to personal data protection coexists with legally protected freedoms of expression and information.⁹²⁴ European courts and data protection authorities are required to consider the proportionality and necessity of any limitation on these rights. While the GDPR and DPA aim to carefully balance these competing rights within a rule-of-law framework, China's approach is primarily shaped by political ideology and state control, leading to significantly different outcomes for both personal information protection and expressive freedoms.⁹²⁵

The lack of an independent judiciary or data protection authority in China exacerbates the situation. In the EU, the presence of independent data protection authorities, such as the ICO in the UK or the CNIL in France, plays a crucial role in enforcing the GDPR and ensuring that

⁹²² See Maria Repnikova, 'Restrictions on Critical Journalism' [2017] *Media Politics in China, Improvising Power under Authoritarianism* Cambridge University Press, pp 76, 108.

⁹²³ Ibid.

⁹²⁴ See discussion *supra* in Chapter 5, section 5.4.

⁹²⁵ Ibid, Harriet Moynihan and Champa Patel, 'Restrictions on Online Freedom of Expression in China the Domestic, Regional and International Implications of China's Policies and Practices International Law Programme Asia-Pacific Programme' (2021) pp 2-3 <<https://www.chathamhouse.org/sites/default/files/2021-03/2021-03-17-restrictions-online-freedom-expression-china-moynihan-patel.pdf>>.

privacy laws are applied fairly and transparently. These authorities are tasked with ensuring that data protection laws are not misused to infringe other fundamental rights, such as in particular freedom of expression. In China, however, there is no independent body or special authority to supervise the implementation of the PIPL,⁹²⁶ and the state's control over the judicial system further limits any potential challenges to its policies.

In this context, the PIPL is part of a broader effort by the Chinese government to regulate and control the flow of information, particularly in the digital sphere. Rather than enabling individuals to assert their privacy rights against the state or private companies, the law functions more as a tool of governance, helping the state manage and control digital information for political and economic purposes. This leaves individuals with limited avenues for seeking redress or challenging the government's use of their personal data, especially when it is used in ways that restrict free expression.

7.4.2 The legislative approach: the 'Rule by Law' system for data protection in China

In the UK, the GDPR and DPA provide specific protections for journalistic expression, ensuring that the public interest in transparency is upheld even when personal data is involved.⁹²⁷ Courts assess whether reporting on private facts serves a legitimate public interest. In contrast, China's system operates under a rule by law model, whereby the law is wielded primarily as an instrument of governance rather than as a mechanism to limit government

⁹²⁶ See Shao Yi, 'Personal Information Protection: China's Path Choice' (2021) 18 US-China Law Review, p 239.

⁹²⁷ *supra* section 5.4.

power. The Law has broad, often vague, legal provisions, such as ‘public interest’ or ‘national security,’ that can be invoked to limit expression, or justify censorship. The enforcement of data protection laws, such as the PIPL, is significantly influenced by state priorities, and there is little space for independent oversight or transparent decision-making.

The CAC, as well as other government bodies, plays a central role in both the enforcement of privacy laws and the regulation of online speech in China. However, these authorities are closely tied to the state and are often seen as tools to maintain control over digital information, including content that could threaten state power or challenge the government’s narrative. In this environment, judicial review, a core aspect of balancing rights in the GDPR framework, is virtually non-existent. Courts in China rarely challenge the government on privacy or expression issues, especially in cases involving politically sensitive content.⁹²⁸

The law is therefore applied in a way that serves the state’s interests, rather than as a mechanism to check state power or protect individuals from abuses. This leads to a one-sided enforcement pattern. While companies may be fined or disciplined for mishandling personal data (especially if it is foreign or high-profile), there is little protection for individuals who suffer privacy violations from state actors or censorship-related data disclosures. As a result, the balancing act seen in GDPR jurisprudence is effectively absent in China.⁹²⁹ For example, the case of

⁹²⁸ Ibid.

⁹²⁹ See cases, for example, a pertinent illustration of these systemic deficiencies is the case of Ouyang, whose photos and videos were exploited in deepfake pornography without her consent. Despite the initial administrative sanction imposed on Li, the accused, a mere ten-day detention, he resumed disseminating synthetic sexual images upon release, having altered his digital identity to evade detection. To initiate a criminal case, Ouyang relied on assistance from friends to accumulate more evidence and ‘meet the threshold.’ Ironically, her objective, to remove existing images, could only be achieved if Li continued committing offenses. The inadequacy of privacy protections is further illuminated by a separate incident dating back to 2013, in which a private enterprise in Zhejiang Province installed covert surveillance cameras in a female

journalist Zhang Zhan, who was detained for reporting on the COVID-19 outbreak in Wuhan, demonstrates how digital information control intertwines with restrictions on expression and privacy. Despite international outcry, courts upheld state actions, underscoring the lack of judicial independence in cases where state interests are involved.

7.4.3 A closer focus on free speech and information values

Fundamentally, the GDPR/DPA regime is built on the concept of individual autonomy, emphasising that every person should have control over their personal information and the ability to participate in public discourse. The balancing of privacy and freedom of expression is thus a negotiation between individuals and public interests, overseen by impartial institutions.⁹³⁰ In *Yang v Lin*,⁹³¹ the plaintiff objected to the continued online publication of her identifiable information, originally made public during a lawful recruitment process. The court held that although the initial publication was deemed lawful, the refusal of the data subject to permit further dissemination triggered new obligations under the PIPL.⁹³² Specifically, Article 27 of the PIPL prohibits continued processing of publicly disclosed personal information if the individual expressly objects and if such continued use could adversely affect their rights and interests. In this case, the identifiable nature of the data: name, academic qualifications, and educational background, even when partially redacted, allowed re-identification. The court

employees' changing room. The footage was surreptitiously live streamed to monitors accessible from public areas of the facility, leaving the women exposed to an ongoing risk of digital exploitation. No consent was sought; no notice was provided. The operation of this clandestine system, undetected for nearly a decade, was facilitated by high employee turnover and a pervasive atmosphere of fear and intimidation. Many female employees were unaware of the violation during their brief periods of employment; others, apprehensive of retaliation, remained silent even when suspicions arose.

⁹³⁰ See *supra* section 5.4.

⁹³¹ *Yang v Lin* [2024] Beijing Internet Court CLI.C.555521261.

⁹³² *Ibid*, section of judgment results.

found that the defendant's failure to delete the content after notification constituted unlawful processing, and thus granted an injunction by deleting the related information online,⁹³³ affirming the growing importance of data subject autonomy and consent, even when data is initially disclosed under lawful conditions. This case suggests that, while recognition of data subject autonomy in China remains at an early stage, the courts are increasingly willing to acknowledge and enforce these rights, signalling a cautious but significant shift towards greater protection of individual privacy interests.

The principle of accountability in data management also featured prominently in *Qi v Beijing [Unnamed] Network Company and Yao*.⁹³⁴ The plaintiff claimed that her social media account, which had been inactive for years, was accessed by a third party who posted sensitive, private content.⁹³⁵ Although the defendant, Yao, used the mobile phone number purchased in connection with the case and logged into and used the social media account in question via SMS verification, Yao did not thereby obtain the right to use the account. While the plaintiff has rights to the personal information generated during the registration and use of the account, the plaintiff should have properly kept the account and registration information. After clearly deciding not to use the social media account in question, the plaintiff should have promptly deactivated it to prevent the leakage of personal information. The court ruled that defendant Yao should deactivate the social media account in question and dismissed the plaintiff's other claims.⁹³⁶ Meanwhile, the platform's refusal to disclose the infringer's identity was not deemed a violation, as it had requested further verification and was not shown to have acted negligently.⁹³⁷ While courts are beginning to recognise the continuing privacy interests of

⁹³³ Ibid, section of judgment reasons.

⁹³⁴ *Qi v Beijing [Unnamed] Network Company and Yao* [2024] Beijing Internet Court CLI.CR.501993222.

⁹³⁵ Including reposts information such as pregnant.

⁹³⁶ Ibid, section of judgment results.

⁹³⁷ Ibid.

inactive users, they also emphasise shared responsibility between users and platforms in maintaining account security and managing legacy data. Moreover, the outcome reflects the judiciary's hesitance to impose liability in the absence of clear fault, even when power asymmetries make it difficult for individuals to trace or control the misuse of their data.

The limitations of individual redress mechanisms are brought into sharper relief in a landmark public interest litigation initiated by the *Yuhang District People's Procuratorate v R video platform*.⁹³⁸ The case involved systemic privacy violations concerning children which were at issue. The platform had collected, processed, and algorithmically disseminated sensitive personal data of minors, such as facial recognition, voiceprints, location, and contact information, without obtaining meaningful or renewed guardian consent. The court found that the platform failed to implement necessary safeguards, including differentiated user management and opt-out options for profiling.⁹³⁹ This constituted a direct breach of the PIPL and the Law on the Protection of Minors, both of which mandate heightened protections for children due to their limited civil capacity. The significance of this case lies in its procedural posture, unlike in private tort actions, which often flounder due to evidentiary hurdles or limited individual harm. The reliance on public interest litigation allowed the state to intervene against systemic risks, compelling corporate actors to rectify their practices in the interest of collective welfare. The case illustrates how public institutions like Procuratorate can play a vital role in bridging enforcement gaps in China's privacy regime, particularly where vulnerable populations such as minors are concerned.

⁹³⁸ *Yuhang District People's Procuratorate v R video platform* (2020) Civil Mediation Statement of the Hangzhou Internet Court, Zhe 0192 Minchu No. 10993.

⁹³⁹ *Ibid*, section of case facts.

China's approach, however, is collectivist and paternalistic, rooted in the belief that information flows must serve the greater good as defined by the state.⁹⁴⁰ In China, media is considered a function of the state, with journalistic freedom tightly regulated, and content moderation guided by party ideology. While the PIPL regulates tech companies' use of personal data, including provisions on algorithmic recommendation and facial recognition, there are no exceptions for journalistic or artistic expression. On the contrary, personal information can be disclosed or censored by authorities to find dissent or control public narratives. The consequences are particularly stark online. In the UK, a person can request delisting of outdated or irrelevant search results through mechanisms like the right to be forgotten,⁹⁴¹ but such requests are adjudicated with attention to freedom of information. In China, online content is frequently removed or altered with no judicial review, often under the pretext of data protection or cybersecurity.

However, courts have begun to recognise the importance of individual autonomy, consent withdrawal, and data minimisation. Although enforcement remains uneven, hinging on the presence of harm and on the plaintiff's ability to produce conclusive evidence or withstand counterarguments based on platform protocols or lack of intent. While state-initiated litigation appears promising in addressing large-scale, systemic risks, the path for individual recourse remains constrained by high burdens of proof and limited judicial willingness to recognise intangible or moral harms. As China's digital economy continues to evolve, these tensions will be likely to shape the future contours of data protection law, raising fundamental questions about how privacy is conceptualised, who bears responsibility, and what kinds of harms are viewed as worth remedying.

⁹⁴⁰ See Ying Miao, 'Managing Digital Contention in China' [2020] *Journal of Cyber Policy* 1, pp 2-3.

⁹⁴¹ See *supra* in section 5.4.2.

The case of *Lin Shengbin v Liu Xinda*,⁹⁴² involving Lin Shengbin's alleged itinerary from 2017, exemplifies the clash between personal information and public interest, particularly with regard to public figures. The dispute emerged after Liu Xinda, driven by the desire to verify Lin Shengbin's alibi in a high-profile criminal case,⁹⁴³ obtained flight records from various airlines. Liu Xinda, questioning Lin Shengbin's account of his whereabouts, publicly shared the results of his investigation, including recorded calls about the flight records, on social media platforms like Weibo. The key issue in this case was the balance to be struck between public interest and the protection of private information. Liu Xinda argued that his actions fell under the category of social oversight, a legitimate effort to challenge a public figure's statements and ensure accountability. He believed that verifying the alibi fell under the 'public interest'. However, the court disagreed, emphasising that the method of obtaining the information was a critical factor; Liu had obtained the information by pretending to be someone else. It ruled that Liu Xinda's actions violated privacy laws, specifically Article 1032 of China's Civil Code, which protects individuals from unauthorised access and disclosure of private information.⁹⁴⁴

This legal controversy highlights the tension between the protection of personal information and the public's right to scrutinise public figures. While Lin Shengbin is a public figure, the court found that his personal travel records, particularly the flight information, were unrelated to the criminal investigation at hand and were not of legitimate public interest.⁹⁴⁵ Therefore,

⁹⁴² *Lin Shengbin v Liu Xinda* (2024) Beijing No. 4 Intermediate People's Court, Jing 04 Minzhong No. 328.

⁹⁴³ Ibid, section of case facts; see news online, Sixth Tone, 'A Deadly Fire Killed His Family. Now He's Being Scorned Online.' (#SixthToneJuly 2021) <<https://www.sixthtone.com/news/1007948>>.

⁹⁴⁴ Ibid, section of judgment reasons.

⁹⁴⁵ Ibid, in view of the fact that the criminal court and the prosecution authorities have made corresponding determinations on the facts of the criminal offense, and the above opinions are not the statutory exemption grounds for Liu to obtain and disclose Lin's personal information.

even though public figures may have reduced privacy expectations in certain areas, the court made it clear that personal and sensitive information, such as flight details, still falls under legal protection when obtained without consent. Furthermore, Liu Xinda's actions were compounded by the means through which he gathered the information. It was found that he used fraudulent methods to access flight records for a period extending beyond the scope of the event in question, spanning from 2015 to 2021.

This breach of privacy was exacerbated by the public dissemination of the information, which violated Lin Shengbin's right to control his personal data.⁹⁴⁶ The court concluded that even if Liu's motivations were based on public interest, verifying Lin Shengbin's claims about his whereabouts, the extent of the private information obtained and the way it was shared were disproportionate. The fact that the information was shared publicly on a platform like Weibo further violated the principle of data protection, as personal information should not be used for sensationalism or public scrutiny without clear consent. The *Lin* case reflects the importance of defining the limits of public interest and the protection of personal information in China, especially for public figures. It also serves as a reminder that the right to privacy remains a fundamental legal protection, irrespective of an individual's public status. The judgment reinforces the notion that personal information, such as travel history, cannot be disclosed freely, even when it pertains to someone in the public eye, without a legitimate and lawful basis.⁹⁴⁷

⁹⁴⁶ Ibid.

⁹⁴⁷ Ibid.

In *Wang v Zhang*,⁹⁴⁸ the court focused on the severe consequences of an individual's private life being publicly disclosed, specifically in the context of Wang's extramarital affair.⁹⁴⁹ Zhang's disclosure resulted in significant harm, including online harassment, defamation, and targeted abuse. Wang Fei's wife, Jiang Yan had committed suicide after discovering that her husband was having an extra-marital affair. Shortly afterwards, Jiang's university friend Zhang Leyi created a website in remembrance of Jiang and as a place for relatives and friends to post their condolences. The website contained personal information about Wang Fei, including his name, address, employer and some photos of him. Zhang Leyi also posted some articles describing the chronological events that led to her friend's death. Visitors to the website copied the material to other websites and discussion boards, including those hosted by the defendants. Daqi.com and Tianya.cn.

The consequence of this was a lot of bad feeling against Wang Fei, who received on-line and face-to-face death threats and was forced to resign from his advertising job.⁹⁵⁰ The Court found in favour of Wang Fei, although Wang only received RMB 8,000 rather than the RMB 135,000 that he was claiming.⁹⁵¹ The court identified Wang's marital life as part of his personal privacy, and Zhang's wrongful disclosure was seen as the catalyst for a broader violation of Wang's privacy rights. The ruling underlines the importance of protecting individuals from harmful invasions of privacy that can cause widespread harm, particularly when such disclosures lead to public shaming and online attacks. Zhang's actions, in this case, were seen as a breach of Wang's privacy rights because they led to a significant and uncontrollable violation of his personal life, clearly justifying the claim for damages and the finding of an invasion of privacy.

⁹⁴⁸ *Wang Fei v Zhang Leyi, Daqi.com and Tianya.cn* (2009) Beijing Chaoyang District Court, No. 10930.

⁹⁴⁹ *Ibid*, section of case facts.

⁹⁵⁰ *Ibid*.

⁹⁵¹ *Ibid*, section of judgment results.

The case illustrates the movement in China towards greater recognition of serious breaches of privacy.

On the other hand, *Gui & Zhang v Xu*⁹⁵² presents a different scenario. In this case, the defendant, Xu, publicly disclosed on the social media platform Weibo detailed information about the prolonged abuse suffered by a child at the hands of his adoptive parents. The disclosure included graphic images of the child's injuries, which quickly went viral and were widely circulated by the public and media outlets. The plaintiffs, Gui and Zhang, who were the child's biological parents, argued that Xu's publication of the images and related information violated their privacy and damaged their reputations. The court ruled in favour of Xu, recognising his actions as a form of 'online whistleblowing' intended to expose abuse and protect the child.⁹⁵³ The court concluded that the publication of such information was in line with the public interest, emphasising the need to protect vulnerable children and ensure their well-being.⁹⁵⁴ In this instance, the court's recognition of public interest outweighed the family's claim to privacy, finding the legal principle that public disclosures, when aimed at protecting vulnerable individuals or exposing wrongdoing, justify a breach of privacy. The case thus exemplifies how public interest considerations can override privacy protections in China, especially when the information disclosed serves a broader societal purpose, such as protecting the welfare of a child. The same outcome would be likely to have arisen under the GDPR/DPA.

⁹⁵² *Gui & Zhang v Xu* (2015) Jiangning District People's Court of Nanjing, Jiangning Shaominchu No. 7.

⁹⁵³ Ibid.

⁹⁵⁴ Ibid, section of judgment reasons.

The previous case of *Gao v Ju*⁹⁵⁵ introduces another layer of complexity regarding the intersection of personal information online and public interest. The defendant, Ju, disclosed personal information about actress Bai's marriage and relationship issues on Weibo, which the court deemed to be an infringement on Bai's privacy. However, when Bai was later tragically murdered, the court acknowledged the public's right to know about the circumstances surrounding her death.⁹⁵⁶ The disclosure of her private life, in this case, was balanced against the public's interest in understanding the event, with the court determining that the newsworthiness of Bai's death outweighed her privacy rights. The court's decision in this instance indicates that, while personal matters unrelated to public duties should be protected, events of significant public interest, such as the violent death of a celebrity, could justify the disclosure of previously private information.

In situations where the public's right to know or protect vulnerable individuals outweighs privacy, Chinese courts are more likely to permit the disclosure of private information. However, *Gao v Ju* raises concerns about the potential for overreach in the name of public interest in China. The excessive deference to the public's curiosity about the private lives of public figures can lead to unnecessary violations on their privacy. In Bai's case, her personal struggles, including her marriage and relationship issues, were not inherently newsworthy and should have been protected from public exposure. When the public's interest in such disclosures serves little more than voyeuristic curiosity, it clearly risks eroding the protection of individual rights and perpetuating a culture of invasive scrutiny in China.

⁹⁵⁵ *Gao v Ju* (2014) Beijing No. 3 Intermediate People's Court, Sanzhong Minzhong No. 04060.

⁹⁵⁶ *Ibid*, section of judgment reasons.

The broader implications of these cases suggest that, while public interest can justify privacy breaches in certain contexts, courts must proceed with caution when determining the scope of such breaches. The balance between privacy protection and freedom of expression in China remains a delicate and evolving legal challenge. Excessive or unjustified disclosures, particularly of matters unrelated to public interest, can undermine individual rights and open the door for unnecessary intrusion into private lives.

7.5 Conclusion

While both the GDPR/DPA and the PIPL contain language about protecting personal information, their underlying goals, enforcement methods, and conceptual foundations are radically different, as this Chapter has found. The GDPR/DPA seeks a balance between privacy and expression, preserving both individual autonomy and public discourse through principled legal processes. China's data protection laws, by contrast, function within an authoritarian framework, where protections are selectively applied. In this light, the notion of a balancing act becomes less about protecting competing rights and more about maintaining the appearance of legality.

Cases analysed in this Chapter reveal the evolving and often contested boundaries between the right to privacy and the demands of public interest in the digital era in China. Courts have demonstrated a willingness to adapt traditional privacy doctrines to new contexts, acknowledging that certain disclosures, particularly those involving public accountability, child protection, or significant social events, can justifiably override individual privacy rights. However, this flexibility also raises concerns about consistency, legal certainty, and the

potential erosion of data protections, especially when the notion of public interest is applied too broadly or imprecisely. As the tension between personal information of a private nature and expression continues to intensify in an age of instantaneous and far-reaching information dissemination, judicial reasoning in China must be grounded in clearer doctrinal distinctions and guided by principled limits.

The evolution of China's traditional privacy regime demonstrates how data protection can be weaponised to reinforce, rather than restrain, state surveillance. While the formal recognition of privacy rights marks a legal milestone, in practice, enforcement remains limited, selective, and subordinate to state interests. As personal data harms become increasingly sophisticated and pervasive, the legal system must evolve beyond superficial protections toward a more meaningful, rights-based approach, one that empowers individuals, closes evidentiary gaps, and ensures access to civil remedies. Without such reforms, privacy and data protection in China risk remaining principles in name, but fictions in practice.

CHAPTER 8 CONCLUSIONS AND POTENTIAL REFORMS

This chapter serves as a critical point of synthesis in the thesis, drawing together findings from the earlier discussions⁹⁵⁷ on both the UK and China and coming to conclusions as regards the research questions of the thesis. Part I revisits the UK data protection framework, not merely to restate and re-analyse its structure and efficacy, but to provide a deeper understanding of the trajectory of online privacy protection and to assess the effectiveness of the remedies available under the GDPR/DPA and MPI, as provided in Chapters 4 and 5.⁹⁵⁸ This reassessment allows for the further identification of strengths and weaknesses in the UK regime, and it sets the stage for comparative reflections with China.

Building on the previous comparative insights of Chapters 6 and 7,⁹⁵⁹ Part II below turns to the Chinese context and argues for the necessity of systemic reforms of data protection. By engaging with recent cases and incidents, and by referring to the UK framework as a point of contrast, section 8.2 demonstrates that the current Chinese regulatory model remains inadequate for protecting personal data.⁹⁶⁰ At the same time, the chapter directly addresses the research questions by evaluating whether certain elements, e.g. the right to be forgotten, of the GDPR could be adapted for the Chinese context. While Chapter 7 has already discussed the cultural and political challenges that complicate such an enterprise, section 8.3 moves toward a set of conclusions about the current remedies for the protection of the personal information in the UK and the viability of drawing upon the UK and EU experience to explore potential reforms in China. The chapter finally comes to overall conclusions as to the research questions.

⁹⁵⁷ See *supra* pp 94-233.

⁹⁵⁸ See *supra* pp 94-193.

⁹⁵⁹ See *supra* pp 194-288.

⁹⁶⁰ *supra* section 7.4.

8.1 Revisiting the UK Framework: Further Evaluating the Effectiveness of the Tort and GDPR/DPA Remedies

8.1.1 The declining impact of traditional injunctions

As Gemma Horton observes, the conceptual foundation of privacy has undergone a significant transformation: it is no longer confined to the safeguarding of secrets but now encompasses broader protections against unwanted intrusion.⁹⁶¹ This doctrinal shift, from confidentiality to spatial and relational autonomy, has redefined the practical utility and normative justification for injunctions, particularly in cases involving public curiosity, press attention, or online harassment. In *CTB v News Group Newspapers*,⁹⁶² Eady J reiterated that ‘the modern law of privacy is not concerned solely with information or ‘secrets’: it is also concerned importantly with intrusion’.⁹⁶³ As Horton argues, this evolution reflects a shift in the role of injunctions, from shielding secrets to proactively safeguarding individuals against intrusion.⁹⁶⁴ Recognising this shift is essential to understanding the continuing relevance of anonymised injunctions, even as their effectiveness is increasingly undermined by technological and cross-jurisdictional challenges.⁹⁶⁵

This emphasis on protecting individuals from intrusive publicity was central in *PJS*,⁹⁶⁶ discussed earlier in Chapter 4. Although the initial application for an injunction was refused,

⁹⁶¹ See Gemma Horton, ‘Injunctions and Public Figures: The Changing Value in Injunctions for Privacy Protection’ (2021) 13 *Journal of Media Law* 1, pp 85-86.

⁹⁶² *CTB v News Group Newspapers Ltd* [2011] EWHC 1326.

⁹⁶³ *Ibid*, § 23.

⁹⁶⁴ Gemma Horton (note 961) p 84.

⁹⁶⁵ *Ibid*, p 85.

⁹⁶⁶ *PJS v News Group Newspapers Ltd* [2016] UKSC 26.

the Court of Appeal overturned that decision, and the Supreme Court upheld the injunction despite widespread publication of the claimant's identity in jurisdictions⁹⁶⁷ such as the United States, Canada, and Scotland. The Supreme Court distinguished between the effects of online and traditional press dissemination, holding that the disproportionate impact of a 'media storm' generated by the mainstream press was significant, even though the information had been published online.⁹⁶⁸ The Court reasoned that the publication of details regarding the claimant's sexual activities would inevitably lead to further intrusive reporting, thereby justifying continued injunctive relief.⁹⁶⁹ The Supreme Court quoted the Court of Appeal in acknowledging the futility of controlling online content, noting that 'the Internet and social networking have a life of their own,' and that the courts have limited power to regulate foreign press or digital platforms.⁹⁷⁰

A similar concern arose in *Mosley*,⁹⁷¹ where the High Court declined to grant an interim injunction to remove a covertly filmed video from an online platform,⁹⁷² despite recognising the significant privacy violation. Eady J observed that while an injunction might be desirable, it would serve little practical purpose once the material had already been widely disseminated.⁹⁷³ He acknowledged that while an order may be 'desirable ... there may come a point where it would simply serve no useful purpose ...'.⁹⁷⁴ Damages were deemed a more appropriate remedy, as Mosley's reasonable expectation of privacy had been irreversibly compromised.⁹⁷⁵

⁹⁶⁷ Gemma Horton (note 961) p 86.

⁹⁶⁸ [2016] UKSC 26, § 35.

⁹⁶⁹ Gemma Horton (note 961) p 87.

⁹⁷⁰ [2016] UKSC 26, § 17 (iv).

⁹⁷¹ [2008] EWHC 687 (QB).

⁹⁷² *Ibid*, § 1.

⁹⁷³ *Ibid*, § 29.

⁹⁷⁴ *Ibid*, § 34.

⁹⁷⁵ Gemma Horton (note 961) p 88.

With the proliferation of digital journalism, particularly the integration of multimedia formats such as videos and photographs alongside text, privacy intrusions have acquired unprecedented speed and intensity.⁹⁷⁶ Once private information is published online, it can be disseminated and re-circulated across social media with viral momentum, rendering traditional injunctions increasingly ineffective.⁹⁷⁷ This was already acknowledged by Tugendhat J in *CTB*,⁹⁷⁸ where he observed that while an injunction might deter harassment in traditional print outlets, it could not shield the claimant or their family from online abuse. Such observations appear outdated, particularly in light of recent statistics indicating that 71% of UK adults now consume news primarily online.⁹⁷⁹ Internet access is now near universal among the UK adult population, with 95% of those aged 16 and over connected at home. As of May 2025, people were spending an average of four and a half hours per day online for personal use, across smartphones, tablets, and computers, representing a ten-minute increase on the previous year.⁹⁸⁰ Young adults aged 18 to 24 are the heaviest users, spending an average of six hours and twenty minutes online each day. This technological shift, coupled with the global reach of digital platforms, has significantly diluted the territorial efficacy of UK injunctions meaning that identities can easily be revealed as a consequence.⁹⁸¹

The challenge is compounded by the diverse range of actors capable of circumventing injunctions. Foreign media outlets, social platforms, and even Members of Parliament have in practice disclosed identities protected by domestic court orders.⁹⁸² The difficulty of maintaining secrecy in such an environment was illustrated by *Mosley v United Kingdom*

⁹⁷⁶ Ibid.

⁹⁷⁷ Ibid, p 93.

⁹⁷⁸ *CTB* § 3.

⁹⁷⁹ Ofcom, 'News Consumption in the UK: 2024 Research Findings' (Ofcom 2024)

<<https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/tv-radio-and-on-demand-research/tv-research/news/news-consumption-2024/news-consumption-in-the-uk-2024-report.pdf?v=379621>>.

⁹⁸⁰ Ibid.

⁹⁸¹ Gemma Horton (note 961) p 91.

⁹⁸² Ibid, p 93.

before the ECtHR, in which Max Mosley unsuccessfully argued for a legal requirement obliging media organisations to provide advance notification (pre-publication notice) before releasing private information.⁹⁸³ Critics of such a requirement have warned of a *chilling effect* on freedom of expression under Article 10 of the ECHR.⁹⁸⁴ However, Gavin Phillipson contends that the absence of such a duty makes it virtually impossible for individuals to obtain meaningful injunctive relief, thereby undermining Article 8 ECHR's protection of private life.⁹⁸⁵ This reflects the central normative conflict, whether a proportionately designed prior-restraint mechanism can protect privacy without imposing an unacceptable burden on journalistic freedom.

Judicial reasoning in this area has often relied on a categorical distinction between national newspapers and internet-based publications.⁹⁸⁶ In *CTB, PJS v News Group Newspapers Ltd*, and *Goodwin v NGN Ltd*, the courts have tended to regard national newspapers as capable of causing greater harm, given their established authority and concentrated readership. Yet such reasoning risks obsolescence in a digital environment where a viral post by an influential online figure, amplified by platform algorithms, may achieve reach and impact comparable to, if not exceeding, that of traditional media.⁹⁸⁷ A purely medium-based classification may therefore misjudge the potential for serious and immediate harm in the online sphere. A functional approach, assessing the actual scale, audience, and velocity of dissemination, would arguably provide a more accurate basis for determining the necessity and proportionality of injunctive

⁹⁸³ Ibid.

⁹⁸⁴ See Conor Gearty, 'Conor Gearty: Max Mosley in Strasbourg' (UK Constitutional Law Association 16 May 2011) <<https://ukconstitutionallaw.org/2011/05/16/conor-gearty-max-mosley-in-strasbourg/>>; Gemma Horton, 'Injunctions and Public Figures: The Changing Value in Injunctions for Privacy Protection' (2021) 13 *Journal of Media Law* 1, p 93.

⁹⁸⁵ See Gavin Phillipson, 'Max Mosley goes to Strasbourg: Article 8 Notification and Interim Injunctions' (2009) 1(1) *Journal of Media Law* 73, p 31.

⁹⁸⁶ [2011] EWHC 1437 (QB).

⁹⁸⁷ Gemma Horton (note 961) p 97.

relief. In this regard, Peter Coe⁹⁸⁸ argues that it is precisely the pragmatic character of such a framework that renders it a suitable normative foundation for regulating the modern media landscape and for giving effect to the concept of media as a constitutional component. By offering a mechanism for distinguishing media actors from non-media actors, the framework provides a principled basis for identifying those who ought to benefit from media freedom and who, correspondingly, should be subject to the obligations and responsibilities that such freedom entails. This in turn clarifies which actors, whether members of the institutional press, citizen journalists, or those disseminating information anonymously or pseudonymously, should be required to operate in conformity with the underlying values of the paradigm and be subject to appropriate regulatory oversight.

Ricki-Lee Gerbrandt develops this analysis further, acknowledging that while functional, content-based protection may be theoretically preferable, institutional protection for ethical journalistic processes offers a pragmatically defensible means of safeguarding the public's access to high-quality news content. Alternative approaches carry significant risks; they may erode the institutional protection currently afforded to news publishers, reduce press freedom to a case-by-case assessment of whether particular content qualifies as 'journalistic,' or eliminate special legal protections for journalism altogether.⁹⁸⁹ These risks must be evaluated against the broader structural realities of the contemporary media environment, in which platforms and the press continue to compete for advertising revenue and reader engagement, platforms retain substantial control over the dissemination of news content, and algorithmic curation by platforms largely determines what content is surfaced to users.

⁹⁸⁸ See Peter Coe, *Media Freedom in the Age of Citizen Journalism* (Edward Elgar Publishing 2021), pp 170-174.

⁹⁸⁹ See Ricki-Lee Gerbrandt, 'Threatening & Protecting Press Publishers and Journalism in the UK's Regulation of Social Media Platforms' (2025) 17 *Journal of Media Law* 1, pp 71, 101.

A further advantage of the functional institutional approach is its capacity to extend protection beyond the traditional boundaries of the established press, encompassing a wider spectrum of content producers, including citizen journalists, civil society actors, and bloggers, whose contribution to public discourse is increasingly significant in the digital era.⁹⁹⁰ This flexibility is particularly important given the growing diversity of journalistic practice, where the production and dissemination of information of genuine public value is no longer the exclusive province of institutional media organisations. A framework that acknowledges this reality is better equipped to protect the public interest in a media landscape that has been fundamentally transformed by digital technology, without sacrificing the normative standards and accountability mechanisms that distinguish legitimate journalism from unregulated expression.

Pre-publication measures, such as advance notification or interim injunctions, can offer essential protection in certain cases but must be accompanied by rigorous evidentiary thresholds and proportionality assessments to avoid over-restriction of speech. Post-publication remedies, including takedown orders and damages, are valuable but often incapable of reversing the harm once information has been widely replicated. Moreover, purely domestic measures are insufficient when cross-border publication is a defining feature of the harm.

This dynamic was illustrated in the case of former footballer Garry Flitcroft.⁹⁹¹ During the period in which injunction remained in force, and even after it was eventually overturned, the national press persistently sought to expose his identity without explicitly naming him. While it is undeniable that speech circulated on the internet can cause significant damage,⁹⁹²

⁹⁹⁰ Ibid, p 92.

⁹⁹¹ *A v B plc (Flitcroft v MGN Ltd)* [2002] EWCA Civ 337; [2003] QB 195; [2002] EMLR 371; [2002] 3 WLR 542; [2002] 2 All ER 545.

⁹⁹² Online content may be delinked under Article 17 of the GDPR, the symbolic and reputational damage from national press exposure is far more difficult to mitigate.

fundamental differences persist between content disseminated online and that appearing in national press. For instance, public figures could elect to establish social media profiles,⁹⁹³ whereas they cannot prevent themselves from becoming the subject of front-page coverage. Engagement with commentary about their private lives on social platforms is therefore a matter of personal choice. In such contexts, attempts to suppress publication can inadvertently provoke the *Streisand effect*,⁹⁹⁴ a phenomenon whereby efforts to hide information lead to greater public interest and dissemination. This effect could trigger the paradoxical nature of modern injunctions; in seeking to protect privacy, they can sometimes fuel the very publicity they aim to prevent.

As private bodies, newspapers of course are not directly bound by the presumption of innocence generally or by duties to respect the Convention rights under the HRA more specifically.⁹⁹⁵ However, courts, as part of the justice system, should have regard both to the presumption of innocence as a general principle and are specifically bound to act compatibly with the ECHR rights, a duty they have notably sought to discharge through the development of MPI itself.⁹⁹⁶ In some MPI cases concerning revelations about a person's arrest, there may be the possibility of a future guilty verdict, but to argue that an arrested person should be named in a publication before charge, in case the claimants are later found guilty, is to turn the presumption of innocence on its head.⁹⁹⁷

⁹⁹³ Gemma Horton (note 961) p 99.

⁹⁹⁴ The Streisand effect is the phenomenon where an attempt to hide, remove, or censor information online actually results in the information being more widely disseminated and publicised.

⁹⁹⁵ Robert Craig and Gavin Phillipson, 'Privacy, Reputation and Anonymity until Charge: ZXC Goes to the Supreme Court' (2021) 13 *Journal of Media Law* 153, p 180.

⁹⁹⁶ Gavin Phillipson, 'Privacy: The Development of Breach of Confidence – the Clearest Case of Horizontal Effect?' [2011] Cambridge University Press eBooks: The Impact of the UK Human Rights Act on Private Law (pp 136-164).

⁹⁹⁷ See Robert Craig and Gavin Phillipson (note 995) p 180.

Building upon these observations, the Marcel principle,⁹⁹⁸ as articulated by Moreham, offers a foundational legal framework for addressing instances in which state actors, particularly law enforcement authorities, are implicated in the unlawful dissemination of private information, which shows the accountability of public institutions in safeguarding informational privacy and provides a basis for legal redress when those institutions fail in their duties. A practical illustration of the application of relevant factors associated with this principle can be found in the landmark case of *NT1 & NT2 v Google LLC*.⁹⁹⁹ In this case, discussed previously, two anonymised claimants-initiated proceedings against Google after the company declined to remove links to reports concerning their spent convictions from its search engine results. Seven years after the ruling, the decision remains a significant point of reference for individuals seeking delisting of information, whether related to criminal convictions or other sensitive matters, under data protection and privacy principles. As detailed in the judgment summary published contemporaneously with the ruling, the court found that Google's continued indexing of the relevant URLs was proportionate and legally justified in relation to NT1 but not NT2. Consequently, the delisting order was issued solely with respect to the URLs identified by NT2. However, the broader applicability of the Marcel principle and the normative reach of the right to be forgotten are limited when the contested information is disseminated *via* unofficial or indirect routes, particularly through media sources that may claim public interest justifications. The decision in *Sicri*¹⁰⁰⁰ exemplifies these limitations, where indirect media circulation complicated the legal assessment of privacy infringements and public interest.

⁹⁹⁸ Nicole A Moreham, 'Privacy, Reputation and Alleged Wrongdoing: Why Police Investigations Should Not Be Regarded as Private' (2019) 11 Journal of Media Law 142.

⁹⁹⁹ [2018] EWHC 799.

¹⁰⁰⁰ *Sicri v Associated Newspapers Ltd* [2020] EWHC 3541 (QB).

A critical insight emerging from the body of case law concerning MPI is the profound instability and contestability of the concept of ‘public.’¹⁰⁰¹ Across these cases, ‘the public’ does not operate as a neutral or stable category;¹⁰⁰² rather, it emerges as a contingent and rhetorically charged construct, deployed variably by courts, litigants, state actors and press. This tension is particularly evident in the recent Grand Chamber decision of the ECtHR in *Hurbain v Belgium*.¹⁰⁰³ In *Hurbain*, the applicant was ordered by the domestic courts to anonymise the name of an individual mentioned in a decades-old article regarding a fatal traffic accident. Although the article itself was factually accurate and lawfully published, the continued accessibility of the information online, particularly via search engines, was found to violate the individual’s right to privacy under Article 8 of the ECHR. The Grand Chamber upheld the Belgian courts’ decision, which was a significant departure from earlier jurisprudence that had prioritised protecting media freedom under Article 10.¹⁰⁰⁴

What makes *Hurbain* especially salient is the way in which the ‘public’ was reconstituted not as a monolithic audience with an unquestionable right to know, but as a shifting, digitally empowered entity whose informational access can perpetuate harm in perpetuity. The decision illustrates how temporal distance, technological dissemination, and the changing contexts of information reception all contribute to reshaping the legal meaning of what is in the ‘public interest.’¹⁰⁰⁵ While the original publication served a legitimate journalistic function, the

¹⁰⁰¹ Rebecca Moosavian, ‘Deconstructing ‘Public Interest’ in the Article 8 vs Article 10 Balancing Exercise’ (2014) 6 Journal of Media Law 234, p 264.

¹⁰⁰² See Edward S Dove, Jiahong Chen, what does it mean for a data subject to make their personal data ‘manifestly public’? An analysis of GDPR Article 9(2)(e), International Data Privacy Law, Volume 11, Issue 2, April 2021, pp 112–114, <https://doi.org/10.1093/idpl/ipab005>.

¹⁰⁰³ *Hurbain v Belgium* (2023) App. no. 57292/16, 04/07/2023.

¹⁰⁰⁴ See Media Defence, ‘European Court of Human Rights Issues Judgment in *Hurbain v Belgium*, Expanding the Application of the “Right to Be Forgotten” - Media Defence’ (Media Defence 14 July 2023)

<<https://www.mediadefence.org/news/judgment-in-hurbain-v-belgium-right-to-be-forgotten/>>.

¹⁰⁰⁵ *Ibid.*

indefinite digital availability of that same information was no longer seen as justifiable in light of the individual's ongoing right to rehabilitation and dignity.

However, the invocation of 'public interest' is often conflated with what interests the public, obscuring the line between democratic accountability and voyeuristic curiosity. As such, the adjudication of MPI claims often turns not on a clear and consistent doctrine, but on contested interpretations of privacy, publicity, and the social value of self-disclosure. This conceptual ambiguity leaves the legal framework vulnerable to inconsistent application and arguably reduces the predictability and coherence of privacy protection under English law. In this context, the logic of *Hurbain*, which frames the issue not around the lawfulness of publication but around the consequences of its digital persistence,¹⁰⁰⁶ may appear to license an expansive and uncertain right to be 'digitally forgotten,' one that could be leveraged to challenge a wide array of previously settled publications.

Thus, *Hurbain* lays bare the conceptual fault lines that run through privacy jurisprudence: the act of publication and the act of accessibility are no longer legally equivalent. The ruling reframes privacy harms not in terms of disclosure *per se*, but in terms of the algorithmically enabled endurance of that disclosure.¹⁰⁰⁷ Domestically, the ripple effects of *Hurbain* are already visible. While the English courts have yet to adopt its full logic, the decision introduces a persuasive authority that claimants may invoke in cases concerning the long-term/historical accessibility of online materials. The reasoning aligns with the trajectory established in *NTI* &

¹⁰⁰⁶ See Sarah de Heer, 'Hurbain v Belgium: Towards a Fairer Balancing Exercise between the Right to Freedom of Expression and the Right to Privacy?' (Strasbourg Observers 26 November 2021) <<https://strasbourgobservers.com/2021/11/26/hurbain-v-belgium-towards-a-fairer-balancing-exercise-between-the-right-to-freedom-of-expression-and-the-right-to-privacy/>>.

¹⁰⁰⁷ Mikel Anderez Belategi, 'The Right to Be Forgotten Concerning the Criminal Past: Developments in the Case Law of the European Court of Human Rights with Particular Reference to the Anonymisation of Digital Press Archives' [2024] *Oñati Socio-legal Series*, section 3.2.

NT2 but goes further by suggesting that even original publishers, not just search engines, might bear ongoing obligations to mitigate informational harm over time. Should this reasoning gain traction, it could radically alter the legal landscape for legacy media and digital archives alike, requiring them to continually reassess the proportionality of data retention and publication practices.

Rather than conceiving of Article 8 and Article 10 of the ECHR as symmetrical rights to be balanced on a case-by-case basis, recent jurisprudence signals an emergent asymmetry. In particular, where personal data is archived digitally and rendered indefinitely accessible via a search engine, privacy claims are increasingly afforded precedence unless a demonstrable, current, and compelling public interest justifies continued dissemination. This departs from traditional models of press freedom, which presume that the public's right to receive information is presumptively valuable even when that information causes reputational harm.

Christopher Docksey contends that the Grand Chamber's ruling in *Hurbain* institutionalises a form of retrospective editorial control.¹⁰⁰⁸ According to Docksey, the judgment alters the operative equilibrium between Articles 8 and 10 by empowering claimants against intermediaries, such as search engines, and directing their de-referencing requests to the primary publishers themselves.¹⁰⁰⁹ This direct engagement with the source outlet is significant, even though de-indexing by search engines would have been functionally sufficient to reduce discoverability. In Docksey's view, such rulings would exert a chilling effect on journalistic practice, compelling media to retrospectively edit, obscure, or even remove content that was

¹⁰⁰⁸ See Christopher Docksey, 'Journalism on Trial and the Right to Be Forgotten' [2022] Verfassungsblog <<https://verfassungsblog.de/journalism-rtbf/>>.

¹⁰⁰⁹ *Ibid.*

lawful, accurate, and publicly significant at the time of publication.¹⁰¹⁰ From this perspective, the judgment risks setting a precedent in which the enduring accessibility of truthful public interest reporting could be subordinated to the evolving reputational claims of individuals, thereby undermining the archival and accountability functions of the press.

From this critical standpoint, *Hurbain* marks a pivotal moment in which the enduring accessibility of historically accurate reporting, especially when archived online, may be subordinated to evolving reputational interests of individuals. This reordering of priorities has the potential to undermine both the archival function and the watchdog role of the press. Notably, in affirming the findings of the Belgian domestic courts, the Grand Chamber held that there had been no violation of the applicant's freedom of expression. In doing so, it relied upon a familiar set of criteria previously articulated in *Axel Springer AG v Germany*,¹⁰¹¹ including: the contribution to a debate of public interest; the public profile of the individual concerned; the subject matter of the report; the prior conduct of the person; the means by which the information was obtained and its accuracy; the form and consequences of the publication; and the severity of any sanctions imposed on the journalist or media entity. These same criteria were applied in earlier cases concerning digital press archives, such as *Fuchsmann v Germany*¹⁰¹² and *M.L. and W.W. v Germany*.¹⁰¹³

However, the Court's approach in *Biancardi v Italy*¹⁰¹⁴ provides an additional recalibration. In that case, which concerned a request for the de-indexing of an article by the owner of an online

¹⁰¹⁰ See Hugh Tomlinson KC, 'Case Law, Strasbourg: *Hurbain v Belgium*, Grand Chamber Upholds Decision That Order Anonymising Newspaper Archive Did Not Violate Article 10 – Hugh Tomlinson KC' (Inform's Blog 26 July 2023) <<https://inform.org/2023/07/26/case-law-strasbourg-hurbain-v-belgium-grand-chamber-upholds-decision-that-order-anonymising-newspaper-archive-did-not-violate-article-10-hugh-tomlinson-kc/>>.

¹⁰¹¹ App. No. 39954/08, §§ 89-95.

¹⁰¹² *Fuchsmann v Germany* App. 71233/13, § 34.

¹⁰¹³ App. Nos. 60798/10 and 65599/10, § 96.

¹⁰¹⁴ *Biancardi v Italy* App. 77419/16, §§ 57-71.

newspaper, the Court supplemented the *Axel Springer* criteria with a new evaluative framework.¹⁰¹⁵ Specifically, it required consideration of (i) the duration of online accessibility, (ii) the sensitivity of the data disclosed, and (iii) the gravity of the legal or reputational sanction resulting from the article's continued availability. This development reveals a more temporally nuanced understanding of informational harm and suggests that the passage of time, in itself, may transform the legal status of past disclosures.

The Grand Chamber's emphasis in *Hurbain* on the 'serious harm'¹⁰¹⁶ enabled by search engine discoverability introduces a more radical conceptual innovation, which reframes the temporal dimension of privacy law. Under this model, the law must continually reassess not only what information is disclosed, but also when its disclosure occurs and how long it persists. Such temporal relativism destabilises conventional assumptions about the finality of lawful speech and presents challenges to legal certainty.¹⁰¹⁷ If truthful content can become disproportionately harmful merely through continued visibility, then the equilibrium between memory and forgetting becomes legally and morally contested terrain.¹⁰¹⁸ Moreover, it remains unclear what mechanisms are available to ensure that such retrospective editorial decisions do not become tools of selective erasure or reputation management by powerful actors. This issue will be explored further in section 8.1.4, with particular reference to the implications for the legal finality of speech-based disputes and the normative legitimacy of post-publication content suppression.

¹⁰¹⁵ App. 57292/16, 04/07/2023, § 204.

¹⁰¹⁶ App. No. 57292/16, 04/07/2023, § 197(c), 231, 236.

¹⁰¹⁷ See Mikel Anderez Belategi, 'The Right to Be Forgotten Concerning the Criminal Past: Developments in the Case Law of the European Court of Human Rights with Particular Reference to the Anonymisation of Digital Press Archives' [2024] *Oñati Socio-legal Series*, pp 1652-1660.

¹⁰¹⁸ *Ibid.*

In sum, injunctions remain an important judicial tool for safeguarding privacy, but their utility in the digital era depends on a shift from a territorially bound, medium-based framework to one grounded in empirical assessments of dissemination risk. Achieving a workable balance between Articles 8 and 10 ECHR will require an integrated approach, combining legal, technological, and transnational mechanisms, that acknowledges both the speed and the persistence of online privacy violations.

8.1.2 Comparative analysis: injunctions and the right to be forgotten

The increasing inefficacy of traditional injunctions in the digital age has prompted comparative reflection on the right to be forgotten, particularly under Article 17 of the GDPR. Both mechanisms, injunctions and the RTBF, seek to limit the dissemination of personal information. However, while injunctions aim to pre-empt publication, the right to be forgotten functions retrospectively, allowing individuals to request the removal of data already made public. The emergence of a more granular, principled, and context-aware model of privacy adjudication suggests that the law is still grappling with the conceptual tensions between data protection and misuse of private information, addressing the harms posed by contemporary information flows. Despite their shared objective of protecting individual privacy, the scope, enforceability, and practical effectiveness of each mechanism diverge considerably, as discussed in Chapter 3.

The judgment in *Driver v CPS*¹⁰¹⁹ holds considerable relevance for the evolving discourse on compensatory thresholds in recent data breach claims. The claimant, Mr. Driver, a locally prominent political figure, was initially treated as a suspect in a police investigation into alleged governmental corruption. In 2016, the police formally notified Mr. Driver that he was no longer

¹⁰¹⁹ *Driver v Crown Prosecution Service* [2022] EWHC 2500 (KB).

a suspect, prompting him to issue a public statement affirming this development. Despite this notification, the criminal investigation persisted, culminating in Mr. Driver's arrest in 2017 on suspicion of conspiring to pervert the course of justice.

The core legal issue arose in 2019, when the Crown Prosecution Service (CPS) responded to a public inquiry with an email indicating, *inter alia*, that a charging file had been submitted for prosecutorial consideration. The recipient of this communication subsequently disseminated the information to multiple journalists and political adversaries of Mr. Driver. Mr. Driver contended that this email rendered him identifiable as a suspect facing potential prosecution and, consequently, constituted (i) unlawful processing of personal data under the UK GDPR and/or the DPA 2018; (ii) an action under MPI; and (iii) a cause of significant emotional distress.

The court, however, rejected the claim based on the GDPR on jurisdictional grounds, holding that the matter fell under the law enforcement provisions of the DPA 2018. Mr. Driver's MPI claim similarly failed. The judgment contains a useful summary of the relevant authorities¹⁰²⁰ and holds that the claimant had no reasonable expectation of privacy over the disclosure that a charging file had been submitted to the CPS. That was because the dissemination was limited and directed towards individuals who were already likely to have known the facts due to prior media coverage.¹⁰²¹ The court concluded that the CPS email did not materially augment the claimant's existing public profile or exposure.

¹⁰²⁰ [2022] EWHC 2500 (KB), §§ 126-147.

¹⁰²¹ *Ibid*, § 156.

The modest award of £250 to the claimant contributed, albeit in a limited way, to the developing body of case law in this area, especially at the lower end of the compensation spectrum.¹⁰²² Importantly, the judgment illustrates the judiciary's increasingly stringent approach to claims of non-material harm in the area of privacy or data protection, particularly where the data in question is not highly sensitive. *Driver* reveals two critical judicial tendencies: first, that the mere occurrence of a data breach does not establish an automatic entitlement to substantial damages; and second, that both the qualitative nature of the disclosed data and the credibility of the alleged harm are subject to robust scrutiny. Mr. Driver's failure to substantiate emotional harm with compelling evidence significantly undermined his claim. Justice Knowles explicitly indicated that the limited nature of the breach, both in scope and consequence, could not reasonably justify the level of distress alleged. His comments suggest that judicial assessment of causation and proportionality will remain central in determining quantum in these cases.

This approach also aligns with broader trends in privacy and data protection jurisprudence, which increasingly emphasise proportionality, evidence-based reasoning, and the avoidance of trivialisation of claims. In *Pacini & Anor v Dow Jones & Company Inc.*,¹⁰²³ a data protection claim was brought by two former investment bankers against Dow Jones, the publisher of the Wall Street Journal. The claimants alleged that two articles published in 2017 and 2018 contained inaccurate and misleading information about their involvement in a conspiracy to defraud a Chinese billionaire and caused damage to their reputations. In July, the defendants unsuccessfully applied for the claim to be struck out as an abuse of process, with the court dismissing its argument that the claim was merely a defamation action disguised as a data protection claim to circumvent the shorter limitation period for defamation. Following the

¹⁰²² See Jade Rawlinson, '*Driver v CPS* – Damages in Data Breach Claims – an Imprecise Science? - 4 Pump Court - Barristers' Chambers' (4 Pump Court 19 October 2022) <<https://www.4pumpcourt.com/driver-v-cps-damages-in-data-breach-claims-an-imprecise-science/>> accessed 29 July 2025.

¹⁰²³ *Pacini & Anor v Dow Jones & Company Inc.* [2024] EWHC 2714 (KB).

dismissal of the strike-out application, the court was asked to determine the preliminary issues: first, the meaning of personal data in the two articles in question; and second, whether any such data was ‘criminal offence data’ within the meaning of Article 10 of the UK GDPR.

This issue was further examined in *ZXC v Bloomberg LP*,¹⁰²⁴ where the Supreme Court held that individuals under investigation but not charged enjoy a reasonable expectation of privacy, affirming that public interest in criminal investigation does not automatically negate Article 8 rights. Similarly, in *MLA v OPO & Anor*,¹⁰²⁵ the Court of Appeal refused to block a memoir’s publication, despite arguments that it would psychologically harm a child indirectly referenced. The Court acknowledged the child’s vulnerability but ultimately gave greater weight to the author’s Article 10 rights, which reveals the judiciary’s reluctance to impose prior restraints, even in emotionally charged, familial contexts, unless exceptional harm is demonstrably proven.

The discussion of a heightened sensitivity to institutional failures relating to a whistleblower’s identity, in *Ali v Chief Constable of Bedfordshire*, is significant.¹⁰²⁶ The High Court recognised multiple privacy breaches, including under the GDPR, MPI, and Article 8 of the ECHR, after the police failed to protect a whistleblower’s identity. Ms. Ali had disclosed her husband’s criminal activity to the police on the condition of anonymity. Her identity was later unlawfully revealed by a council employee. Despite the third-party nature of the breach, the police were held liable for failing to implement adequate protective safeguards. The court awarded £3,000 in damages under the GDPR, MPI, and Article 8 ECHR, thereby reinforcing the heightened duty of care owed by public authorities in handling sensitive personal data. Significantly, the

¹⁰²⁴ [2022] UKSC 5.

¹⁰²⁵ *MLA v OPO & Anor* [2014] EWCA Civ 1277.

¹⁰²⁶ *Ali v Chief Constable of Bedfordshire* [2023] EWHC 938 (KB).

court refused to absolve the police merely because the proximate cause of harm was a third-party criminal act. The Police would have been responsible for that distress: Chamberlain J could ‘see no reason why the Police should be better off than they would have been [...] merely because of [the] subsequent criminal disclosure’.¹⁰²⁷ This affirms that data controllers bear residual responsibility when inadequate institutional controls contribute to foreseeable breaches. *Ali* illustrates a widening duty of care owed by public authorities that handle sensitive personal data, particularly where disclosure could endanger the individual’s safety or violate their expectations of confidentiality.

In *FGX v Gaunt*,¹⁰²⁸ the covert recording of naked images of the claimant and their publication on a pornographic website gave rise to this claim for (i) intentionally exposing the claimant to a foreseeable risk of injury or severe distress which resulted in injury; (ii) infringement of the claimant’s privacy; and (iii) breach of the claimant’s confidence. It recognised multiple overlapping causes of action arising from the same egregious facts. An especially egregious invasion of privacy occurred in *FGX v Gaunt*, where the unauthorised recording and online publication of intimate images led to an award of £97,041.61 in damages. The judgment is notable for its recognition of multiple causes of action, intentional infliction of emotional distress, breach of privacy, and breach of confidence, a holistic judicial approach to remedying modern privacy violations to deal with the intersection of voyeurism, online exploitation, and psychological harm.

A similar trend is observable in *WFZ v BBC*,¹⁰²⁹ where the court granted an interim injunction to restrain publication of a high-profile individual’s identity in connection with uncharged

¹⁰²⁷ *Ibid*, § 51.

¹⁰²⁸ *FGX v Gaunt* [2023] EWHC 419 (KB).

¹⁰²⁹ *WFZ v BBC* [2023] EWHC 1618 (KB).

allegations of sexual misconduct, to prevent the BBC from publishing his name as part of a broader story concerning the failings in the industry concerned properly to deal with such allegations. Relying on the reasoning in *ZXC v Bloomberg*,¹⁰³⁰ the court reaffirmed that individuals under criminal investigation but not charged retain a legitimate expectation of privacy. The court controversially invoked the law of contempt to buttress its order, an innovative legal manoeuvre that illustrates the expanding jurisprudential toolkit available to courts; it was found that having been arrested, publication of the man's name would likely give rise to a contempt of court such as to justify restraint. The novel invocation of contempt of court principles to support the grant of an interim injunction provides a willingness to explore unconventional legal grounds to prevent premature reputational damage.

In the latest attempt to open the floodgates for group data privacy claims, a representative claimant brought a misuse of private information claim against DeepMind and Google on behalf of 1.6 million people arising from the transfer of their NHS medical records. *Prismall v Google*¹⁰³¹ represents a judicial caution against the expansive use of collective action mechanisms in privacy litigation. The court dismissed the representative claim for failing to establish that, on the lowest common denominator basis, all claimants would be able to establish a reasonable expectation of privacy in the data shared and were entitled to more than nominal damages. *Prismall* thus reaffirms the precedent in *Lloyd v Google*, which rejected 'loss of control' as a free-standing head of damage in data protection claims.¹⁰³² The decision indicates that aggregate claims for privacy violations will be likely to remain limited unless the law evolves to accommodate alternative models of harm.

¹⁰³⁰ The Supreme Court affirmed that individuals under criminal investigation, but not charged, generally enjoy a protected status and suggests that the courts are willing to extend privacy protection even further, particularly in cases involving uncharged individuals and sexual misconduct allegations.

¹⁰³¹ *Prismall v Google UK Ltd and DeepMind Technologies Ltd* [2024] EWCA Civ 15.

¹⁰³² [2021] UKSC 50, §§ 109, 110.

The dynamic interplay between injunctions, data protection rights, and evolving technological threats shows that as online platforms become more pervasive and data sharing more fluid, the effectiveness of traditional legal tools is increasingly called into question. The trajectory of case law from *Driver* through *FGX*, *WFZ*, and *Ali* points towards a common judicial ethos: that privacy law must respond meaningfully to the realities of reputational risk, digital permanence, and institutional accountability, without opening the floodgates to speculative or unmeritorious litigation.

Courts are therefore tasked with reconciling long-standing legal principles, such as the presumption of innocence and the right to a fair trial, with emerging doctrines around data control, digital erasure, and reputational rehabilitation. The comparative landscape also points out that while injunctive relief and the RTBF share overlapping aims, their success often depends on contextual factors such as the timing of the disclosure, the sensitivity of the data, and the claimant's ability to demonstrate concrete harm. In this regard, the development of jurisprudence in both areas will be likely to be shaped by normative considerations of dignity, autonomy, and informational self-determination, values increasingly recognised as foundational to contemporary data protection law.

8.1.3 Dealing with anonymous or hard-to-locate publishers

As Eady J remarked in *Mosley*,¹⁰³³ 'Once the cat is out of the bag, and the intrusive publication has occurred, most people would think there was little to gain [by litigation].'¹⁰³⁴ This

¹⁰³³ [2008] EWHC 1777 (QB).

¹⁰³⁴ *Ibid*, § 209.

observation encapsulates a fundamental tension in privacy law; its remedial architecture is often reactive, struggling to offer meaningful redress after the harm has crystallised. The issue becomes significantly more pronounced in the digital sphere, where privacy-invasive content can be disseminated rapidly, widely, and crucially, by anonymous or untraceable actors. In such contexts, traditional legal tools premised on identifiability, jurisdiction, and enforceability begin to unravel.

This challenge is partially mitigated by the courts' willingness to engage with the legal fiction of Persons Unknown. In *AMP v Persons Unknown*,¹⁰³⁵ the court granted an injunction against an anonymous group responsible for the publication of stolen, explicit images of the claimant on a Swedish torrent-hosting website.¹⁰³⁶ While this demonstrates commendable flexibility, the enforcement power of injunctions against unidentified or foreign-based defendants is often symbolic rather than effective, potentially creating a false sense of remedy.

The trend continues in *LJY v Persons Unknown*,¹⁰³⁷ Mr Justice Warby granted an interim injunction to prevent unidentified individuals from disseminating serious criminal allegations targeting a public figure, anonymised as 'LJY'. The case centred on restraining online harassment by anonymous users and the safeguarding of LJY's right to privacy. Warby J determined that the information at issue fell unequivocally within the scope of the claimant's private life and emphasised that attempts at blackmail constitute a fundamental abuse of free expression. In his reasoning, the judge noted that the misuse of free speech in the form of coercive or defamatory threats significantly undermines any legitimate weight such speech might otherwise carry under Article 10 of the ECHR. The court further held that the widespread

¹⁰³⁵ *AMP v Persons Unknown* [2011] EWHC 3454 (TCC).

¹⁰³⁶ See Fiona Brimblecombe and Helen Fenwick (note 320) p 478.

¹⁰³⁷ *LJY v Persons Unknown* [2017] EWHC 3230 (QB).

publication of demonstrably false allegations would almost certainly amount to a misuse of private information. While the publication of true allegations may, under certain circumstances, be defensible, Warby J made clear that in *LJY*, the likelihood of successfully contesting the veracity of such claims was high. Crucially, in the context of blackmail, even truthful information may be subject to legal restraint,¹⁰³⁸ reflecting the courts' increasing willingness to distinguish between the formal legality of speech and its underlying motives and consequences. However, the readiness of the courts to grant such injunctions, often in urgent, *ex parte* proceedings, risks privileging privacy over transparency, particularly where the public interest in the underlying allegations remains contestable.

The case of *GYH v Persons Unknown*¹⁰³⁹ further complicates this picture. The court granted an interim non-disclosure order in favour of the claimant, a sex worker, aimed at restraining a sustained campaign of harassment involving the dissemination of both actual and alleged private information. The judgment, delivered by Warby J, engages with a complex intersection of legal issues, including jurisdictional considerations, the permissibility of claims against unidentified defendants, the boundaries of privacy rights in the context of prior disclosures, and the interplay between claims in harassment and defamation. Warby J invoked section 41(1) of the County Courts Act 1984 and Civil Procedure Rules 30.3(2)(b) and (c) to justify retaining the case at the High Court level, reasoning that the claimant bore no procedural fault and that centralised judicial management would serve both fairness and the efficient allocation of court resources.

¹⁰³⁸ See Brett Wilson, 'Celebrity Blackmail Victim Obtains Injunction Restraining Publication of Allegation of Serious Criminality - Brett Wilson' (Brett Wilson 13 December 2017) <<https://www.brettwilson.co.uk/celebrity-blackmail-victim-obtains-injunction-restraining-publication-allegation-serious-criminality/>> accessed 14 August 2025.

¹⁰³⁹ *GYH v Persons Unknown* [2017] EWHC 3360 (QB).

Warby J considered the procedural challenge posed by the defendant's anonymity, emphasising the judiciary's responsibility to uphold fairness even in the absence of an identifiable respondent. This concern appeared to rely on established precedent, particularly *Bloomsbury Publishing Group plc v News Group Newspapers Ltd*,¹⁰⁴⁰ which affirmed the principle that justice must remain equitable and balanced, irrespective of whether the defendant is known. This issue was directly connected to the interpretation of section 12(2)(a) of the HRA 1998, which requires claimants seeking pre-publication relief to demonstrate that all practicable steps have been taken to identify the alleged wrongdoer.

Equally contentious is the use of Spycatcher-style relief,¹⁰⁴¹ whereby injunctions are extended to third-party intermediaries, such as internet service providers or hosting platforms. In *GYH*, this was justified on the basis that notifying these intermediaries in advance might escalate the harmful conduct. While the *Practice Guidance on Interim Non-Disclosure Orders*¹⁰⁴² permits such steps, it nevertheless raises critical concerns about proportionality, freedom of expression, and the chilling effects on platforms that would feel compelled to over-comply to avoid liability.¹⁰⁴³ This is especially problematic where the allegations involve contested facts or intersect with matters of public concern.

More fundamentally, these scenarios promote the increasing overlap, (this engaged a raft of caselaw, including Warby J's recent decision in *LJY*) and at times, confusion, between defamation, MPI, and online harassment. As observed in *Terry (previously 'LNS') v Persons*

¹⁰⁴⁰ *Bloomsbury Publishing Group plc v News Group Newspapers Ltd* [2003] EWHC 1205 (Ch).

¹⁰⁴¹ The term 'Spycatcher relief' refers to an injunction granted in the 'Spycatcher' case, where the UK government sought to prevent the publication of confidential information about the British Security Service. In that case, the government sought to extend the injunction to various publications, including newspapers and individuals involved in the publication process.

¹⁰⁴² See Practice Guidance: Interim Non-Disclosure Orders [2012] 1 WLR 1003, pp 9-15.

¹⁰⁴³ *JIH v News Group Newspapers Ltd* [2011] 1 WLR 1645, § 21.

Unknown,¹⁰⁴⁴ courts are required to scrutinise the ‘nub’ of the claim,¹⁰⁴⁵ resisting claimants’ attempts to repackage one cause of action as another for strategic advantage (e.g., sidestepping the Defamation Act 2013’s serious harm threshold). While this approach is doctrinally sound, it does little to address the substantive challenge posed by online smear campaigns.

The arguments supporting each cause of action may be meritorious however, the Court will take an objective approach to assessing what the ‘nub’ of the Claimant’s claim is. Such an approach is highly fact sensitive, discouraging Claimants from ‘shopping’ for a cause of action.¹⁰⁴⁶ As in the instant case, smear campaigns involving the dissemination of private, typically false, information are usually most suitably addressed by a complaint of harassment. This action provides the most adequate remedy, an injunction to prevent the conduct at issue and an award of damages.¹⁰⁴⁷

The challenge posed by anonymous or difficult-to-locate publishers is not merely legal but fundamentally structural. It intersects with global questions of technological governance, extraterritorial jurisdiction, and digital accountability. More significantly, an injunction can provide a degree of protection in instances of online misuse of private information where the privacy invader is not identifiable; an injunction could be sought against the intermediary that has enabled access to information posted anonymously, requiring that the offending pages should be removed. Or an erasure request to the effect that the links to the information should be expunged could be sent to the intermediary in question.¹⁰⁴⁸

¹⁰⁴⁴ *Terry (previously ‘LNS’) v Persons Unknown* [2010] EWHC 119 (QB); See also chapters 2 and 5.

¹⁰⁴⁵ [2010] EWHC 119 (QB), § 95.

¹⁰⁴⁶ See Suneet Sharma, ‘Case Law: *GYH v Persons Unknown*, Interim Injunction to Restrain Campaign of Vilification – Suneet Sharma’ (Inform’s Blog 17 January 2018) <<https://inform.org/2018/01/17/case-law-gyh-v-persons-unknown-interim-injunction-to-restrain-campaign-of-vilification-suneet-sharma/>> accessed 5 August 2025.

¹⁰⁴⁷ See Godwin Busuttil and Patrick McCafferty, ‘Interim Injunctions and the Overlap between Privacy and Libel’ (2010) 2 *Journal of Media Law* 1, pp 7, 11.

¹⁰⁴⁸ Fiona Brimblecombe and Helen Fenwick (note 320) p 478.

8.1.4 Are injunctions and erasure rights constrained by speech-friendly standards in courts?

A growing body of academic commentary has critiqued the structural bias embedded within this legal framework, particularly the observation that it was developed in the context of legacy media institutions.¹⁰⁴⁹ As in the 2022 special case law report on the RTBF by Columbia University's Global Freedom of Expression project,¹⁰⁵⁰ regional human rights courts and domestic judiciaries have frequently engaged with the RTBF,¹⁰⁵¹ seeking to develop the doctrinal elements absent in *Google Spain*, particularly regarding the tension between data protection and freedom of expression. Importantly, this line of jurisprudence in Europe reflects a shift away from the conventional pre-internet equilibrium between privacy and speech. The ECtHR is currently deliberating how the RTBF interacts with digitised press archives, weighing the public's right to access historic material against an individual's right to privacy.¹⁰⁵² Critically, as Gavin Phillipson cautions, extending horizontal application of privacy norms, such as through private causes of action derived from Convention rights, could fundamentally unsettle common law doctrine. He argues that direct horizontality would 'threaten whole swathes of the common law with replacement by private HRA actions'.¹⁰⁵³ While some may view this prospect as a welcome shift toward individual empowerment,

¹⁰⁴⁹ See Richard Fletcher and others, 'The Link between Changing News Use and Trust: Longitudinal Analysis of 46 Countries' (2024) 75 *Journal of Communication* <<https://doi.org/10.1093/joc/jqae044>>, pp 1, 2, 4, 12.

¹⁰⁵⁰ See online website on 'Special Collection of the Case Law on Freedom of Expression - Global Freedom of Expression' (Global Freedom of Expression 10 June 2024) <<https://globalfreedomofexpression.columbia.edu/a-special-collection-of-the-case-law-of-freedom-of-expression/>>.

¹⁰⁵¹ See Does Our Past Have a Right to Be Forgotten by the Internet, in Special Collection of the Case Law on Freedom of Expression 1, 28 (Ramiro Álvarez Ugarte ed., 2022), pp 4-5, <https://perma.cc/S7Z9-D3W5>.

¹⁰⁵² See Harriet Ni Chinneide, 'Hurbain v Belgium: Navigating the Intersection of Privacy and Press Freedom in the Digital Age - Strasbourg Observers' (Strasbourg Observers 3 October 2023) <<https://strasbourgobservers.com/2023/10/03/hurbain-v-belgium-navigating-the-intersection-of-privacy-and-press-freedom-in-the-digital-age/>>.

¹⁰⁵³ See Gavin Phillipson, 'Clarity Postponed: Horizontal Effect after Campbell' [2007] In H. Fenwick, G. Phillipson, & R. Masterman (Eds.), *Judicial reasoning under the UK Human Rights Act* (143-173). Cambridge University Press. <https://doi.org/10.1017/cbo9780511493775.009>; Gavin Phillipson, 'Privacy: The Development of Breach of Confidence – the Clearest Case of Horizontal Effect?' [2011] Cambridge University Press eBooks 136.

Phillipson warns that it could provoke resistance on institutional and systemic grounds, especially if political winds shift and the HRA or UK's ECHR membership were to be undermined or repealed. Phillipson's critique invites caution against overreliance on individualised judicial vehicles, lest they unsettle broader legal stability or become vulnerable to legislative rollback.

However, it can be argued that the existing legal framework fails to fully reflect the realities of contemporary digital privacy violations, particularly in environments where speech is decentralised and perpetrators operate outside traditional media such as newspapers.¹⁰⁵⁴ While the traditional emphasis on journalistic protections has long served as a necessary shield against state intrusion, its continued privileging of expression now risks becoming counterproductive, especially in cases involving anonymous online actors, high-profile influencers, or private individuals engaging in harmful practices such as doxxing or unauthorised dissemination of personal material.¹⁰⁵⁵

In this regard, the legal architecture of injunctive relief, as currently constructed, creates significant asymmetries. Traditional media typically possess the resources to both comply with and contest injunctions using legal counsel. In contrast, individual online wrongdoers, particularly those acting anonymously, often escape scrutiny altogether.¹⁰⁵⁶ This results in a double bind for potential claimants. They must overcome both the high expressive threshold

¹⁰⁵⁴ See Mohamed Chawki, Subhajit Basu and Kyung-Shick Choi, 'Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety' (2024) 13 *Laws* 33, p 5 <<https://www.mdpi.com/2075-471X/13/3/33>>; Sam Stockwell, Georgia Wake and Tooska Dargahi, 'Privacy-Preserving Moderation of Illegal Online Content' (Centre for Emerging Technology and Security 2025), section 2, <<https://cetas.turing.ac.uk/publications/privacy-preserving-moderation-illegal-online-content>>.

¹⁰⁵⁵ See Steven Koh, 'Cancel Culture' and Criminal Justice, (2022) in 74 *Hastings Law Journal* 79, pp 87, 88 <https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4347&context=faculty_scholarship>; Urs Gasser (note 43) p 197.

¹⁰⁵⁶ See Eliza Bechtold, 'Regulating Online Harms: An Examination of Recent Developments in the UK and the US through a Free Speech Lens' (2024) 16 *Journal of Media Law* 1, p 359.

set by s.12(4)(a) of the HRA and the practical difficulties of identifying and attributing digital harms to untraceable non-institutional actors.¹⁰⁵⁷

This structural limitation raises broader questions about whether current remedial doctrines are sufficiently responsive to the realities of contemporary digital harm/intrusion, which is the main question raised in this thesis.¹⁰⁵⁸ Unlike the finite and editorially curated nature of traditional media, online content could remain permanently accessible, undergo viral dissemination, and be algorithmically prioritised,¹⁰⁵⁹ thereby exacerbating the severity of privacy breaches. Yet courts continue to apply speech-protective standards conceived in an age of editorial gatekeeping and professional media ethics, which are arguably ill-suited to the diffuse, anonymous, and often intentionally malicious forms of online expression that characterise the current digital ecosystem.¹⁰⁶⁰

This concern is reflected in Judge Darian Pavli's dissenting opinion in *Hurbain*, where he robustly defended the press's Article 10 ECHR rights, stressing the need for digital press archives to remain historically accurate and complete.¹⁰⁶¹ He criticised the ECtHR majority's approach as a 'facile cleansing'¹⁰⁶² of archives and instead endorsed delisting search results, rather than altering source content, as 'a well-established and functional remedy'.¹⁰⁶³ Complementing this position, the CJEU has stipulated that individuals seeking de-indexing

¹⁰⁵⁷ Fiona Brimblecombe and Helen Fenwick (note 320) p 478.

¹⁰⁵⁸ See *supra* p 29.

¹⁰⁵⁹ See Urs Gasser (note 43) pp 199, 205.

¹⁰⁶⁰ Kyu Ho Youma and Ahran Park, 'The Right to Be Forgotten: Google Spain as a Benchmark for Free Speech versus Privacy?' | Chicago Journal of International Law' (cjil.uchicago.edu2023) section V, pp 185, 186 <<https://cjil.uchicago.edu/print-archive/right-be-forgotten-google-spain-benchmark-free-speech-versus-privacy>>.

¹⁰⁶¹ App. no. 57292/16§ 6 (Pavli, J., dissenting).

¹⁰⁶² Ibid, § 22.

¹⁰⁶³ Ibid, § 12.

must meet the burden of proving ‘manifest inaccuracy’¹⁰⁶⁴ in the contested material.¹⁰⁶⁵

Moreover, the Court extended the RTBF principles to thumbnails and image search results, requiring search engine operators to assess whether the continued display of such images is necessary to uphold certain internet users’ freedom of information.¹⁰⁶⁶

Therefore, while the balance between Articles 8 and 10 remains at the heart of judicial decision-making, there is an urgent need to re-evaluate how these competing rights are balanced in the context of online privacy breaches. The current legal standard, as shaped by s.12(4)(a) HRA and case law on prior restraint, may no longer adequately reflect the asymmetries of power, anonymity, and harm that typify online environments.¹⁰⁶⁷ There is thus a compelling case for future case law or statutory reform to recalibrate this balance, ensuring that privacy rights are not routinely subordinated to outdated conceptions of expressive freedom.

Nevertheless, the UK High Court has touched upon the issue in several influential cases.¹⁰⁶⁸ As Paul Lambert persuasively observes, in the post-Brexit era EU law and CJEU jurisprudence no longer have direct legal effect in the UK, but they continue to exert substantial indirect influence on domestic interpretations of RTBF principles.¹⁰⁶⁹ The tension between privacy and expression has found its clearest articulation in injunctive relief jurisprudence.

¹⁰⁶⁴ See Case C-460/20, *TU and RE v Google LLC*, ECLI:EU:C:2022:962 (Dec. 8, 2022), § 68.

¹⁰⁶⁵ See Kyu Ho Youma and Ahran Park, ‘The Right to Be Forgotten: Google Spain as a Benchmark for Free Speech versus Privacy?’ | *Chicago Journal of International Law* (cjil.uchicago.edu2023) section V, pp 185. 186 <<https://cjil.uchicago.edu/print-archive/right-be-forgotten-google-spain-benchmark-free-speech-versus-privacy>>.

¹⁰⁶⁶ *Ibid.*, ECLI:EU:C:2022:962 (Dec. 8, 2022) § 96.

¹⁰⁶⁷ See Kir Nuthi and Mella Tesfazgi, ‘Reforming the UK Online Safety Bill to Protect Legal Free Expression and Anonymity’ (Itif.org29 August 2022) <<https://itif.org/publications/2022/08/29/reforming-the-uk-online-safety-bill-to-protect-legal-free-expression-and-anonymity/>>; see also on ‘UK’s Online Safety Regime Unable to Tackle the Spread of Misinformation and Cannot Keep Users Safe Online, MPs Warn - Committees - UK Parliament’ (Parliament.uk2019) <<https://committees.parliament.uk/committee/135/science-innovation-and-technology-committee/news/208296/uks-online-safety-regime-unable-to-tackle-the-spread-of-misinformation-and-cannot-keep-users-safe-online-mps-warn/>> accessed 5 August 2025.

¹⁰⁶⁸ See, e.g., *NT1 & NT2 v Google LLC* [2018] EWHC 7999 (QB).

¹⁰⁶⁹ See Paul Lambert, *Right to Be Forgotten*. (Bloomsbury Professional 2022), pp 2–3.

A case in point is *PJS v News Group Newspapers Ltd*,¹⁰⁷⁰ in which the UK Supreme Court upheld an injunction to prevent the publication of details concerning a sexual encounter, even though the information was already circulating online in foreign jurisdictions. The Court rejected the ‘futility’ argument, acknowledging that additional amplification by domestic media would compound the claimant’s harm. However, it also reveals that courts may be willing to restrain institutional media within the jurisdiction but are largely powerless to curtail extraterritorial or anonymous online speech, drawing the attention to the limits of domestic injunctions.¹⁰⁷¹

By contrast, *Mosley v News Group Newspapers Ltd*¹⁰⁷² reveals the limitations of relying solely on post-publication remedies. Although the High Court found that Mosley’s privacy had been violated by the publication of secretly recorded footage of private sexual activity, no injunction was available at the time. The damages awarded were insufficient to fully redress the reputational and emotional harm already done, proving the often-irreversible nature of privacy intrusions and the need for timely injunctive relief in appropriate cases.

The judiciary also recognises the importance of free expression in matters of genuine public interest, as demonstrated in *ABC v Telegraph Media Group Ltd*.¹⁰⁷³ In that case, an interim injunction initially restrained the press from reporting allegations of sexual misconduct by a prominent businessman, protected by non-disclosure agreements. However, the Court of

¹⁰⁷⁰ [2016] UKSC 26.

¹⁰⁷¹ See Thomas De Bennett, *PJS v News Group Newspapers Ltd* (2016). In: Wragg, P. & Coe, P. (Eds.), (2023) *Landmark Cases in Privacy Law. Landmark Cases*. pp 302, 317. Bloomsbury Publishing. ISBN 9781509940783; The Authority of the House of Lord, ‘Regulating in a Digital World’ (2019), p 52, <<https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>>.

¹⁰⁷² [2020] EWHC 3545 (QB).

¹⁰⁷³ *ABC v Telegraph Media Group Ltd* [2018] EWCA Civ 2329.

Appeal later lifted the injunction, finding that the public interest in transparency outweighed the claimant's privacy and contractual expectations. The ruling illustrates the Court's reluctance to impose prior restraints where matters of public debate and accountability are at stake.

More recently, anti-harassment injunctions have emerged as a more adaptable legal tool for tackling online privacy violations, particularly where misuse of private information or defamation claims may fall short. As in *LYJ v Persons Unknown*,¹⁰⁷⁴ the High Court issued an injunction against anonymous online harassers responsible for publishing abusive and defamatory material, which demonstrates the legal system's evolving capacity to engage with anonymity in digital spaces, using harassment law as a doctrinal workaround. As Tugendhat J observed in *ZAM v CFW*,¹⁰⁷⁵ courts may issue interim injunctions in harassment cases even where the content includes private or defamatory allegations, provided it constitutes a course of conduct causing alarm or distress. In *ZAM*, no privacy claim was pursued; rather, the injunction was based solely on harassment via defamatory publications, and the claimant's anonymisation was ordered not for privacy, but to safeguard their Article 8 reputational rights.

What emerges from this analysis is a clear mismatch between legal doctrine and digital harm. Courts continue to operate under a remedial logic shaped by the assumptions of a prior media paradigm, namely, that expression is attributable, traceable, and subject to ethical standards. In contrast, online speech is often fragmented, anonymised, and amplified beyond editorial control. This disjuncture creates a systemic bias in favour of expression, not as a principled commitment to open discourse, but as a legacy of an outdated legal imagination.

¹⁰⁷⁴ [2017] EWHC 3230 (QB).

¹⁰⁷⁵ *ZAM v CFW* [2011] EWHC 476 (QB).

Injunctions and erasure rights, as currently conceived, often function as symbolic remedies: available in theory, but inaccessible or ineffective in practice, especially against digital actors who fall outside the traditional media. The rigid application of s.12(4)(a) HRA, alongside the judiciary's continued deference to journalistic standards, risks institutionalising a hierarchy of harms, one in which victims of decentralised, viral harm are routinely excluded from meaningful redress.

8.2 Reforming China's Data Protection Framework

Building on the foundational analysis provided in Chapters 6 and 7,¹⁰⁷⁶ this section turns to a more focused evaluation of China's personal data protection framework. Having previously examined the broader regulatory architecture, this section deliberately sets aside the general body of laws, excluding the PIPL, in order to concentrate on two key objectives. First, it scrutinises the efficacy and limitations of the PIPL as the primary legislative instrument for safeguarding personal data. Second, and more ambitiously, it explores the feasibility of enacting a specialised, unified Data Protection Act/Law¹⁰⁷⁷ to an extent reflective of the GDPR, that would complement the PIPL, rather than merely exist alongside it.

This proposal draws on comparative insights from the UK's evolving data protection landscape.¹⁰⁷⁸ The idea is to replicate the logic underpinning the codification of the *Civil Code*,¹⁰⁷⁹ whereby disparate legal norms are consolidated into a cohesive and mutually

¹⁰⁷⁶ *supra* pp 194-288.

¹⁰⁷⁷ For example, similar to the UK DPA 2018.

¹⁰⁷⁸ The UK model does not consist of a single, all-encompassing piece of legislation, but rather a complementary legal framework comprising a core regulation.

¹⁰⁷⁹ *supra* p 195, fn 628 and associated text.

reinforcing statutory framework. Such an approach would transform China's fragmented data protection legal landscape into a more coherent model by integrating multiple data-related laws, currently dispersed across administrative, health, cybersecurity, and commercial sectors, into a single, comprehensive Act/Law designed to work in tandem with the PIPL.

This legal unification would serve two vital functions. First, it would resolve persistent issues of regulatory overlap and jurisdictional ambiguity, as discussed in Chapter 6.¹⁰⁸⁰ Under the current regime, multiple regulatory authorities¹⁰⁸¹ may claim concurrent jurisdiction over the same dataset, particularly in sensitive domains like healthcare or financial services. This redundancy not only undermines enforcement efficiency but also creates legal uncertainty for both data subjects and controllers. Second, such a reform would clarify the scope and application of the law, providing individuals with a more predictable, navigable framework and reducing interpretive inconsistencies among courts and regulators.

8.2.1 Is a specific Data Protection Act necessary?

At present, China's data protection system remains fragmented and reactive,¹⁰⁸² governed by a mixture of general laws, sectoral rules, and administrative orders that lack the coherence and enforceability of the GDPR. This divergence leaves China at a critical juncture, whereby the strategic implementation of a dedicated Data Protection Act could bridge this institutional gap and consolidate its governance ambitions. Since 2022, the Chinese social media platform Weibo has published over 115 community announcements addressing the issue of online privacy breaches.¹⁰⁸³ Among the most concerning phenomena is the practice of 'doxxing',

¹⁰⁸⁰ *supra* section 6.2.3.

¹⁰⁸¹ *supra* pp 209-210.

¹⁰⁸² See *supra* pp 200-203.

¹⁰⁸³ See online community announcements on <http://weibo.com/7006227546/5188331732469926>.

which derived from the informal abbreviation of ‘dropping documents,’ refers to the deliberate researching, aggregating, and public disclosure of private or personally identifying information about an individual, typically without their knowledge or consent, and with the purpose or foreseeable effect of exposing them to harassment, reputational harm, intimidation, or physical danger. The information disclosed through doxxing may include home addresses, telephone numbers, workplace details, financial information, relationship status, photographs, and any other personal data whose targeted public disclosure renders the subject identifiable and vulnerable to harm. There are instances where the doxxing originates from foreign websites, particularly Telegram, which has long been criticised for enabling privacy violations. In several widely discussed incidents, personal images and information circulated on Weibo were initially disseminated on Telegram before being reproduced within the platform’s ecosystem.

One illustrative example occurred in May 2023, when a web influencer, known as Jack Latiao,¹⁰⁸⁴ was exposed for committing acts of extreme cat cruelty and selling videos of the abuse on Telegram. The incident drew public attention to the phenomenon of performative, violent animal abuse. In the wake of the backlash, a number of celebrities, such as Zhang Xinyu, Zhao Lusi, and Wang Yibo, publicly condemned the abuse on Weibo. Jack therefore alleged that he had their private information, including ID numbers, phone numbers, and social security records, and leaked that information online to obtain ‘revenge’. Despite the apparent illegality of these disclosures, he has not been punished.¹⁰⁸⁵ The lack of legal response may be attributed, in part, to the public nature of ‘celebrities,’¹⁰⁸⁶ which discourage them from initiating legal action due to reputational risk or futility.

¹⁰⁸⁴ See Diyicaijing, “‘人肉开盒’深度调查：谁在售卖你的隐私’ (Yicai.com2023) <<https://www.yicai.com/news/101922672.html>> accessed 6 August 2025 (only Chinese text).

¹⁰⁸⁵ Ibid.

¹⁰⁸⁶ See further analysis on Aisha Hussain, ‘Privacy, Celebrities and the Media’ (Legal Cheek12 November 2019) <<https://www.legalcheek.com/lc-journal-posts/privacy-celebrities-and-the-media/>>.

A second common scenario involves organised doxxing within Weibo's own fan communities (commonly structured around 'chaohua').¹⁰⁸⁷ These instances often entail coordinated attacks by fans against both celebrities and ordinary individuals, involving the intentional exposure of private information. This form of digital vigilantism is frequently not monetarily motivated; rather, it is driven by affective impulses such as indignation, own idol protection, or retaliation.

Thirdly, Weibo serves as a secondary dissemination channel for doxxed content originating on other domestic platforms. These privacy violations result from the uncritical reproduction and amplification of personal data, often under the pretext of supporting online narratives or public debates. Here, the fan-based digital culture operates outside of profit incentives and instead mobilises privacy violations as a form of collective punishment or symbolic retribution.

The issue is not confined to fans or civilians acting without institutional resources. A case from Foshan further illustrates how government officers have become complicit in systemic privacy violations. According to the Nanhai District People's Court,¹⁰⁸⁸ from 2019 onwards, five employees of a high-speed railway station exploited their positions to illegally access and sell personal travel data and identity numbers of celebrities. A secondary group of three individuals profited by reselling this data at a markup, ultimately making over 560,000 RMB. The case was heard at first instance by the Nanhai District People's Court and on appeal by the Foshan Intermediate People's Court. Following a full trial, the courts held that the eight defendants had violated national data protection regulations by selling personal information acquired either

¹⁰⁸⁷ See online <http://weibo.com/>.

¹⁰⁸⁸ There is no original judgment available online; See official report of Foshan court on their web account: <https://mp.weixin.qq.com/s?biz=MzA3NDQ4MDA4NA==&mid=2652809642&idx=1&sn=a8104d9b39ba8b9a5dbefb9d56b83e0e&chksm=84952911b3e2a007afdad858227b31ed596cb73d570975b64879a1bc08ff4d0bd346b4b4d6de&scene=27>.

through the discharge of official duties or by other unlawful means. Their actions constituted the criminal offence of violating citizens' personal information, as set out under Article 253 of Chinese Criminal Law.¹⁰⁸⁹

The court further found that the conduct of the defendants harmed not only the specific individuals targeted but also disrupted the general order of lawful data collection and processing.¹⁰⁹⁰ In particular, the dissemination of such information affected a broad, indeterminate group of data subjects, thereby undermining public trust in information governance and damaging the public interest. As a result, the court imposed custodial sentences ranging from nine months to three years and eight months. In addition to criminal liability, the defendants were held jointly liable in civil law for the infringement of public interest. The judgment ordered them to pay a total of 567,530 RMB in civil compensation for the harm caused, to delete the unlawfully obtained information, and to issue a public apology.¹⁰⁹¹

Apparently, the action of the invading of the personal information expanded to include video creators, niche performers, and online influencers, eventually even extending to ordinary internet users. Disagreements in comments (on X or Instagram) have led to individuals being targeted, with users submitting screenshots for wider dissemination and public condemnation. In reality, the threat of privacy invasion is not limited to public figures. Any individual may become vulnerable to being 'digitally stripped bare.'¹⁰⁹² Investigative journalism into the black

¹⁰⁸⁹ *supra* pp 217-218 fn 742 and associated text; Article 253 of the Criminal Law: addresses violations of citizens' personal information, including illegal sale or provision of such information.

¹⁰⁹⁰ See Diyicaijing, ““人肉开盒”深度调查：谁在售卖你的隐私” (Yicai.com2023) <<https://www.yicai.com/news/101922672.html>> accessed 6 August 2025 (only Chinese text).

¹⁰⁹¹ *Ibid.*

¹⁰⁹² *Ibid.*

and grey data markets has revealed that for as little as 700 RMB (roughly £75),¹⁰⁹³ a person's private information, including hotel check-ins, flight records, mobile data usage, and banking activity, can be easily purchased. Vendors within this illicit ecosystem even claim to provide 24/7 global surveillance and data access services.¹⁰⁹⁴

This dystopian commodification of personal data, combined with the weaponisation of private information in online culture, exposes critical structural and regulatory deficiencies in current data protection regimes. Not only does this landscape facilitate unchecked intrusions into personal life, but it also creates an environment in which violations of dignity, autonomy, and legal identity can occur with minimal consequence. The failures to effectively regulate doxxing, whether originating from foreign platforms, domestic fan cultures, or institutional insiders, raise urgent questions about the limits of existing legal frameworks, enforcement capabilities, and the role of platforms in facilitating or failing to prevent such abuses.

These cases thus exemplify the current systemic risks inherent in China's fragmented data protection apparatus, judicial system and enforcement protections.¹⁰⁹⁵ While individual accountability could be pursued in clear-cut cases, the institutional enforcement landscape remains underdeveloped, particularly when it comes to resolving the tension between individual rights and competing state or economic interests.¹⁰⁹⁶ Without reform, the current

¹⁰⁹³ See news on Fazhiribao, '粉丝购买航班信息只为与偶像同机_法治网' (Legaldaily.com.cn2022) <http://www.legaldaily.com.cn/zt/content/2022-04/13/content_8702790.htm> accessed 6 August 2025 (only Chinese text).

¹⁰⁹⁴ Ibid.

¹⁰⁹⁵ See Xiongbiao Ye and others, 'Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective' (2024) 48 Telecommunications Policy 102851, p 6.

¹⁰⁹⁶ Ibid, pp 7, 8.

regime risks entrenching a double standard,¹⁰⁹⁷ whereby symbolic enforcement actions substitute for meaningful structural accountability, despite the existence of the CAC.¹⁰⁹⁸

In conclusion, the enactment of a unified and specialised Data Protection Act represents not merely a legislative reform, but a strategic recalibration of China's approach to data governance. Such a statute would provide conceptual clarity, institutional coordination, and normative coherence, all of which are essential for a rights-based and transparent data protection ecosystem.

8.2.2 Toward legal harmonisation: unifying fragmented personal data regulations in China

A key reform step involves harmonising these fragmented regulations into a comprehensive and cohesive legal framework. This would require clarifying regulatory responsibilities, standardising data processing principles, and consolidating enforcement practices. The harmonisation process could benefit from lessons drawn from the GDPR and the DPA 2018, which unifying diverse data protection rules into a coherent framework.

In China, the illicit trade and dissemination of personal information are particularly prevalent within the entertainment industry, as discussed above.¹⁰⁹⁹ While most of these practices are profit-driven,¹¹⁰⁰ some are motivated by non-commercial interests, such as the fan culture practice of sharing celebrities' personal data, especially flight/airport information or phone

¹⁰⁹⁷ See Raymond Yang Gao, 'A Battle of the Big Three? —Competing Conceptualizations of Personal Data Shaping Transnational Data Flows' (2023) 22 Chinese journal of international law 707, pp 771, 784, 785.

¹⁰⁹⁸ See official website on 'CyberspaceAdministrationofChinaLaunchesInitiativeonChina-AfricaJointlyBuildingaCommunitywithaSharedFutureinCyberspace' (www.cac.gov.cn) <https://www.cac.gov.cn/2021-08/25/c_1631480920680924.htm>.

¹⁰⁹⁹ See *supra* pp 321-323.

¹¹⁰⁰ See Yan Luo, 'Analysing China's PIPL and How It Compares to the EU's GDPR' (Inside Privacy 25 August 2021) <<https://www.insideprivacy.com/data-privacy/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/>>.

number, for entertainment or communal engagement purposes. These instances often involve limited circulation within small, closed groups rather than large-scale dissemination.

This institutional deficiency becomes particularly salient when viewed through the lens of recent high-profile privacy breaches, such as the case involving actress Kathy Chow Hoi-mei, which was previously examined in Chapter 7.¹¹⁰¹ In that incident, a hospital employee unlawfully accessed and disseminated the actress's confidential medical records via WeChat groups, triggering widespread public condemnation.¹¹⁰² Authorities responded with administrative detention for the employee and an investigation into the hospital.

However, while these responses suggest a growing awareness of data protection imperatives, the case reveals critical gaps in institutional safeguards and legal enforcement. For example, there has been no transparent disclosure from authorities regarding whether the hospital faced financial penalties or regulatory sanctions. This opacity raises questions about the deterrent strength of the current legal framework. Without clear outcomes or a publicly accessible enforcement log, the public is left uncertain about whether institutional actors are being held accountable. Such ambiguity weakens both the perceived legitimacy of the legal system and its practical effectiveness in deterring future breaches. Moreover, the absence of a centralised information platform, incorporating updates from authorities, official records, and media coordination, further exacerbates the deficit of public trust in the data governance regime.

¹¹⁰¹ See *supra* pp 269-270.

¹¹⁰² See news on Anndrea A Webber, 'Staff Who Leaked Late HK Actress Kathy Chow's Medical Report to "Show Off" Gets Arrested' (The Star 14 December 2023) <https://www.thestar.com.my/lifestyle/entertainment/2023/12/14/staff-who-leaked-late-hk-actress-kathy-chows-medical-report-to-039show-off039gets-arrested#goog_rewarded> accessed 6 August 2025.

As demonstrated, the fragmented nature of China's data governance system, spread across overlapping laws, departmental policies, and sector-specific guidelines, produces inconsistencies that ultimately weaken the credibility, predictability, and enforceability of online privacy rights.¹¹⁰³ A case that exemplifies this issue is *Maskpark*.¹¹⁰⁴ It refers to a series of large-scale groups on the Telegram, where tens of thousands of users from China shared private information as to their female family members and some sexually explicit content, much of it non-consensually obtained. The group's members covertly filmed women in public spaces such as Metro and shopping malls and disseminated intimate photos and videos of their girlfriends, wives, and even, in the most horrifying cases, reportedly involving a father livestreaming the sexual assault of his biological daughter.¹¹⁰⁵

The *Maskpark*, in which large volumes of sensitive personal data, were illegally collected, distributed, and monetised through a subscription-based Telegram channel, is emblematic of how existing legal tools fail to address tech-forms of data exploitation. Unlike the case of *Ma*,¹¹⁰⁶ which was arguably the result of individual misconduct within a semi-closed academic environment, *Maskpark* was industrialised in nature. It represented a coordinated, anonymised, and transnational form of digital abuse, involving multiple perpetrators, blockchain payments, and transboundary hosting platforms. Despite public outcry, the *no* response from regulatory authorities was indicative of a system that lacks not only institutional readiness but also the jurisdictional coherence necessary to tackle data crimes in the digital era. Unlike South Korea's

¹¹⁰³ *supra* section 6.2.3 and section 7.4.

¹¹⁰⁴ See Jiang Xinyi, Chinese Women, Children Targeted in Cross-Border Voyeurism Ring (2025) (Sixthtone.com2025) <<https://www.sixthtone.com/news/1017409>> accessed 6 August 2025.

¹¹⁰⁵ See News Desk, "Mask Park" Exposed: Secret Telegram Group Triggers Outrage in China after Thousands Share Intimate Photos' (@mathrubhumi26 July 2025) <<https://english.mathrubhumi.com/news/world/mask-park-telegram-group-triggers-outrage-in-china-after-thousands-share-intimate-photos-dziw9fud>> accessed 6 August 2025.

¹¹⁰⁶ See *supra* pp 262.

'Nth Room' case,¹¹⁰⁷ which had a central figure orchestrating the crimes, the group in *Maskpark* lacked a clear leader. Instead, it was composed of ordinary individuals, students, seemingly respectable citizens, whose disturbing actions under anonymity exemplify what Hannah Arendt famously termed the banality of evil.¹¹⁰⁸ The anonymity, online misogyny¹¹⁰⁹ and decentralisation of such abuse networks make them more pervasive and harder to detect, exacerbating their social and legal danger.

The inability to rapidly identify and prosecute those responsible in the *Maskpark* demonstrates how existing legal frameworks in China remain ill-equipped to handle multi-jurisdictional, tech-enabled privacy violations. Even though the PIPL provides foundational principles of data processing and user rights, it functions more as a declaratory framework than an effective enforcement mechanism when deployed in isolation. Furthermore, the lack of transparency surrounding outcomes, such as whether the platforms were sanctioned, whether the victims were compensated, or what long-term policy reforms followed, undermines the legitimacy of the existing enforcement regime. Public trust is eroded when laws appear ineffective,¹¹¹⁰ and victims are left without clear avenues for restitution. Just as the *Ma* case pertained to insufficient preventive measures within educational institutions, the *Maskpark* one exposes

¹¹⁰⁷ Since 2019, South Korea has been grappling with a particularly complex case of online sexual exploitation involving a network of encrypted chat rooms known as the Nth Room case. These chatrooms functioned as exclusive messaging groups where users produced, distributed, and exchanged sexually exploitative content, often obtained through coercion and blackmail targeting women and girls. Perpetrators would initially approach victims via twitter or messages, luring them with deceptive messages claiming that their private photos had been leaked. Upon clicking the provided link, victims inadvertently exposed their photos and videos, which was then used to further manipulate and exploit them. The Nth Room case not only revealed the dangers of digital exploitation but also triggered the similar exploitative networks on Telegram.

¹¹⁰⁸ Lyndsey Stonebridge, 'Hannah Arendt's Lessons for Our Times: The Banality of Evil, Totalitarianism and Statelessness' (The British Academy 2024) <<https://www.thebritishacademy.ac.uk/blog/hannah-arendts-lessons-for-our-times-the-banality-of-evil-totalitarianism-and-statelessness/>>.

¹¹⁰⁹ See Haiyan Wang and Lulu Yuan, 'State, Platform, and Misogynistic Disinformation in China' (2023) 8 Global Media and China; Sara Liao, 'Gender Trolling: Digital Manosphere and Misogyny in China | GJIA' (Georgetown Journal of International Affairs 5 May 2025) <<https://gjia.georgetown.edu/2025/05/05/gender-trolling-digital-manosphere-and-misogyny-in-china/>>.

¹¹¹⁰ *supra* section 7.4.

failures in cross-platform regulation, especially regarding intermediary responsibility and proactive takedown obligations.

While the previous cases reveal structural deficiencies, the *Maskpark* incident offers an even sharper lens through which to examine the limitations of the current regulatory model and the urgent need for legal harmonisation. The incident raised questions about accountability and remedial mechanisms: what penalties were imposed, and were they sufficient to deter similar conduct? The answer is no: the *Maskpark* incident tells us that the efforts are still insufficient, or even non-existent.

Harmonisation would clarify liability in cases where harm results from third-party use of data, such as platform distribution or automated algorithmic profiling. It would also address the current ambiguity between civil, administrative, and criminal liability in data abuse cases. The *Maskpark* incident blurs the boundary between criminal conduct, privacy invasion, and gender-based harassment. Without a coherent legal structure to bridge these domains, responses remain disjointed. The silence of the mainstream media in reporting¹¹¹¹ these cases further exacerbate the secondary victimisation experienced by those affected, contributing to a culture of impunity and marginalisation.

Maskpark illustrates that China's current piecemeal approach to data protection regulation is not only insufficient but increasingly obsolete in the face of fast evolving, decentralised digital harms. Harmonisation is no longer a normative ideal; it is a pragmatic necessity. Drawing inspiration from the GDPR's structural clarity and the UK's post-Brexit adaptive regulatory

¹¹¹¹ See News Desk, “‘MaskPark’ Exposed: Secret Telegram Group Triggers Outrage in China after Thousands Share Intimate Photos’ (@mathrubhumi26 July 2025) <<https://english.mathrubhumi.com/news/world/mask-park-telegram-group-triggers-outrage-in-china-after-thousands-share-intimate-photos-dziw9fud>>.

thinking, a unified legal framework would consolidate scattered norms, reduce institutional ambiguity, and create the conditions for timely, transparent, and rights-focused enforcement.

8.2.3 Embracing a GDPR-style, rights-based approach for China

Victims in China frequently find themselves with no clear legal recourse in cases of personal data violations, due in large part to the fragmented nature of existing legal provisions. With no structured remedies available, many are left with no option but to turn to the internet, particularly platforms like Weibo, to seek help. This has led to a troubling phenomenon whereby Weibo, a social media platform, becomes a ‘self-judging court,’ relying on public opinion to pressure authorities into action. Such reliance on extrajudicial influence indicates a dysfunctional legal system and reflects a concerning absence of institutional responsiveness.

Attempts at legal redress, such as collective litigation similar to that attempted in *Lloyd v Google*,¹¹¹² are virtually impossible in this context. The dispersed and anonymous nature of perpetrators, combined with the overwhelming scale of data exposure, renders coordinated legal action among victims highly impractical. So far, responses have been largely limited to feminist activists protesting on various online platforms. It is worthy of mention that no victims in *Maskpark* had pursued legal remedies under the PIPL, the Cybersecurity Law, or even the Criminal Law as yet. Recent judicial decisions demonstrate a tentative but growing recognition of data subject autonomy within China’s legal system. In the case of *Yang v Lin*,¹¹¹³ for example, the plaintiff objected to the continued online publication of her identifiable information, initially disclosed lawfully during a recruitment process. The court ruled that

¹¹¹² [2021] UKSC 50.

¹¹¹³ *Yang v Lin* [2024] Beijing Internet Court CLI.C.555521261.

despite the original lawful publication, the refusal to permit further dissemination under Article 27 of the PIPL triggered new obligations, requiring the defendant to delete the relevant data. This ruling affirms that data subjects can exercise control over their personal information post-disclosure.¹¹¹⁴

However, any transition to a rights-based framework must be carefully attuned to China's unique institutional and political configuration.¹¹¹⁵ The primacy of national security, the strategic role of data in economic governance, and the centralised regulatory structure are likely to remain dominant considerations in the legislative and enforcement process. Thus, the success of rights-based reform will hinge on the extent to which legal theory is matched by institutional practice, and on whether privacy rights are positioned as genuinely actionable within the broader governance ecosystem. Absent such reform, the promise of digital rights in China will remain unevenly realised, vulnerable to both bureaucratic inertia and selective enforcement.

8.3 Conclusions as to the Research Questions of the Thesis

Following the discussions and analysis presented in the preceding seven chapters and above, this concluding section synthesises the core findings of the thesis and systematically addresses the key research questions posed at the outset:¹¹¹⁶ 1) how far is the GDPR effective in regulating the misusing of personal information online? It asks how far it can provide for effective *ex ante* action to shield data subjects from privacy invasion online? 2) Through a

¹¹¹⁴ *supra* p 278.

¹¹¹⁵ See Xiongbiao Ye and others, 'Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective' (2024) 48 Telecommunications Policy 102851, p 6.

¹¹¹⁶ *supra* p 29.

comparative analysis of the UK experience, it asks whether China can feasibly consolidate its fragmented data regulatory framework and assesses the necessity of enacting a dedicated and unified Data Protection Act to supplement and embraces a GDPR-style, rights-based approach.

This thesis has offered an in-depth comparative analysis of the data protection legal regimes in the UK (chapters 3-5) and China (chapters 6-7), contextualised within the accelerating datafication of the digital age. As personal data is collected, processed, and disseminated on an unprecedented scale, online privacy has emerged as a critical legal and societal concern. In this evolving environment, courts in the UK and EU have become central forums for interpreting, enforcing, and at times reshaping data protection norms.

This thesis has used a range of recent cases to evaluate the effectiveness of the current data protection regime in the UK and China in order to consider whether the present remedies for individuals are sufficient or whether there is too much emphasis on the protection of the individuals' privacy in the UK. It has also considered the instances of protection of the freedom of expression in the area of the media/press where privacy is also at stake, and the new trend of the self-publisher online in the UK and China.

8.3.1 The United Kingdom

The thesis finds that current UK remedies are meaningful but incomplete: judges have responsibly filled statutory gaps, yet the combination of procedural hurdles, technological permanence, and cross-border diffusion means that many victims still receive inadequate

protection. Central to this inquiry of whether data protection and other measures can effectively regulate the misuse of personal information online is the capacity of the regime to deliver *ex ante* protection, i.e., preventive measures that shield data subjects from privacy invasions before the harm materialises, as opposed to relying on post-publication remedies. In *NT1 & NT2 v Google*, the High Court adapted data protection (reflective of the later GDPR provisions) provisions to the realities of search engine indexing, ordering the delisting of links while balancing this restriction with the public's Article 10 ECHR rights. This reflects the GDPR's latent *ex ante* potential; by compelling removal of content from search results, it can significantly reduce further dissemination. However, as the *PJS v News Group Newspapers* line of cases demonstrate, injunctive relief often struggles to contain information already in circulation, especially in the networked online sphere. The resulting tension is clear: while the GDPR's Article 17 'right to erasure' can operate preventively in theory, its practical effect is constrained once information has gone viral or crossed borders.

Chapters 3 to 5 examined the UK's trajectory in detail, revealing a marked judicialisation of data protection law. UK courts have emerged as central actors in developing privacy jurisprudence, especially in interpreting vague statutory provisions, scrutinising governmental surveillance practices, and responding to emergent threats such as algorithmic profiling and mass data breaches. This judicial ascendancy is not coincidental. It stems from several interrelated pressures: the inherent ambiguity of legislative frameworks, the regulatory vacuum left by Brexit, and the technological acceleration outpacing statutory reform. Consequently, courts have played a quasi-legislative role in shaping privacy doctrine, extending tort-based remedies, delineating the boundaries of informed consent, and evolving doctrines such as the right to be forgotten.

In order to understand and evaluate the effectiveness of the current remedies for individuals, this thesis bringing these threads together yields three critical observations: (1) the UK's judicialisation of data protection is rational and largely inevitable, but it cannot substitute wholly for legislative clarity;¹¹¹⁷ (2) the 'medium-based' distinction (traditional press v. internet) that appears in precedent risks miscalibrating harm in an era of algorithmic amplification;¹¹¹⁸ and (3) the lack of injunctive relief under the GDPR.

Although the UK GDPR is substantively similar to its EU counterpart, courts have shown an emerging tendency to require demonstrable damage for compensation, potentially raising the bar for claimants and reducing access to remedies for minor infringements.¹¹¹⁹ The reliance on courts as primary arbiters of online privacy reflects the persistent tension globally between law and technology, and between state power and individual rights. While the judiciary has played a formative role, not only in interpreting but also in shaping data protection norms, the resulting regime in the UK privileges litigants with the means to pursue complex claims, raising normative questions about justice and fairness. As new technologies constantly continue to

¹¹¹⁷ See Orla Lynskey, 'Complete and Effective Data Protection' (2023) 76 Current Legal Problems 297 <<https://academic.oup.com/clp/article/76/1/297/7304257>>, pp 318, 322.

¹¹¹⁸ See Benjamin Laufer & Helen Nissenbaum, 'Algorithmic Displacement of Social Trust' (Knightcolumbia.org2015) <<https://knightcolumbia.org/content/algorithmic-displacement-of-social-trust>> pp 28-30; House of Commons committee report, 'social media, Misinformation and Harmful Algorithms' (Parliament.uk2024) <<https://publications.parliament.uk/pa/cm5901/cmselect/cmsctech/441/report.html>>; section 1.6.

¹¹¹⁹ For example, in *Lloyd v Google LLC*, the UK Supreme Court ruled against a claim for damages based on the unlawful processing of personal data where there was no quantifiable harm; see Will Murphy, 'Suffering, Damage, the GDPR – and All That | Cornerstone Barristers' (Cornerstone Barristers5 May 2023) <<https://cornerstonebarristers.com/suffering-damage-the-gdpr-and-all-that/>> accessed 14 August 2025.

generate online privacy harms, and as legislative reform remains reactive at best, courts are likely to remain the *de facto* first responders to data protection disputes.¹¹²⁰

Litigation, therefore, has become the primary mechanism for vindicating online privacy, but this litigation-centric model has three structural drawbacks. First, access to judicial relief is unequal: sophisticated claimants with resources and specialist counsel are advantaged, while low-income, anonymous or cross-border claimants are effectively shut out. Second, judicial remedies are typically too slow or too brittle to undo viral harms, the removal of a link or an award of damages rarely restores the pre-publication status quo. Third, recent authority (the Supreme Court's treatment of representative and damages claims in *Lloyd v Google*)¹¹²¹ provides a tightening of evidentiary requirements for redress in data-processing cases, potentially raising the hurdle for aggregate or non-material harms and narrowing collective-action routes. Together these trends produce a paradox, which is that of courts expanding doctrinal protection, but procedural and evidential rules may in practice restrict meaningful relief for many victims.

This thesis has evaluated these dynamics through a series of landmark cases. For instance, *NT1 & NT2 v Google*, *Axel Springer*, *Hurbain*, and *M.L. & W.W.* illustrate the evolution of the right to be forgotten and its balancing against the public interest in freedom of expression.¹¹²² While early jurisprudence maintained a tenuous equilibrium between Articles 8 and 10 of the ECHR, recent decisions, especially *Hurbain*, provide a doctrinal tilt toward privacy, even at the cost of

¹¹²⁰ See Leon Trakman, Robert Walters and Bruno Zeller, Tort and Data Protection: Are There Any Lessons to be Learnt? (2019) EDPR Review, 5(4), 1-20 UNSW Law Research Series No. 19-104, pp 14-16, Available at SSRN: <https://ssrn.com/abstract=3630004> or <http://dx.doi.org/10.2139/ssrn.3630004>.

¹¹²¹ *supra* pp 117-118.

¹¹²² *supra* section 5.4.2.

archival integrity and press freedom. This shift reflects judicial anxiety about the enduring visibility of reputationally damaging content in the digital sphere, but it also generates legal uncertainty for media actors and online publishers, including self-publishers who now function within quasi-journalistic roles.

The RTBF has migrated from a narrow data-protection remedy (CJEU's *Google Spain*) to a layered doctrine that now implicates press archives, search engines, and primary publishers. *Google Spain* established that links to lawful historical content might nonetheless become incompatible with processing rules and therefore removable from search indexes; Strasbourg and domestic courts have since grappled with how that logic applies as against traditional newspapers and archives. *Hurbain* and *M.L. & W.W.* illustrate the resulting doctrinal complexity: the courts must weigh archival integrity and the public-interest value of the press against the enduring reputational harms of persistent online availability. Those decisions show the RTBF is not merely a technical 'delisting' exercise but a normative judgment about collective memory, historical record and individual rehabilitation, issues the judiciary currently resolves without a single, uniform legislative mandate.

Similarly, the court's evolving approach to the reasonable expectation of privacy, grounded in precedents such as *Campbell v MGN*, reveals a heightened sensitivity to context, content, and individual identity. Yet this contextualism, while flexible, renders outcomes unpredictable. In terms of collective redress, cases such as *Lloyd v Google* highlight the challenges of conceptualising non-material damage and the scope of class claims. Although *Lloyd* curtailed representative actions for data misuse, it invites a broader conversation about the doctrinal tools necessary to address systemic and latent harms.

The CJEU has, through *Google Spain* and *GC and Others*,¹¹²³ clarified that search engines may be obliged to delist links where the continued processing is incompatible with GDPR principles, even if the original publication was lawful. This doctrinal move strengthens *ex ante* protection by targeting secondary dissemination rather than the original content, thus limiting exposure before further harm accrues. Yet, as the ECtHR acknowledged in *M.L. and W.W. v Germany*, persistent online availability, even in news archives, can perpetuate reputational harm long after the initial publication. The challenge lies in applying preventive orders to actors across multiple jurisdictions, a domain where the GDPR's territorial scope under Article 3 meets realpolitik and enforcement fragmentation.¹¹²⁴

The GDPR's preventive capacity is tempered by several systemic constraints. First, enforcement remains complaint-driven and reactive: supervisory authorities seldom act preemptively without a trigger, leaving many infringements unaddressed until after harm occurs. Second, procedural timelines and appeal rights, while crucial for due process, dilute the immediacy needed for online harm prevention. Third, platforms can comply formally while undermining substantive outcomes, for instance, by removing specific URLs but allowing the same content to reappear under new identifiers. As Orla Lynskey notes, the GDPR's architecture prioritises accountability and *post-hoc* correction over continuous real-time intervention, making it less suited to the speed and replicability of online dissemination.¹¹²⁵

¹¹²³ *GC and Others v Commission nationale de l'informatique et des libertés* (CNIL) (2019) C-136/17, ECLI:EU:C:2019:773.

¹¹²⁴ *supra* section 4.3

¹¹²⁵ See Orla Lynskey, 'Complete and Effective Data Protection' (2023) 76 *Current Legal Problems* 297, p 299 <<https://academic.oup.com/clp/article/76/1/297/7304257>>.

Preventive measures inevitably engage Article 10 ECHR and the GDPR's own Recital 4, which recognises the need to balance data protection with other fundamental rights. Cases such as *Axel Springer v Germany* and *Hurbain v Belgium* illustrate that courts privilege privacy where the public-interest value of information is low and the harm to the individual is severe, but they also show judicial caution about undermining archival integrity and press freedom. The GDPR does provide derogations for journalistic purposes under Article 85, which can significantly narrow *ex ante* action in media contexts, especially against traditional news outlets. The result is a differentiated regime in which preventive relief is more attainable against intermediaries (like search engines) than primary publishers.

The GDPR has clearly demonstrable *ex ante* capabilities, mostly in delisting, erasure, and restriction-of-processing provisions, but these are mediated by jurisdictional limits, and the need to balance competing rights. Its preventive effect is strongest when targeting intermediaries that amplify rather than originate content, and weakest against primary publishers, especially where journalistic exemptions apply.¹¹²⁶

8.3.2 China

China's data governance approach, as analysed in Chapters 6 and 7, is characterised by legislative decentralisation and administrative enforcement. The promulgation of the PIPL, the DSL, and the CSL between 2017 and 2021 constitutes a rapid and ambitious attempt to erect a comprehensive statutory architecture. However, it is embedded within a broader governance

¹¹²⁶ *supra* pp 168-169, 173-174, 276.

paradigm that prioritises national security, public morality, and state sovereignty over individual autonomy and judicial independence.

The PIPL builds GDPR-style substantive rights into statutory form but locates enforcement predominantly through administrative regulators and state levels. That arrangement produces faster administrative takedown and sanctioning tools in some contexts, but it also embeds greater state control that complicate claims about individual autonomy. China's statutory-administrative model can deliver quick, top-down remedies, yet it does so within a political architecture that privileges state interests in ways that liberal democracies would find difficult to reconcile with free expression norms.

As revealed in case studies such as the *Maskpark* incident, discussed in Section 8.2.2,¹¹²⁷ victims of data abuse often face substantial hurdles in securing effective remedies. This thesis argues that this gap is not merely institutional but sociopolitical, reflecting deeper tensions between individual rights and dominant norms, including widespread online misogyny and insufficient institutional commitment to online gender-based harm. Furthermore, China's lack of a robust system of judicial review and binding precedent limits the capacity of its courts to shape privacy doctrine in real-time or to adapt flexibly to novel harms. Moreover, while the PIPL provides a detailed substantive framework, its implementation remains opaque, and mechanisms for individual redress are often underdeveloped or procedurally inaccessible. As algorithmic profiling, biometric surveillance, and cross-border data transfers become more pervasive, the limitations of China's state-led model may become increasingly salient.

¹¹²⁷ *supra* pp 328-330.

8.3.3 Conclusions

At this final stage, it is necessary to return to the research questions that animated this thesis. The analysis has shown that neither the UK nor China offers a definitive model for securing data protection in a digitalised regulatory order, but both provide instructive lessons for understanding how institutional structures shape the enforceability of individual rights. The first research question,¹¹²⁸ whether judicial enforcement can provide an effective safeguard for personal data, has been addressed through the UK experience. Courts have expanded the boundaries of data protection through doctrines such as misuse of private information and the awarding of damages for non-pecuniary harm. Yet the judicial model, while dynamic, generates uncertainty, cost barriers and inconsistent application, revealing that effectiveness is contingent on procedural accessibility rather than purely on substantive legal rights.

The second research question,¹¹²⁹ whether China can feasibly consolidate its fragmented data regulatory framework, has been examined in its unique context. China's top-down regulatory architecture delivers efficiency and coherence, but it also entrenches opacity, renders individual agency limited, and leaves key concepts such as harm, consent and redress under-defined. The contrast between judicial pluralism and regulatory centralism reveals that institutional design is inseparable from socio-political conditions. Both systems struggle to provide accessible and meaningful remedies for mass data breaches, but they fail for different reasons.¹¹³⁰

¹¹²⁸ *supra* p 29; 1) how far is the GDPR effective in regulating the misusing of personal information online? It asks how far it can provide for effective *ex ante* action to shield data subjects from privacy invasion online?

¹¹²⁹ *Ibid*; 2) whether China can feasibly consolidate its fragmented data regulatory framework and assesses the necessity of enacting a dedicated and unified Data Protection Act to supplement and enhance the existing legal system, possibly relying on aspects of the GDPR as a model.

¹¹³⁰ See *supra* sections 8.1 and 8.2.

China's evolving data protection architecture could, in principle, draw on aspects of the GDPR to enhance accountability and individual redress. However, any reform must recognise that legal norms cannot be divorced from their ideological foundations; meaningful convergence is possible only within parameters set by political legitimacy and administrative control. Any such borrowing is constrained by China's socio-political priorities, particularly the centrality of state interests and the limited role of courts. As argued in Chapter 6,¹¹³¹ the right to be forgotten, one of the GDPR's symbolically and practically significant innovations, illustrates these limits in China.

This comparative inquiry analyses that while the UK and China represent divergent models, one grounded in judicial dynamism, the other in regulatory centralism, they confront similar structural challenges. Both systems struggle to define harm and calibrate effective remedies in the context of widespread data breaches. Yet their institutional responses diverge sharply. The UK's reliance on courts risks legal inconsistency and exclusionary access, China's administrative dominance risks opacity and overreach. The tension between innovation and individual rights, between state interest and personal autonomy, runs as a common thread through both jurisdictions.

Having returned to the research questions, this thesis contends that courts in the UK and in China, although institutionally distinct, have become *de facto* arbiters of data protection and privacy in practice. The evolution of data protection law will depend less on legislative design than on how legal actors interpret, enforce and internalise evolving principles of autonomy and

¹¹³¹ *supra* pp 219-225.

dignity. As technologies continue to transform the landscape of human dignity and vulnerability, the law's response must be principled, adaptive, and equitable.

Overall, the thesis contributes to legal scholarship by bridging doctrinal analysis with comparative and socio-legal perspectives. The findings suggest that while no single model offers a perfect solution, meaningful data protection must grapple with a complex interplay of legal traditions, technological developments, and political priorities. The comparative insights drawn from China demonstrate the necessity of enacting a dedicated and unified Data Protection Act to supplement and enhance the existing legal system.¹¹³² This thesis contends that a genuinely effective unified legislative Act, one that supplements the PIPL, in the manner that the DPA 2018 supplements the UK GDPR, could clearly improve the current data protection framework to some extent. The Act should consolidate the three existing legislative instruments into a single, coherent statutory regime whose provisions are designed from the outset to operate as an integrated system rather than as a collection of historically contingent and imperfectly coordinated laws. This consolidation would require the resolution of the fundamental normative tension that currently pervades Chinese data protection law, between the individual rights orientation of the PIPL and the state security and economic resource orientations of the Cybersecurity and Data Security Laws, in favour of a framework that treats the protection of individual informational autonomy as the primary legislative purpose, to which state security and economic considerations are accommodated as qualified exceptions rather than competing primary objectives. This normative reorientation is the most fundamental and most politically challenging aspect of the proposed reform, because it requires a legislative commitment to treating data subjects as ends in themselves, in the Kantian sense developed in the preceding section, that is in tension with the Chinese state's current conception of the

¹¹³² With the necessity of contextualising data protection within broader legal and political environments.

relationship between individual rights and collective state authority. For example, it is essential to establish accessible and effective mechanisms for individual redress, including a low-cost complaints process, a representative action mechanism for large-scale data protection violations, and a judicial enforcement pathway that is genuinely accessible to ordinary data subjects without the prohibitive costs and procedural barriers that currently render individual enforcement practically impossible in the Chinese legal context.

BIBLIOGRAPHY

BOOKS

- Altman I, *The Environment and Social Behaviour: Privacy, Personal Space, Territory, and Crowding.* Monterey, California (Ed.gov 1975)
- Bell DA, *China's New Confucianism: Politics and Everyday Life in a Changing Society* (Princeton University Press 2010)
- Bernal P, *The Internet, Warts and All: Free Speech, Privacy and Truth* (Cambridge University Press 2018)
- Bradford A, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020)
- Coe P, *Media Freedom in the Age of Citizen Journalism* (Edward Elgar Publishing 2021)
- Fenwick H, Phillipson G and Williams A, *Text, Cases and Materials on Public Law and Human Rights* (Routledge 2017)
- Griffin J, *On Human Rights* (Oxford University Press 2008)
- Hoffman D, *The Impact of the UK Human Rights Act on Private Law* (Cambridge University Press 2011)
- Hustinx P, 'EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation' in *Oxford Scholarship Online* (2017)
- Inness J, *Privacy, Intimacy, and Isolation* (Oxford University Press 1992)
- Kosta E, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, Leiden 2013)
- Lambert P, *The Right to Be Forgotten* (Bloomsbury Professional 2022)
- McStay A, *Privacy and the Media* (SAGE 2017)

- Miller AR, *The Assault on Privacy*, (1970) 15 Law Quadrangle
- Peerenboom R, *China's Long March toward Rule of Law* (Cambridge University Press 2002)
- Rafferty G, *Forecasting Time Series Data with Facebook Prophet* (Packt Publishing - eBooks Account, 2021)
- Repnikova M, 'Restrictions on Critical Journalism' in *Media Politics in China, Improvising Power under Authoritarianism* (Cambridge University Press, 2017)
- Rosa H, *Social Acceleration: A New Theory of Modernity* (Columbia University Press 2013)
- Skinner-Thompson S, *Privacy at the Margins* (Cambridge University Press 2020)
- Solove D, *The Digital Person: Technology and Privacy in the Information Age* (NYU Press 2004)
- Solove D, *Understanding Privacy* (Harvard University Press 2008)
- Van Den and Weckert J, *Information Technology and Moral Philosophy* (Cambridge University Press 2010)
- Viola LA and Laidler P, *Trust and Transparency in an Age of Surveillance* (Routledge 2021)
- Watson A, *Legal Transplants: An Approach to Comparative Law* (1 ed. 1974)
- Westin A, *Privacy and Freedom* (1968) 25 Washington and Lee Law Review 166
- Wragg P, *A Free and Regulated Press* (Bloomsbury Publishing 2020)
- Zuboff S, *The Age of Surveillance Capitalism* (Profile Books 2019)

JOURNAL ARTICLES

- Aidinlis S, 'The Right to Be Forgotten as a Fundamental Right in the UK After Brexit' [2020] 25(2) Communications Law
- Arneson R, 'Egalitarianism' (Stanford Encyclopedia of Philosophy 2013)
- Bechtold E, 'Regulating Online Harms: An Examination of Recent Developments in the UK and the US through a Free Speech Lens' (2024) 16 Journal of Media Law 1
- Belategi MA, 'The Right to Be Forgotten Concerning the Criminal Past: Developments in the Case Law of the European Court of Human Rights with Particular Reference to the Anonymisation of Digital Press Archives' [2024] Oñati Socio-legal Series
- Bellman S and others, 'International Differences in Information Privacy Concerns: A Global Survey of Consumers' (2004) 20 The Information Society 313
- Bennett TDC, 'Triangulating Intrusion in Privacy Law' (2019) 39 Oxford Journal of Legal Studies
- Birnhack MD and Mundlak G, 'The Brussels Effect(s) and the Rise of a Privacy Profession' [2025] International Data Privacy Law
- Bradford A, 'The Brussels Effect' (2012) 107(1) Northwestern University Law Review 1
- Brimblecombe F and Fenwick H, 'Keeping Control of Personal Information in the Digital Age: Efficacy and Equivalence of Tortious and GDPR/DPA Relief?' (2022) 138 Law Quarterly Review 456
- Brimblecombe F and Fenwick H, 'Protecting Private Information in the Digital Era: Making the Most Effective Use of the Availability of the Actions under the GDPR/DPA and the Tort of Misuse of Private Information' (2022) 73 Northern Ireland Legal Quarterly 26

- Brimblecombe F and Phillipson G, 'Regaining Digital Privacy? The New 'Right to Be Forgotten' and Online Expression' (2018) 4 Canadian journal of comparative and contemporary law
- Bu-Pasha S, 'Cross-Border Issues under EU Data Protection Law with Regards to Personal Data Protection' (2017) 26 Information & Communications Technology Law 217
- Busuttil G and McCafferty P, 'Interim Injunctions and the Overlap between Privacy and Libel' (2010) 2 Journal of Media Law 1
- Butler OM, 'Confidentiality and Intrusion: Building Storm Defences Rather than Trying to Hold Back the Tide' (2016) 75 The Cambridge Law Journal 452
- Calzada I, 'Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)' (2022) 5 Smart Cities 1129
- Cao J, "Protecting the Right to Privacy in China" [2005] 36(3) Victoria University of Wellington Law Review 645
- Chawki M, Basu S and Choi K-S, 'Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety' (2024) 13 Laws 33
- Chen ZT and Cheung M, 'Privacy Perception and Protection on Chinese Social Media: A Case Study of WeChat' (2018) 20 Ethics and Information Technology 279
- Choromidou A, 'EU Data Protection under the TCA: The UK Adequacy Decision and the Twin GDPRs' (2021) 11 International Data Privacy Law 390
- Coe P, 'Tackling Online False Information in the United Kingdom: The Online Safety Act 2023 and Its Disconnection from Free Speech Law and Theory' (2023) 15 Journal of Media Law 1
- Craig R and Phillipson G, 'Privacy, Reputation and Anonymity until Charge: ZXC Goes to the Supreme Court' (2021) 13 Journal of Media Law 153

- Crain M, 'The Limits of Transparency: Data Brokers and Commodification' (2016) 20 New Media & Society 88
- Creemers R, 'The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy' (2023) 33 Journal of Contemporary China 1
- Creemers R, 'China's Emerging Data Protection Framework' (2022) 8 Journal of Cybersecurity
- Custers B and others, 'A Comparison of Data Protection Legislation and Policies across the EU' (2018) 34 Computer Law & Security Review 238
- de Bruin R, A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence, (2022) 13 UC LAW SF SCI. & TECH. JUST. L.J. 127
- de Terwangne C, 'Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data' (2021) 40 Computer Law & Security Review 105497
- Dove ES, Chen J, what does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e) (2021) International Data Privacy Law, Volume 11, Issue 2
- Duan Y, China's Private Law Approach to Personal Data Protection (May 26, 2019) SSRN Electronic Journal
- Dworkin G, 'The Younger Committee Report on Privacy' (1973) 36 The Modern Law Review 399
- Erdos D, 'The Development of European Data Protection Law and Regulation' in David Erdos (ed), European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope? (Oxford University Press 2019)

- Erdos D, ‘The UK and the EU Personal Data Framework after Brexit: A New Trade and Cooperation Partnership Grounded in Council of Europe Convention 108+?’ (2022) 44 Computer Law & Security Review 105639
- Erdos D, ‘Assessing UK Data Protection Reform in Transnational Context: What New Direction?’ [2021] University of Cambridge Faculty of Law Research Paper No. 28/2021
- Erdos D, ‘The UK and the EU Personal Data Framework After Brexit: Another Switzerland?’ [2021] University of Cambridge Faculty of Law Research Paper No. 15/2021
- Erdos D, ‘Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government’s Statutory Reform Plans’ [2022] University of Cambridge Faculty of Law Research Paper No. 16/2022
- Erie M and Streinz T, ‘The Beijing Effect: China’s Digital Silk Road as Transnational Data Governance’, (2021) 54 NYU Journal of International Law and Politics
- Fan J and Tang W, ‘China Law Update a Balance Between Social Media Users’ Personal Information Protection and Combating (Mis) And (Dis)Information in China’ (2022) Tsinghua China Law Review
- Farrall KN, Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S., (2008) 2 International Journal of Communication 993
- Feng Y, ‘The Future of China’s Personal Data Protection Law: Challenges and Prospects’ (2019) 27 Asia Pacific Law Review 62
- Fenwick H and Coe P, ‘The Online Safety Act 2023: Fostering Democratic Participation While Combatting Anti-Democratic Harms?’ (2025) 76 Northern Ireland Legal Quarterly 83

- Fenwick H, Reflections on balancing Articles 8 and 10 in the context of MPI - past, present and future (2024) *Journal of Communications and Law*, 29(4)
- Fletcher R and others, ‘The Link between Changing News Use and Trust: Longitudinal Analysis of 46 Countries’ (2024) 75 *Journal of Communication*
- Fried C, ‘Privacy’ (1968) 77:3 *The Yale Law Journal* 475
- Gao RY, ‘A Battle of the Big Three? —Competing Conceptualizations of Personal Data Shaping Transnational Data Flows’ (2023) 22 *Chinese journal of international law* 707
- Geller A, ‘How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective’ (2020) 69 *GRUR International* 1191
- Gerber B, ‘Conceptualizing Privacy’ (2010) 40 *ACM SIGCAS Computers and Society* 8
- Gerber N, Gerber P and Volkamer M, ‘Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behaviour’ (2018) 77 *Computers & Security* 227
- Gerbrandt R-L, ‘Threatening & Protecting Press Publishers and Journalism in the UK’s Regulation of Social Media Platforms’ (2025) 17 *Journal of Media Law* 1
- Gertz R, ‘An Analysis of the Icelandic Supreme Court Judgment on the Health Sector Database Act’, (2004) 1:2 *SCRIPT-ed* 241
- Gil González E and de Hert P, ‘Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and Principles,’ (2019) 19 *ERA Forum* 597
- Greenleaf G, “The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108” (2012) *International Data Privacy Law* 2

- Hallinan D, Friedewald M and McCarthy P, 'Citizens' Perceptions of Data Protection and Privacy in Europe' (2012) 28 Computer Law & Security Review 263
- Hartshorne J, 'The Standard of Liability in Claims for Misuse of Private Information' (2021) 13 Journal of Media Law 216
- He Y, 'On the Construction of Chinese Legislation Path Concerning Data Protection - the Introduction of the Right of Data Portability' [2022] 2021 2nd International Conference on World Economy and Project Management (WEPM 2021)
- Heeks R and others, 'China's Digital Expansion in the Global South: Systematic Literature Review and Future Research Agenda' (2024) 40 The Information Society 1
- Heiss R, Nanz A and Matthes J, 'Social Media Information Literacy: Conceptualization and Associations with Information Overload, News Avoidance and Conspiracy Mentality' (2023) 148 Computers in Human Behavior 107908
- Henschke A, 'Surveillance Technologies and Ethical Vacuums' [2017] Cambridge Core 1
- Hoffman LH and Slater MD, 'Evaluating Public Discourse in Newspaper Opinion Articles: Values-Framing and Integrative Complexity in Substance and Health Policy Issues' (2007) 84 Journalism & Mass Communication Quarterly 58
- Horton G, 'Injunctions and Public Figures: The Changing Value in Injunctions for Privacy Protection' (2021) 13 Journal of Media Law 1
- Horton G, 'Celebrities' families and privacy: the need for enhanced self-regulatory protection. [2022] Communications Law: Journal of Computer, Media and Telecommunications Law, 27 (1)
- Huang J (Jeanne), 'Chinese Private International Law and Online Data Protection' (July 9, 2018). Journal of Private International Law

- Isaak J and Hanna MJ, ‘User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection’ (2018) 51 Computer 56
- Jia M, ‘Authoritarian Privacy’ (2023) 91 SSRN Electronic Journal 753
- Joinson AN and others, ‘Watching Me, Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom’ (2006) 32 Journal of Information Science 334
- Karjalainen T, ‘All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm’ (2022) 8 European Data Protection Law Review 19
- Kierkegaard S and others, ‘30 Years on – The Review of the Council of Europe Data Protection Convention 108’ (2011) 27 Computer Law & Security Review 223
- Koh S, ‘Cancel Culture’ and Criminal Justice, (2022) in 74 Hastings Law Journal 79
- Landi S, Misuse of Private Information: A Legal Analysis of Privacy Precedent in Connection to Media Abuses in England and Wales [2023] the King’s Student Law Review, Vol XIII, Issue II
- Li W and Chen J, ‘From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China’ (2024) 54 Computer law & security report 105994
- Liao S, ‘Gender Trolling: Digital Manosphere and Misogyny in China | GJIA’ (Georgetown Journal of International Affairs 5 May 2025) <<https://gjia.georgetown.edu/2025/05/05/gender-trolling-digital-manosphere-and-misogyny-in-china/>>
- Liebman BL, ‘Ordinary Tort Litigation in China: Law versus Practical Justice?’ (2020) 13(2) Journal of Tort Law

- Löfgren K and Webster CWR, 'Policy Innovation, Convergence and Divergence: Considering the Policy Transfer Regulating Privacy and Data Protection in Three European Countries' (2010) 14 Information Polity 295
- Lynskey O, 'Deconstructing Data Protection: The 'Added-Value' of the Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly
- Lynskey O, 'Complete and Effective Data Protection' (2023) 76 Current Legal Problems 297
- Markin KM, 'Discovering China's Free Expression Values' [2024] Ohio Northern University International Law Journal: Vol. 2
- Mason S, 'Exploring Privacy from a Philosophical Perspective: Conceptual and Normative Dimensions' [2024] Technology, work and globalization 23
- Mattiello H, 'Exposing the Hidden Costs of "Free": Personal Data Commodification in the Digital Economy via X.0 Theory, Fuzzy Delphi, Thematic Analysis, and Problem-Solving Frameworks' (2025) 2 Journal of Policy and Society 2330
- Mazzi F and others, 'The UK GDPR Reform: Missing Data Privacy, Regulatory Probity, and Harm Prevention' [2021] SSRN Electronic Journal
- McCrudden C, 'Human Dignity and Judicial Interpretation of Human Rights' (2008) 19 European Journal of International Law 655
- Michailova S and Hutchings K, "National Cultural Influences on Knowledge Sharing: A Comparison of China and Russia" (2006) Journal of Management Studies 43
- Miao Y, 'Managing Digital Contention in China' [2020] Journal of Cyber Policy 1
- Moore AD, 'Free Speech, Privacy, and Autonomy' (2020) 37 Social Philosophy and Policy 31

- Moosavian R and Coe P, Balancing Privacy Against Free Speech: In Defence of Exposing Hypocrisy (2025) Forthcoming in D. Clifford, M. Richardson, and N. Witzleb, Research Handbook on Privacy and Confidentiality in Media Law (Edward Elgar, 2026)
- Moosavian R, 'Deconstructing 'Public Interest' in the Article 8 vs Article 10 Balancing Exercise' (2014) 6 Journal of Media Law 234
- Moosavian R, Jigsaws and Curiosities: The Unintended Consequences of Misuse of Private Information Injunctions. (2016) Communications Law, 21 (4)
- Moreham NA, 'Privacy, Reputation and Alleged Wrongdoing: Why Police Investigations Should Not Be Regarded as Private' (2019) 11 Journal of Media Law 142
- Moreham NA, Compensating for Loss of Dignity and Autonomy in the Misuse of 'Private Information Tort (December 20, 2017). in 'Remedies for Breach of Privacy' Varuhas & Moreham eds (2018, Hart Publishing), Victoria University of Wellington Legal Research Paper No. 6/2019
- Mulligan DK, Koopman C and Doty N, 'Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy' (2016) 374 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20160118
- Naef T, 'Restrictions on Data Transfers and Trade Agreements' [2022] European Yearbook of International Economic Law 367
- Nyman J, 'Towards a Global Security Studies: What Can Looking at China Tell Us about the Concept of Security?' (2023) 29 European Journal of International Relations 673
- Pang X, 'Civil Law Protection of Personal Information in the Era of Big Data' (2021) 08 OALib 1

- Pernot-Leplay E, China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.? 2020, 8 PENN. ST. J.L. & INT'L AFF. 49
- Peukert C and others, 'Regulatory Spillovers and Data Governance: Evidence from the GDPR' (2022) 41 Marketing Science 746
- Phillipson G, 'Max Mosley goes to Strasbourg: Article 8 Notification and Interim Injunctions' (2009)1(1) Journal of Media Law 73
- Phillipson G, 'Clarity Postponed: Horizontal Effect after Campbell' [2007] In H. Fenwick, G. Phillipson, & R. Masterman (Eds.), Judicial reasoning under the UK Human Rights Act (143-173). Cambridge University Press
- Phillipson G, 'Privacy: The Development of Breach of Confidence – the Clearest Case of Horizontal Effect?' [2011] In: Hoffman D, ed. The Impact of the UK Human Rights Act on Private Law, Cambridge University Press eBooks 136
- Phillipson G, 'Supreme Court Confirms Suspects' Privacy Rights: The Judgment Clarified, Two Criticisms Answered' (2022) 14 Journal of Media Law 1
- Phillipson G and Fenwick H, 'Breach of Confidence as a Privacy Remedy in the Human Rights Act Era' (2000) 63 Modern Law Review 660
- Pleger LE, Guirguis K and Mertes A, 'Making Public Concerns Tangible: An Empirical Study of German and UK Citizens' Perception of Data Protection and Data Security' (2021) 122 Computers in Human Behavior 106830
- Powell F and Needleman S, 'How Radical an Instrument Is Section 3 of the Human Rights Act 1998?' (UK Constitutional Law Association 24 March 2021)
- Pyo G, 'An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts' (2021) 60 Colum J Transnat'l L 228
- Raab C and Goold B, 'Protecting Information Privacy' (2011)

- Reiman JH, 'Privacy, Intimacy, and Personhood' (1976) 6 *Philosophy & Public Affairs* 26
- Reis O and others, 'Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement' (2024) 6 *International Journal of Applied Research in Social Sciences* 73
- Rowbottom JH, 'Power and the Public Eye: Why the Limits of Acceptable Criticism Are Wider for Public Figures' [2025] *Public Law Sweet & Maxwell* 1
- Rucz M, 'SLAPPED by the GDPR: Protecting Public Interest Journalism in the Face of GDPR-Based Strategic Litigation against Public Participation' (2022) 14 *Journal of Media Law*
- Sage N, *Relational Wrongs and Agency in Tort Theory*, *Oxford Journal of Legal Studies*, [2021] Volume 41, Issue 4
- Satra HS, 'Privacy as an Aggregate Public Good' (2020) 63 *Technology in Society* 101422
- Schade F, 'Dark Sides of Data Transparency: Organized Immaturity after GDPR?' [2023] *Business Ethics Quarterly* 1
- Schaub F, Konings B and Weber M, 'Context-Adaptive Privacy: Leveraging Context Awareness to Support Privacy Decision Making' (2015) 14 *IEEE Pervasive Computing* 34
- Seipp DJ, 'English Judicial Recognition of a Right to Privacy' (1983) 3 *Oxford Journal of Legal Studies* 325
- Shao Y, 'Personal Information Protection: China's Path Choice' (2021) 18 *US-China Law Review*
- Solove DJ, 'A Taxonomy of Privacy' (2006) *University of Pennsylvania Law Review* 477

- Solove DJ, ‘The Myth of the Privacy Paradox the Myth of the Privacy Paradox’ (2021) 89 George Washington Law Review 1
- Solove DJ, ‘Why is Privacy Important?’, On Privacy and Technology (New York, NY, 2025; online edn, Oxford Academic, 3 Jan. 2025)
- Stone GR, ‘Privacy, the First Amendment, and the Internet’ in Saul Levmore & Martha Nussbaum, eds, *The Offensive Internet: Speech, Privacy, and Reputation* (Harvard University Press 2010)
- Taddicken M, ‘The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure’ (2013) 19 *Journal of Computer-Mediated Communication* 249
- Townend J, ‘Data Protection and the ‘Right to Be Forgotten’ in Practice: A UK Perspective’ (2017) 45 *International Journal of Legal Information* 28
- Tzanou M, ‘Data Protection as a Fundamental Right next to Privacy? “Reconstructing” a Not so New Right’ (2013) 3 *International Data Privacy Law* 89
- van Ooijen I and Vrabec HU, ‘Does the GDPR Enhance Consumers’ Control over Personal Data? An Analysis from a Behavioural Perspective’ (2018) 42 *Journal of Consumer Policy* 91
- Walgate R, ‘Data Protection Laws: UK Lags Behind’ (1981) 289 *Nature* 527
- Wang H and Yuan L, ‘State, Platform, and Misogynistic Disinformation in China’ (2023) 8 *Global Media and China*
- Warren AR and Dearnley J, ‘Data Protection Legislation in the United Kingdom’ (2005) 8 *Information, Communication & Society* 238
- Warren SD and Brandeis LD, ‘The Right to Privacy’ (1890) 4 *Harvard Law Review* 193

- Wong R and Savirimuthu J, 'All or Nothing: This Is the Question? The Application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet', (2007) Forthcoming John Marshall Journal of Computer and Information Law 2007/8
- Wragg P, 'A Freedom to Criticise? Evaluating the Public Interest in Celebrity Gossip after Mosley and Terry' (2010) 2 Journal of Media Law 295
- Wragg P, 'Protecting Private Information of Public Interest: Campbell's Great Promise, Unfulfilled' (2015) 7 Journal of Media Law 225
- Wragg P, 'Recognising A Privacy-Invasion Tort: The Conceptual Unity of Informational and Intrusion Claims' (2019) 78 The Cambridge Law Journal 409
- Ye X and others, 'Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective' (2024) 48 Telecommunications Policy 102851
- Youma KH and Park A, 'The Right to Be Forgotten: Google Spain as a Benchmark for Free Speech versus Privacy?' (Chicago Journal of International Law 2023)
- Zhang C, 'China's Privacy Protection Strategy and Its Geopolitical Implications' (2024) 3 Asian Review of Political Economy
- Zhang K and Schmidt A, 'Looking at China's Facebook (RenRen) through the Lens of European Data Protection Principles' [2013] SSRN Electronic Journal
- Zhang L, 'Personal Information of Privacy Nature' under Chinese Civil Code' (2021) 43 Computer Law & Security Review 105637
- Zhang Y and Liu Z, 'The Rise of the Chinese Judiciary and Its Limits: Administrative Litigation in the Reform Period' [2024] SSRN Electronic Journal

WEBSITES AND BLOGS

- Aleksandr, 'GDPR in the USA: GDPR Compliance in US: GDPR and Pii' (Cookiebot) July 7, 2020
- Amnesty International, 'Everything You Need to Know about Human Rights in China 2020' (Amnesty International 2023)
- Barker D, 'Misuse of Private Information' (Pinsent Masons 9 May 2023)
- Bollinger D and others, 'Automating Cookie Consent and GDPR Violation Detection Automating Cookie Consent and GDPR Violation Detection' (2022)
- Breese R, 'Insurers Are Critical to Protecting Investigative Journalism' (Tmhcc.com 2024)
- Bullard E, 'Right to Be Forgotten: Overview | EBSCO' (EBSCO Information Services, Inc. | www.ebsco.com 2024)
- Cathcart B, 'Three Key Reasons Why the Royal Charter Is Better for Journalists than IPSO - Hacked Off' (Hacked Off - A Campaign for a Free and Accountable Press 13 August 2014)
- Chinneide HN, '*Hurbain v Belgium*: Navigating the Intersection of Privacy and Press Freedom in the Digital Age - Strasbourg Observers' (Strasbourg Observers 3 October 2023)
- De Freitas I and Matthews A, 'Ruling Threatens to Extend the Extra-Territorial Reach of GDPR' (Farrer & Co January 1, 1970)
- Dixon P, 'A Brief Introduction to Fair Information Practices | World Privacy Forum' (World privacy forum.org September 2012)
- Docksey C, 'Journalism on Trial and the Right to Be Forgotten' [2022] Verfassungsblog

- Erdos D, ‘The UK Information Commissioner’s Annual Report 2024/25: Surveying a Systematic Trend Away from Adequate Enforcement’, U.K. Const. L. Blog (22nd July 2025) (available at <https://ukconstitutionallaw.org/>)
- The Economist, ‘The World’s Most Valuable Resource Is No Longer Oil, but Data’ (The Economist 6 May 2017)
- Flynn B, Parnell G and Maurice C, ‘An Overview of the UK’s Data Privacy Regime’ (Stevens & Bolton LLP)
- Gallop B, Walker-Parr L of 5RB and Bishop D, ‘Privacy Law-Misuse of Private Information Produced in Partnership (2021), 5RB
- Gearty C, ‘Conor Gearty: Max Mosley in Strasbourg’ (UK Constitutional Law Association 16 May 2011)
- Grant P, ‘Strategic Communication Laboratories and the Mysterious Origins of Cambridge Analytica’ (Medium 12 September 2023)
- Grisaffe G, ‘English Court of Appeal Rules on Compensation for Data Breaches - Cyber/Data/Privacy Insights’ (cyber/data/privacy insights4 September 2025) <<https://cdp.cooley.com/english-court-of-appeal-rules-on-compensation-for-data-breaches/>> accessed 9 February 2026
- Heer S de, ‘*Hurbain v. Belgium*: Towards a Fairer Balancing Exercise between the Right to Freedom of Expression and the Right to Privacy?’ (Strasbourg Observers 26 November 2021)
- Henderson K and Askew A, ‘Case Comment: *Lloyd v Google LLC* [2021] UKSC 50’ (UKSC Blog 31 January 2022)
- Hussain A, ‘Privacy, Celebrities and the Media’ (Legal Cheek 12 November 2019)
- ICO, ‘Information Commissioner’s Office’ (Ico.org.uk21 March 2024) <<https://ico.org.uk/>>

- IMPRESS, The Independent Monitor of the Press (Impress)
<<https://www.impressorg.com/>>
- IPSO, 'Home' (Ipsos.co.uk 2019) <<https://www.ipsos.co.uk/>>
- Kingsley-Hughes A, 'Why Apple's Disabling of iCloud Encryption in the UK Is Bad News for Everyone' (ZDNET 25 February 2025)
- Kouvakas I, 'You Can't Have Your Apple and Eat It Too: Decryption Orders and the Perilous Future of U.K. Data Adequacy', U.K. Const. L. Blog (13th March 2025) (available at <https://ukconstitutionallaw.org/>)
- Kowalski J, Data (Use and Access) Bill: Third time lucky for UK data protection reform? (2024) DAC Beachcroft LLP
- Laney DB, 'GDPR Violations and Fines: Trends, Insights, and Compliance Strategies' (Forbes 12 June 2024)
- Laufer B & Nissenbaum H, 'Algorithmic Displacement of Social Trust' (Knightcolumbia.org 2015)
- Lenin V, 'Once Again on the Trade Unions' (Marxists.org 2025)
- Lomas N, 'UK pauses data reform bill to rethink how to replace GDPR', TechCrunch 4 October 2022
- Marriage M, 'Men Only: Inside the Charity Fundraiser Where Hostesses Are Put on Show' (Financial Times 23 January 2018)
- McMahon F, 'Supreme Court Refuses Permission in DPA/Libel Claim - 5RB Barristers' (5RB Barristers 31 July 2017)
- Media Defence, 'European Court of Human Rights Issues Judgment in *Hurbain v Belgium*, Expanding the Application of the "Right to Be Forgotten" - Media Defence' (Media Defence 14 July 2023)

- Moynihan H and Patel C, ‘Restrictions on Online Freedom of Expression in China the Domestic, Regional and International Implications of China’s Policies and Practices International Law Programme Asia-Pacific Programme’ (2021)
- Mulhern H, ‘Can an Individual Get a GDPR Fine?’ (Measured Collective 13 June 2021)
- Murphy W, ‘Suffering, Damage, the GDPR – and All That | Cornerstone Barristers’ (Cornerstone Barristers 5 May 2023)
- Nuthi K and Tesfazgi M, ‘Reforming the UK Online Safety Bill to Protect Legal Free Expression and Anonymity’ (Itif.org 29 August 2022)
- OECD, ‘About the OECD’ (OECD2023) <<https://www.oecd.org/en.html>>
- Rawlinson J, ‘Driver v CPS – Damages in Data Breach Claims – an Imprecise Science? - 4 Pump Court - Barristers’ Chambers’ (4 Pump Court 19 October 2022)
- Sahin K, ‘The West, China, and AI Surveillance’ (Atlantic Council 18 December 2020)
- Sharma S, ‘Case Law: GYH v Persons Unknown, Interim Injunction to Restrain Campaign of Vilification – Suneet Sharma’ (Inform’s Blog 17 January 2018)
- Sixth Tone, ‘Are Chinese People ‘Less Sensitive’ about Privacy?’ (#SixthTone March 2018)
- Sixth Tone, ‘A Deadly Fire Killed His Family. Now He’s Being Scorned Online.’ (#SixthTone July 2021)
- Tomlinson H, ‘*Hurbain v Belgium*, Grand Chamber upholds decision that order anonymising newspaper archive did not violate Article 10’ (26 July 2023) INFORMBlog
- Webber AA, ‘Staff Who Leaked Late HK Actress Kathy Chow’s Medical Report to “Show Off” Gets Arrested’ (The Star 14 December 2023)
- Wilson B, ‘Celebrity Blackmail Victim Obtains Injunction Restraining Publication of Allegation of Serious Criminality - Brett Wilson’ (Brett Wilson 13 December 2017)

- Woods L, “‘You Were Only Supposed to Blow the Bloody Doors Off!’: Schrems II and External Transfers of Personal Data’ (Blogspot.com16July2020) <<https://eulawanalysis.blogspot.com/2020/07/you-were-only-supposed-to-blow-bloody.html>> accessed 8 March 2026
- Yan M, ‘Beijing Police Detain Man Responsible for Leaking Personal Medical Records’ (Chinadaily.com.cn 2023)
- Luo Y, ‘Analysing China’s PIPL and How It Compares to the EU’s GDPR’ (Inside Privacy 25 August 2021)

ONLINE REPORTS AND OFFICIAL PUBLICATIONS

- Backhouse, James, and Ruth Halperin, ‘A Survey on EU Citizen’s Trust in ID Systems and Authorities’, FIDIS Deliverable 4.4, London School of Economics and Political Science, London, 2007
- China Internet Network Information Centre (CNNIC), ‘The 54th Statistical Report on China’s Internet Development’ (2024)
- Communications and Digital Committee, Free for all? freedom of expression in the Digital age (2021) the Authority of the House of Lords, 1st Report of Session 2021–22
- CMS, Law GDPR Enforcement Tracker 2024
- DLA Piper, ‘Data Protection Laws in the United Kingdom - Data Protection Laws of the World’ (Dlapiperdataprotection.com2024)
- European Union Agency for Fundamental Rights., Your Rights Matter: Data Protection and Privacy: Fundamental Rights Survey (Publications Office 2020)
- ICM, ‘State of the Nation Survey 2010’, Joseph Rowntree Foundation, York, 2010

- ICO, Data Protection and Journalism Code of Practice, data-protection-and-journalism-code-202307.pdf
- Information Commissioner's Office, Response to DCMS consultation 'Data: a new direction' (6 October 2021)
- Information Commissioner, Annual Report and Financial Statements 2023-24 (2024)
- Lords Hansard, 'House of Lords - Hansard - UK Parliament' (Parliament.uk2026) <<https://hansard.parliament.uk/lords/2026-03-19>>
- Niestadt M and Reichert J, The global reach of the EU's approach to digital transformation, 2024 EPRS European Parliamentary Research Service
- Ofcom, 'News Consumption in the UK: 2024 Research Findings' (Ofcom 2024)
- Prinsley M and Yaros O, 'UK ICO Imposes a £250,000 Penalty for a Security Breach Which Exposed the Personal Data of Millions of Consumers' (2013) <<https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2013/01/uk-ico-imposes-a-250000-penalty-for-a-security-bre/files/130129-ip-sony/fileattachment/130129-ip-sony.pdf>> accessed 16 September 2025
- Privacy (Younger Report) HC Deb 13 July 1973 vol 859 cc1955-2058

CHINESE LANGUAGE SOURCES

- Chen X, Personal Information Protection and Improvement of Information Disclosure System for Network Service Providers. Journal of South-Central Minzu University (Humanities and Social Sciences) 40, 1 (2020)

- Cheng X, 'On the Relationship Between the Civil Code and the Personal Information Protection Law' (2022) 3 Science of Law (Journal of Northwest University of Political Science and Law)
- Li W, 'Privacy Protection and the Right to Be Forgotten in the Era of Big Data' (2015) 30(2) Graduate Law Review (CUPL)
- Li X, 'Research on the Establishment of the Right to Be Forgotten in China under the Background of GDPR Implementation' (Ccssn.cn, 2018)
- Shen W, 'On the Construction and Systematization of Personal Information Rights' (2021) 5 Journal of Comparative Law
- Shi J, 'How to Connect and Coordinate the Personal Information Protection Law and the Civil Code' (2021) 2 People's Forum
- Shi J, 'The Private Law Dimension of Personal Information Protection: On the Relationship between Civil Code and Personal Information Protection Law' (2021) 5 Journal of Comparative Law
- Sun X, 'Recommendations for Amendments to the Draft Personal Information Protection Law (Ccssn.cn, 2020)
- Wang L, 'Harmony in Diversity: The Rule Differentiation and Application of Privacy Rights and Personal Information' (2021) 2 Law Review
- Wang Z and Lei Y, 'The Boundaries and Reexamination of the 'Right to Be Forgotten' in social media' (2024) 5 Southeast Communication
- Yang L and Du Z, 'Commentary on the Judicial Reasoning in China's First Case on the 'Right to Be Forgotten': *Ren Jiayu v Baidu Company Reputation Dispute*' (2017) 16 Application of Law: Judicial Cases
- Yang L and Han X, 'Localisation and Legal Application of the Right to Be Forgotten in China' (2015) 2 Journal of Law Application

- Zhang W and Liu Y, 'On the News Exception in Personal Information Protection' (2024) 1 Human Rights CN
- Zhang X, 'On the Exercise of the Right to Request Protection of Personal Information' (2023) 2 Tribune of Political Science and Law 29
- Zhou H, 'The Legal Positioning of Personal Information Protection' (2020) 3 Studies in Law and Business
- Zhu W, 'The 'Right to Be Forgotten' Forgotten in the Era of Big Data' (China Social Sciences Network, 2014)