

Serge Gutwirth • Yves Poullet • Paul De Hert
(Editors)

Data Protection in a Profiled World

Springer

Contents

Part I	Generic Issues.....	1
1	About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?.....	3
	<i>Yves Poullel</i>	
1.1	Is Personal Data the Adequate Concept?.....	9
1.1.1	New Kinds of Sensitive Data in Our Modern Networks: Identifiers and Contact Data.....	11
1.1.2	IP Address, Cookies, Data Generated by RFID, Always "Personal Data"? Why Regulate Them Anyway?.....	13
1.1.3	New Data to be Protected: The Profiles.....	16
1.2	New Objects and New Actors to be Regulated?.....	18
1.2.1	EU Commission's Support to PETS.....	20
1.2.2	Towards a Liability of Terminal Equipments Producers and Information System Designers: The RFID Case.....	21
1.2.3	Terminal Equipment as a Virtual Home?.....	23
1.2.4	Conclusions of Sect. 1.2.....	27
1.3	Final Conclusions.....	28
2	Some Caveats on Profiling.....	31
	<i>Serge Gutwirth and Mireille Hildebrandt</i>	
2.1	Introduction.....	31
2.2	What Is It with Profiling?.....	31
2.3	From Measurement to Detection.....	32
2.4	A Risky Dependence.....	33
2.5	Privacy, Fairness (Non-discrimination) and Due Process.....	34
2.6	Causality and (Criminal) Liability.....	35
2.7	Who Owns My Data; Who Authors the Profiles I Match with?.....	35
2.8	Transparency and Anticipation.....	36
2.9	Privacy and Data Protection.....	36
2.10	From Data Minimisation to Minimal Knowledge Asymmetries?.....	38

2.11 Am Law: From Privacy Enhancing Technologies to Transparency Enhancing Tools?.....	39
2.12 Call for Attention.....	39
References.....	40
3 Levelling up: Data Privacy and the European Court of Human Rights.....	43
<i>Gordon Nardell QC</i>	
3.1 The Background.....	43
3.2 Legality, Necessity, Secrecy.....	46
3.3 Legality: The Liberty Case.....	47
3.4 Necessity and Proportionality: The S. and Marper Case.....	49
3.5 Where Does It Leave Us?.....	51
4 Responding to the Inevitable Outcomes of Profiling: Recent Lessons from Consumer Financial Markets, and Beyond.....	53
<i>Tal Zarsky</i>	
4.1 Preface.....	53
4.2 Rethinking the Regulation of Profiling: In a Nutshell.....	55
4.2.1 A Brief Introduction to the Flow of Personal Information.	55
4.2.2 The Limits and Troubles of Regulating Data Collection.	57
4.2.3 The Limits and Troubles of Regulating Data Analysis.	57
4.2.4 Regulating Profiling by Addressing Uses: Possibilities, Factors and Limits.....	58
4.3 A Tale of Four Data Miners.....	61
4.4 Some Conclusions and Summing Up.....	72
References.....	73
Part II Specific Issues: Security Breaches, Unsolicited Adjustments, Facebook, Surveillance and Electronic Voting.	75
5 The Emerging European Union Security Breach Legal Framework: The 2002/58 ePrivacy Directive and Beyond.....	77
<i>Rosa Barcelo and Peter Tranng</i>	
5.1 Introduction.....	78
5.1.1 The EU Security Breach Legal Framework: The Background.....	78
5.1.2 The Review of the ePrivacy Directive.....	79
5.1.3 An Overview of the Security Breach Framework Under the Revised ePrivacy Directive.....	80
5.2 Purposes and Existing Data Protection Principles Underpinning the New EU Security Breach Framework.....	81
5.2.1 Preventing and Minimising Adverse Effects for Individuals ...	81
5.2.2 The Security Principle.....	82
5.2.3 The Data Minimisation Principle.....	84
5.2.4 The Information Principle.....	84

5.2.5	The Accountability Principle.....	85
5.3	Elements of the EU Security Breach Notification Framework.....	86
5.4	Scope of the EU Security Breach Notification Framework.....	86
5.4.1	Entities Obligated to Notify: Covered Entities.....	86
5.4.2	The Application to Information Society Services and Beyond.....	87
5.4.3	Definition of 'Personal Data Breach'.....	89
5.5	The Threshold Triggering the Obligation to Notify.....	90
5.5.1	Description of the Threshold.....	90
5.5.2	"Likely to Adversely Affect the Personal Data and Privacy" ...	92
5.5.3	Exceptions Relating to Technological Protection Measures and Law Enforcement.....	93
5.6	Means of Providing Notice, Timing and Content.....	95
5.6.1	Means of Providing Notice.....	95
5.6.2	Timing of the Notification.....	96
5.6.3	Content of the Notification.....	97
5.7	Enforcement of the Provisions.....	98
5.7.1	Audit and Other Tools Available to the Authorities.....	98
5.7.2	Selective to be Effective.....	99
5.7.3	Damages.....	100
5.8	The Next Steps.....	100
5.8.1	Technical Implementing Measures Through Comitology.....	100
5.8.2	Areas/Subjects Covered by Comitology.....	101
5.8.3	Towards the Application of a Security Breach Notification Scheme Across Sectors.....	102
5.9	Conclusions.....	104
6	From Unsolicited Communications to Unsolicited Adjustments	105
	<i>Gloria Gonzalez Fuster, Serge Gutwirth and Paul de Hert</i>	
6.1	Protecting the Individual in front of Technology.....	105
6.2	The Regulation of Unsolicited Communications.....	107
6.3	The Shift Towards Unsolicited Adjustments.....	110
6.3.1	Upcoming Practices.....	111
6.3.2	Present Problematic Practices.....	112
6.3.3	The (Other) Limits of Current Legislation.....	114
6.4	Concluding Remarks.....	115
	References.....	116
7	Facebook and Risks of "De-contextualization" of Information	119
	<i>Franck Dumortier</i>	
7.1	Introduction.....	119
7.2	The Risks of De-contextualization Deriving from Interactions on Facebook.....	121
7.2.1	The Simplification of Social Relations on OSNS.....	122
7.2.2	The Large Information Dissemination Implied by Interactions on Facebook.....	123

7.2.3	The Globalization and Normalization Effects of Facebook ...	126
7.3	Consequences of the Threat of De-contextualization on the Rights to Privacy and to Data Protection.....	127
7.3.1	Consequences of the Threat of De-contextualization on Privacy as a Right of the Human Being	128
7.3.2	Consequences of the Threat of De-contextualization on Data Protection as a Right of Data Subjects.....	132
7.4	Conclusion.....	135
8	Surveillance in Germany: Strategies and Counterstrategies	139
	<i>Gerrit Hornung, Ralf Bendrath and Andreas Pfitzmann</i>	
8.1	Introduction.....	139
8.2	The Online Searching Judgement of February 27th, 2008	140
8.2.1	Background of the Case.....	140
8.2.2	Other Fundamental Rights.....	141
8.2.3	Content of the "New" Fundamental Right	142
8.2.4	Interferences.....	143
8.2.5	Further Developments.....	143
8.3	The German Federal Constitutional Court: Closer to ICT and Technology Assessment than German Politicians.....	144
8.3.1	Actors and Their Knowledge.....	144
8.3.2	Strategies Working Against Privacy and Appropriate Counterstrategies Working Towards Privacy.....	147
8.3.3	Summing up: Government vs. Court.....	148
8.4	The Rise of the Anti-Surveillance Movement 2.0.....	148
8.4.1	Data Retention and the Participatory Resistance Against Surveillance.....	149
8.4.2	From the Internet to the Streets and into Pop Culture	151
8.4.3	Putting Privacy on the Political Agenda.....	152
8.4.4	Lessons Learned.....	154
	References.....	155
9	Verifiability of Electronic Voting: Between Confidence and Trust	157
	<i>Wolter Pieters</i>	
9.1	Introduction.....	157
9.2	Trust.....	158
9.2.1	Good and Bad Trust.....	158
9.2.2	Confidence and Trust.....	159
9.2.3	Trust in E-voting.....	161
9.3	Verifiability.....	163
9.3.1	Voter-Verifiable Elections.....	163
9.3.2	Verifiability and Receipt-Freeness.....	165
9.3.3	Variants of Verifiability.....	166
9.4	Verifiability and Trust.....	168
9.4.1	The Politics of Voting Technology.....	169
9.4.2	What Proof Do We Prefer?.....	169

9.4.3	Beyond Electronic Voting	171
9.5	Conclusions.....	173
	References.....	174
10	Electronic Voting in Germany.....	177
	<i>Melanie Volkamer</i>	
10.1	Introduction.....	177
10.2	Approaches Applied in Germany.....	178
10.2.1	Mechanical Voting Machines.....	178
10.2.2	Direct Recording Electronic (DRE) Voting Computers ...	179
10.2.3	Paper-Based Electronic Voting Systems.....	180
10.2.4	Internet Voting Systems.....	183
10.3	Requirement Documents.....	184
10.3.1	German Federal Ordinance for Voting Machines.....	184
10.3.2	Protection Profile for the Digital Voting Pen.....	184
10.3.3	Online-Voting System Requirements for Non- parliamentary Elections.....	185
10.3.4	Catalogue of the German Society of Computer Scientists ...	185
10.3.5	GI/BSI/DFKI Protection Profile.....	185
10.4	Activists'Activities.....	186
10.5	The Federal Constitutional Court Judgment.....	186
10.6	Future of Electronic Voting in Germany.....	187
	References.....	188
Part III	Third Pillar Issues.....	191
11	The New Council Decision Strengthening the Role of Eurojust: Does It also Strengthen Data Protection at Eurojust?.....	193
	<i>Diana Alonso Blas</i>	
11.1	Introduction.....	193
11.2	Amendments with Data Protection Relevance.....	195
11.2.1	Preservation of the Specificity of the Eurojust Data Protection Regime.....	195
11.2.2	Clear Definition of National Competences.....	196
11.2.3	Extension of the Categories of Personal Data which Eurojust may Legally Process.....	196
11.2.4	Improvement of the Information Provision from Member States.....	198
11.2.5	CMS-Related Issues and Secure Communication with Member States.....	200
11.2.6	Time Limits.....	203
11.2.7	Relations with Third Parties.....	205
11.2.8	EU Classified Information.....	208
11.3	Amendments with Relevance to the Joint Supervisory Body of Eurojust (JSB).....	208
11.4	Concluding Remarks.....	210

12	The Case of the 2008 German-US Agreement on Data Exchange: An Opportunity to Reshape Power Relations?	211
	<i>Rocco Bellanova</i>	
12.1	Introduction.....	211
12.2	Towards a "Prum Model"?......	212
12.3	Context: Transitional Periods?.....	213
12.4	Contents and Core Provisions. Which Core? Which Provisions?	215
12.5	Memberships and Actors.....	216
12.6	Divergences Among Provisions of Prum Instruments	218
12.7	Resistance to the "Prum Model"?......	220
12.8	Final Considerations.....	222
	References.....	223
13	DNA Data Exchange: Germany Flexed Its Muscle	227
	<i>Sylvia Kierkegaard</i>	
13.1	Introduction.....	227
13.2	Background.....	228
13.3	Substantive Law.....	232
13.4	German Hegemony & Democratic Deficit.....	233
13.5	Innocent 'Lambs for Slaughter'.....	236
13.6	Data Protection.....	238
13.7	Conclusion.....	240
	References.....	241
Part IV	Technology Assessment Views	245
14	Information Privacy in Europe from a TA Perspective	247
	<i>Walter Peissl</i>	
14.1	Introduction.....	247
14.2	About EPTA.....	248
14.3	ICT and Privacy in Europe: The First Common EPTA Project	249
	14.3.1 Methodology of the Project.....	250
	14.3.2 Outcome.....	251
	14.3.3 Some Findings.....	252
	14.3.4 The Challenges: and How to Deal with Them.....	253
	References.....	254
15	Privacy and Security: A Brief Synopsis of the Results of the European TA-Project PRISE	257
	<i>Johann Cas</i>	
15.1	Introduction.....	257
15.2	Background and Objectives of PRISE.....	258
15.3	Project Methods.....	259

15.4	Results of the Interview Meetings	_____260
15.5	Criteria for Privacy Enhancing Security Technologies.....	260
15.6	Next Steps and Continuitive Recommendations.....	261
	References.....	262
Part V Legal Practitioner's Views.....		263
16	The Role of Private Lawyers in the Data Protection World.....	265
	<i>Christopher Kuner</i>	
16.1	The Roles of Data Protection Lawyers.....	265
16.1.1	Legal Practice.....	265
16.1.2	Speaking, Writing, and Other Pro Bono Activities.....	267
16.2	The Challenges of Practicing Data Protection Law.....	267
16.3	Outlook for Data Protection Law Practice.....	268
16.4	Conclusions.....	269
17	Transfer and Monitoring: Two Key Words in the Current Data Protection Private Practice: A Legal Practitioner's View.....	271
	<i>Tanguy Van Overstraeten, Sylvie Rousseau and Guillaume Couneson</i>	
17J	Introduction.....	271
17.2	International Data Flows: The Issue of Transfer.....	272
17.2.1	Unambiguous Consent: A Subsidiary Solution?.....	273
17.2.2	Standard Contractual Clauses: A Solution to be Further Harmonised.....	274
17.2.3	Binding Corporate Rules: The Way Forward.....	275
17.2.4	No One Size Fits-All Solution to the Data Transfer.....	277
17.3	Big Brother Is Watching You: the Issue of Monitoring.....	277
17.3.1	Monitoring by Private Companies.....	278
17.3.2	Monitoring by Public Authorities.....	283
17.3.3	Monitoring by Individuals.....	285
17.4	Conclusion.....	285
Part VI Technologist's Views.....		287
18	Architecture Is Politics: Security and Privacy Issues in Transport and Beyond.....	289
	<i>Bart Jacobs</i>	
18.1	Architectural Issues.....	289
18.2	What Went Wrong: Smart Cards in Public Transport.....	291
18.3	What Can Still Go Right: Road Pricing.....	295
18.4	Privacy and Trust for Business.....	297
	References.....	298

19	PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm	301
	<i>Seda Gürses and Bettina Berendt</i>	
19.1	Introduction.....	301
19.2	Privacy as Data Confidentiality and Anonymity.....	303
19.2.1	Personal Data as the Focus of PETs.....	303
19.2.2	Anonymity as a Privacy Enhancing Mechanism.....	305
19.2.3	Anonymity and Confidentiality in the Internet: Assumptions of PETs.....	306
19.3	Surveillance Society and Its Effects on PETs.....	308
19.3.1	The Daily Perspective on Surveillance.....	308
19.3.2	The Marketing Perspective on Surveillance.....	309
19.3.3	The Political Perspective on Surveillance.....	309
19.3.4	The Performative Perspective on Surveillance.....	310
19.4	The Information Perspective on Surveillance.....	311
19.5	Revisiting the Assumptions.....	313
19.6	Conclusion.....	316
	References.....	319
20	Privacy by Design: A Matter of Choice	323
	<i>Daniel Le Métayer</i>	
20.1	Introduction.....	323
20.2	What Do We Mean by Privacy by Design?.....	323
20.3	A Matter of Choice.....	326
20.4	From a Vicious Cycle to a Virtuous Cycle.....	328
20.4.1	Lawyers and Legislators.....	329
20.4.2	Computer Scientists.....	331
20.4.3	A Virtuous Cycle.....	332
	References.....	332