

PRIVACY ONLINE, LAW AND THE EFFECTIVE REGULATION
OF ONLINE SERVICES

PRIVACY ONLINE, LAW AND
THE EFFECTIVE REGULATION
OF ONLINE SERVICES

Marcin BETKIER



intersentia

Cambridge – Antwerp – Chicago

Intersentia Ltd
8 Wellington Mews
Wellington Street | Cambridge
CB1 1HW | United Kingdom
Tel.: +44 1223 736 170
Email: mail@intersentia.co.uk
www.intersentia.com | www.intersentia.co.uk

Distribution for the UK and Ireland:

NBN International
Airport Business Centre, 10 Thornbury Road
Plymouth, PL6 7PP
United Kingdom
Tel.: +44 1752 202 301 | Fax: +44 1752 202 331
Email: orders@nbninternational.com

Distribution for Europe and all other countries:

Intersentia Publishing nv
Groenstraat 31
2640 Mortsel
Belgium
Tel.: +32 3 680 15 50 | Fax: +32 3 658 71 21
Email: mail@intersentia.be

Distribution for the USA and Canada:

Independent Publishers Group
Order Department
814 North Franklin Street
Chicago, IL 60610
USA
Tel.: +1 800 888 4741 (toll free) | Fax: +1 312 337 5985
Email: orders@ipgbook.com

Privacy Online, Law and the Effective Regulation of Online Services

© Marcin Betkier 2019

The author has asserted the right under the Copyright, Designs and Patents Act 1988, to be identified as author of this work.

No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, without prior written permission from Intersentia, or as expressly permitted by law or under the terms agreed with the appropriate reprographic rights organisation. Enquiries concerning reproduction which may not be covered by the above should be addressed to Intersentia at the address above.

Artwork on cover: © Ed Buziak/Alamy Stock Photo

ISBN 978-1-78068-820-6

D/2019/7849/91

NUR 820

British Library Cataloguing in Publication Data. A catalogue record for this book is available from the British Library.

As every man goes through life he fills in a number of forms for the record, each containing a number of questions. A man's answer to one question on one form becomes a little thread, permanently connecting him to the local centre of personnel records administration.

There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialised as rubber bands, buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence.

The point is that a so-called completely clean record was almost unattainable, an ideal, like absolute truth. Something negative or suspicious can always be noted down against any man alive. Everyone is guilty of something or has something to conceal. All one has to do is to look hard enough to find out what it is.

Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads, who manage personnel records administration, that most complicated science, and for these people's authority.

Aleksandr Solzhenitsyn, *Cancer Ward*

PREFACE

This book is different from other books about online privacy. This is because it does not focus on describing how our democracies have been subverted and our souls have been sold to the holders of our personal data. Instead, it concentrates on showing a way out of these problems. Importantly, this ‘way out’ is not a list of best wishes or broad-brush principles with little practicality. The solution to privacy problems related to online services presented in this book is a carefully planned-out regulation that comprises quite a few elements, but it is completely possible to introduce. The key to achieve this lies in reframing our understanding of online privacy and slightly modifying the incentives of data holders.

I recognise that lawyers reading this book may be waiting for the description of data protection laws, which comes only in the last chapter (Chapter 7). I can almost hear their: ‘What about the GDPR?’ But, the laws have been, so far, quite ineffective in solving online privacy problems. To build an effective regulatory model, the laws are, of course, instrumental and necessary, but only as necessary as a hammer for building a wooden fence. That is, the laws come last to put together all the other elements. Therefore, the book needs to be read as a whole, because it introduces the regulatory model starting from its philosophical underpinnings through the description of the privacy problems, presentation of a theoretical solution and a number of economic, technological and, finally, legal regulatory tools. All of this gives a possibly complete description of our ‘way out’.

Having said all of this, I am far from complacent about the content. Although I have done my best to prepare it well, it is just a proposal. However, the protection of our democracies and souls is important. Our increasingly consolidated markets fuelled by personal data also need regulation that would introduce more balance and competition, and could support innovation. This proposal leads exactly this way. And these goals can be achieved by empowering and helping individuals to manage their own personal data.

Marcin Betkier
Wellington, 23 March 2019

ACKNOWLEDGEMENTS

This book is an extended and revised version of the PhD thesis that was submitted and defended at the Faculty of Law of Victoria University of Wellington. This was only possible thanks to Nicole Moreham, my primary supervisor. I would like to express my deepest gratitude to her for being generous with her time, knowledge and practical advice, and for her thoughtfulness. I am also very lucky to have received a great deal of helpful advice and guidance from Tony Angelo and from my secondary supervisor, Susy Frankel. I am immensely thankful for their support. I am also very thankful for the insightful comments, questions and recommendations of my examiners: Ursula Cheer, Neil Dodgson, Dean Knight and Megan Richardson. I took on board all their recommendations.

Also, I will not forget about invaluable comments, suggestions and other forms of support given by Graeme Austin, Petra Butler, Carwyn Jones, Katarzyna Szymielewicz, Jason Bosland, Paul De Hert, Katrine Evans, David de Joux, Antonio Pabón Cadavid, Nikita Melashchenko, Joel Colón-Ríos, Geoff McLay, Matteo Solinas, Mark Hickford, Markus Luczak-Roesch, Mary-Ellen Gordon, Julia Talbot-Jones, Hedwig Eisenbarth, Carol Sorenson, Bill Atkin and Nessa Lynch. I apologise if I have forgotten anyone.

I also very much appreciated the support of my academic colleagues from the Faculty of Law, and the thoughtful help from its professional staff, especially from Jonathan Dempsey. I am grateful to Victoria University of Wellington and its community for providing me with indispensable help and financial support for my research.

Special thanks to all the staff at Intersentia who have worked on this book. I am lucky to have you as a publisher and I am hoping we can work together again on future projects. I am very grateful for the proofreading and editing help of a professional editor, Madeleine Collinge, whose assistance was immensely valuable, and also to Angus Graham and Tom White, research assistants at the Faculty of Law, for their careful help in automating citations.

Dear friends and family. Your friendship and aroha kept me going during the years I was stubbornly and selfishly pursuing my ambition of writing this book. I will do my best to give it back.

CONTENTS

<i>Preface</i>	vii
<i>Acknowledgements</i>	ix
<i>List of Cases</i>	xv
<i>List of Legislation and International Instruments</i>	xvii
<i>List of Tables, Figures and Schedules</i>	xix
<i>List of Abbreviations</i>	xxi

Chapter 1. Introduction	1
--------------------------------------	---

PART I. THE PROBLEM

Chapter 2. What is Data Privacy and What is the Role of Consent?	9
---	---

1. The Scope: Personal Data Collection and Use by Service Providers	9
1.1. Data and Information	9
1.2. Individuals and Personal Data Collection	11
1.3. Service Providers, the Use of Personal Data and Authorisation	14
2. Data Privacy	19
2.1. Normative and Non-Normative Accounts of Privacy	19
2.2. Data Privacy as Informational Self-Determination (Autonomy)	21
2.3. The Importance of Privacy Values	24
2.4. Online Privacy as a Process of Controlled Self-Revelation	28
3. Autonomy and Consent in the Privacy Process	29
3.1. Autonomy and Consent	29
3.2. Problems of Consent in Respect of Data Privacy	33
3.3. Autonomous Choice in Respect of Privacy Process	36

Chapter 3. What are the Challenges from Online Services?	41
---	----

1. How Do 'Data Markets' Work?	41
1.1. Control Over Data is a Key Success Factor in Online Markets	41
1.2. Which Activities of Service Providers Pose Privacy Problems?	45
1.2.1. 'Enhanced' Service Model	46
1.2.2. Trading Platform Model	49
1.2.3. Non-Trading Platform Model	50
1.3. The Economic Value of Data	54

2.	What Makes ‘Cyber’ Special?	58
2.1.	The Architecture of the Online Environment	58
2.2.	Information Asymmetry and Individualisation	62
3.	Privacy Problems in Respect of Online Services	66
3.1.	Risk of Tangible Loss to the Individual.	67
3.2.	Harm to Individual Values: Autonomy and Dignity.	70
3.3.	Interference with Social Values	74

PART II. PRIVACY MANAGEMENT AS A SOLUTION

Chapter 4. How to Regulate Online Services 79

1.	Regulating Privacy with the Privacy Management Model	80
1.1.	What Privacy Regulation should Achieve	80
1.2.	Problems of Data Privacy Regulation	82
1.3.	Privacy Management Model.	87
2.	Why Regulate Privacy with the Privacy Management Model?	92
2.1.	Achieving Values-Related Goals	92
2.2.	Correcting Market Failure	95
2.3.	Oiling the Wheels of the Digital Economy.	99
3.	What is Needed to Regulate for Privacy Management?	105
3.1.	Which Regulatory Tools are Needed to Implement Privacy Management?	106
3.1.1.	Market (or Economic Regulation)	108
3.1.2.	‘Norms’	109
3.1.3.	The ‘Code’ (Architecture)	110
3.1.4.	The Fourth Modality: Law.	113
3.2.	Which Regulatory Regime should Implement PMM?	116

Chapter 5. Economic Regulation of ‘Data Markets’ 123

1.	Could ‘Data Markets’ Introduce Privacy Management by Themselves? ...	123
1.1.	It may be Too Early to Find Monopoly and Abuse of Market Power	124
1.2.	Why Does the ‘Invisible Hand’ of the Market Not Improve Privacy?	130
1.3.	Self-Regulation is Not a Viable Option.	132
2.	How to Influence ‘Data Markets’ to Improve Informational Self-Determination.	135
2.1.	Employing Personal Information Administrators.	136
2.2.	Increasing Competition by Data Portability	144
2.3.	Increasing ‘Data Sensitivity’ by Monitoring and Advice	147
2.4.	Securing Data Subjects from Uncontrolled Tracking	149

Chapter 6. The Architecture of Privacy Management	153
1. How to Express and Communicate Data Subjects' Privacy Decisions	154
1.1. Privacy Policies and Policy Languages for PMM	154
1.2. Other Initiatives Allowing Individuals to Express Their Preferences	159
1.2.1. 'Do Not Track' Technology	159
1.2.2. One-Stop Shopping Opt-Out Tools	160
1.2.3. Privacy Dashboards	161
2. How to Categorise and Present Data and Data Uses	165
2.1. Categorisation of Data and Data Uses	165
2.1.1. Categories of Data	166
2.1.2. Categories of Data Use	169
2.2. Presentation of Choices to Data Subjects	170
3. How Technology Supports Enforcement and Accountability	174
3.1. Technologies Used to Handle Personal Data in the ICT Systems of Service Providers	174
3.2. Enforcement and Accountability Tools	176
 Chapter 7. How to Construct Laws for Privacy Management	 183
1. Marking the Gaps: Privacy Management in the Laws Based on Fair Information Practice Principles	184
1.1. Why there is Little Privacy Management in National Data Privacy Laws	184
1.2. How National Data Privacy Laws Fit into Privacy Management ...	190
1.3. The Deficiencies of a Procedural Approach	197
2. Closing the Legal Gaps: Privacy Management on Top of the General Data Protection Regulation	199
2.1. Closing Gaps in Controlling	200
2.1.1. Data Subjects should be Able to Decide about the Collection of Particular Data Types and Their Uses	201
2.1.2. Data Subjects should be Able to Delete Their Data	203
2.1.3. Data Subjects should be Able to Change Service Provider and Take All Their Data with Them	204
2.1.4. Data Subjects should be Able to Monitor the Use of Their Data	206
2.2. Closing Gaps in Organising	208
2.2.1. Data should be Organised in a Way that Enables Visibility of All Data Types and Uses by Data Subjects	211
2.2.2. Data Subjects should be Able to Control Their Data and Policy by Means of a Standardised UI and API	212
2.3. Closing Gaps in Planning	214

2.3.1.	Data Subjects should be Able to Define and Change Their Own Policy	216
2.3.2.	Data Subjects' Policies should be Stable (Preserved and Guaranteed)	217
3.	Closing the Legal Gaps: The Necessary General Legal Requirements.	218
3.1.	Enacting an Overarching Principle of Informational Self-Determination	219
3.1.1.	Why the Right to Informational Self-Determination is Necessary	219
3.1.2.	What the Right to Informational Self-Determination should Look Like	222
3.1.3.	Can it be Developed in Europe?	224
3.2.	Extraterritorial Reach of the Law	228
3.3.	Keeping PMM within Bounds	234
3.3.1.	Limiting the Scope of Regulation	234
3.3.2.	Restrictions on PIAs and Their Activities	235
3.3.3.	Restrictions on Binding Up Services with Blanket Consent	235
4.	Conclusion	237
	<i>Schedules</i>	239
	<i>Bibliography</i>	247
	<i>Index</i>	281

LIST OF CASES

AUSTRALIA

Duffy v Google Inc. [2015] SASC 170. 232

CANADA

A.T. v Globe24h.com 2017 FC 114 233–234
Bears v Saldanha 2003 SCC 72 233
Eldridge v British Columbia (Attorney General) (1997) 3 SCR 624 (SC). 221
Google Inc. v Equustek Solutions Inc. 2017 SCC 34 234
Lawson v Accusearch Inc. 2007 FC 125 233
Libman v The Queen (1985) 2 SCR 178 (SC) 233
RWDSU v Dolphin Delivery Ltd. (1986) 2 SCR 573 (SC) 221

EUROPEAN COURT OF HUMAN RIGHTS

Amann v Switzerland, 27798/95, ECHR 2000-II 24, 224
Evans v The United Kingdom, 6339/05, ECHR 2007-I. 226
Flinkkilä and Others v Finland, 25576/04, [2010] ECHR 446 225
Malone v The United Kingdom, 8691/79, Series A no. 82 225
M.S. v Sweden, 20837/92, 1997-IV 188
Odièvre v France, 42326/98, ECHR 2003-III 226
P.G. and J.H. v the United Kingdom, 44787/98, ECHR 2001-IX. 225
Pretty v The United Kingdom, 2346/02, 2002–3 225
Reklos and Davourlis v Greece, 1234/05, [2009] ECHR 200 226
Rotaru v Romania, 28341/95, ECHR 2000-V 24
Sciaccia v Italy, 50774/99, ECHR 2005-I 225
Uzun v Germany, 35623/05, [2010] ECHR 2263 225
Verlagsgruppe News GmbH and Bobi v Austria, 59631/09, [2012] ECHR 201. 225
Von Hannover v Germany, 59320/00, ECHR 2004-VI 225
Von Hannover v Germany (No. 2), 40660/08, 60641/08, 2012 226

EUROPEAN UNION

*Digital Rights Ireland Ltd v Minister for Communications, Marine and
Natural Resources and Others*, C-293/12, C-594/12, ECLI:EU:C:2014:238 17, 227
Europemballage and Continental Can v Commission, Case 6/72, ECLI:EU:C:1973:22. 125
Facebook/WhatsApp (Case COMP/M7217) Commission Decision, 10 March 2014. 129

<i>František Ryněš v Úřad pro ochranu osobních údajů (Office for Personal Data Protection)</i> , C-212/13, ECLI:EU:C:2014:2428	227
<i>Google Android</i> (Case AT.40099) Commission Decision 18 July 2018 (no public version available)	127
<i>Google/DoubleClick</i> (Case COMP/M4731) Commission Decision, 11 March 2008	129
<i>Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)</i> , C-131/12, ECLI:EU:C:2014:317	17, 85, 192
<i>Irish Sugar plc v Commission of the European Communities</i> , T-228/97, ECLI:EU:T:1999:246	236
<i>Maximilian Schrems v Data Protection Commissioner</i> , C-362/14, ECLI:EU:C:2015:650	134
<i>N. S. v Secretary of State for the Home Department</i> , C-411/10 and C-493/10, ECLI:EU:C:2011:8652	221
<i>Rechnungshof v Österreichischer Rundfunk</i> , C-465/00, C-138/01 and C-139/01, ECLI:EU:C:2003:294	225
<i>Schecke v Land Hessen</i> , C-92/09, C-93/09, ECLI:EU:C:2010:662	226
<i>Schwarz v Stadt Bochum</i> , C-291/12, ECLI:EU:C:2013:670	227
<i>Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis</i> , C-203/15, C-698/15, ECLI:EU:C:2016:970	227
<i>United Brands Company v Commission of the European Communities</i> , C-27/76, ECLI:EU:C:1978:22	236
<i>WebMindLicenses Kft. v Nemzeti Adó- és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság (Hungarian National Tax and Customs Authority)</i> , C-419/14, ECLI:EU:C:2015:832	227
<i>YS v Minister voor Immigratie, Integratie en Asiel</i> , C-141/12, ECLI:EU:C:2014:2081	191, 207

GERMANY – BUNDESVERFASSUNGSGERICHT

<i>Census Act (Volkszählungsurteil)</i> , 1 BvR 209/83 et al., BVerfGE 65, 1	21, 223–224
<i>North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen)</i> , 1 BvR 370/07, BVerfGE 120, 274	21–22, 223–225
<i>Nuremberg Higher Regional Court</i> , 1 BvR 3167/08, BVerfGE 84, 192	223–224
<i>Release of Confidentiality (Schweigepflichtentbindung)</i> , 1 BvR 2027/02	223

NEW ZEALAND

<i>A v Google New Zealand Ltd</i> [2012] NZHC 2352	233
<i>Allistair Patrick Brooker v The Police</i> [2007] NZSC 30	220
<i>Hosking v Runting</i> [2004] NZCA 34	83

UNITED KINGDOM

<i>Malone v Commissioner of Police of the Metropolis (No 2)</i> [1979] Ch 344	220
<i>Titchener v British Railways Board</i> [1983] UKHL 10	33

LIST OF LEGISLATION AND INTERNATIONAL INSTRUMENTS

AUSTRALIA

Privacy Act 1988 (Cth) 15, 34, 194–195, 229, 232, 276, 278

CANADA

Personal Information Protection and Electronic Documents Act 2000..... 194, 233

COUNCIL OF EUROPE

Convention for the Protection of Human Rights and Fundamental
Freedoms (Rome, signed 4 November 1950)..... 120–121, 185, 187
Convention for the Protection of Individuals with regard to Automatic
Processing of Personal Data, European Treaty Series No. 108
(Strasbourg, signed 28 January 1981)..... 120–121, 185, 187, 190
Parliamentary Assembly of the Council of Europe, Resolution 1165 (1998)..... 222
Protocol amending the Convention for the Protection of Individuals with
regard to Automatic Processing of Personal Data, European Treaty Series No. 223
(Strasbourg, opened for signatures on 10 October 2018) 185

EUROPEAN UNION

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
(Data Protection Directive) [1995] OJ L 281/31 119, 192, 198, 276, 278
Directive 2002/22/EC of the European Parliament and of the Council
of 7 March 2002 on Universal Service and Users' Rights relating to Electronic
Communications Networks and Services (Universal Service Directive)
[2002] (OJ L108/51)..... 131, 160
Directive 2002/58/EC of the European Parliament and of the Council
of 12 July 2002 Concerning the Processing of Personal Data and the Protection
of Privacy in the Electronic Communications Sector (Directive on Privacy
and Electronic Communications) [2002] OJ L201/37 160

European Parliament resolution of 27 November 2014 on supporting consumer rights in the digital single market 2014/2973(RSP)	125
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 (General Data Protection Regulation) 95/46/EC [2016] OJ L119/1	192, 198

OECD

OECD Guidelines governing the protection of privacy and transborder flows of personal data (1980)	185
OECD Guidelines governing the protection of privacy and transborder flows of personal data (2013)86, 185–186

NEW ZEALAND

Fair Trading Act 1986	236
Privacy Act 1993	34, 115, 117, 194, 199, 229, 232–233, 276, 278
Telecommunications Act 2001	131

LIST OF TABLES, FIGURES AND SCHEDULES

TABLES

Table 1.	Types of authorisation of data processing (or collection and use) in the researched jurisdictions	15
Table 2.	Sources of personal data available to service providers	42
Table 3.	Different levels of the influence of the ‘code’	112
Table 4.	Market capitalisation of global Internet companies in 2018, according to Kleiner Perkins Caufield Byers	118
Table 5.	Proposal for data types/categories, following the Kantara Initiative’s ‘Consent Receipt Specification’	167
Table 6.	Proposal for data use categories	170

FIGURES

Figure 1.	Entities processing personal data online.	16
Figure 2.	Data processing activities	17
Figure 3.	Varying levels of autonomous choice in respect of the privacy process	38
Figure 4.	Enhanced service model	46
Figure 5.	Flow of personal data and money in the business model of a trading platform	49
Figure 6.	Flow of personal data and money in the non-trading platform model.	51
Figure 7.	The value chain of Internet services.	60
Figure 8.	Direct and indirect control over data	85
Figure 9.	PMM and its functions	88
Figure 10.	Organising – interfaces and the role of a third party	89
Figure 11.	Privacy management cycle	90
Figure 12.	Evaluation criteria for data subjects’ autonomy in PMM.	91
Figure 13.	Lessig’s four modalities (regulating forces).	107
Figure 14.	PIA acting for data subjects to manage data.	137
Figure 15.	Example of the exchange of communications with PIA during the initiation of a service and afterwards	138
Figure 16.	PDS model.	141

Figure 17.	Privacy policies and languages to express them.	155
Figure 18.	Standardised table version of privacy 'nutrition label'	172
Figure 19.	Individual privacy management interface	173
Figure 20.	Technologies to enforce privacy management	175
Figure 21.	Non-normative and normative dimensions of privacy in the national data privacy laws	195
Figure 22.	Evaluation criteria for data subjects' autonomy in PMM	200

SCHEDULES

Schedule 1.	Comparison of early privacy principles and recommendations.	239
Schedule 2.	Comparison of privacy principles and rules in the researched jurisdictions.	242

LIST OF ABBREVIATIONS

API	Application Programming Interface
Article 29 WP	Article 29 Working Party – an advisory body of representatives from the DPAs of each EU Member State, replaced by the EDPB with the introduction of the GDPR
BVerfG	Bundesverfassungsgericht – German Federal Constitutional Tribunal
ChFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Convention 108	Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108 (1981, modernisation of 2018 is waiting for ratification)
DNT	‘Do Not Track’ (technology standard)
DPA	Data Protection Authority
DPD	Data Protection Directive – 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 L 281/31
ECHR	European Convention on Human Rights – Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board – an EU body comprising the European DPAs according to Article 68 of the GDPR
ePrivacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) [2002] OJ L 201/37
FIPPs	Fair Information Practice Principles

GDPR	General Data Protection Regulation – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC [2016] OJ L 119/1
ICT	Information and Communications Technology
OECD	Organisation for Economic Co-operation and Development
OECD Guidelines	Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development (1981, amended in 2013)
P3P	Platform for Privacy Preferences (technology standard)
PDS	Personal Data Store
PIA	Personal Information Administrator
PIMS	Personal Information Management System
PIPEDA	Personal Information Protection and Electronic Documents Act 2000 (Canada)
PMM	Privacy Management Model
SNMP	Simple Network Management Protocol (technology standard)
T&Cs	Terms and Conditions
UI	User Interface
UMA	User-Managed Access (technology standard)
VRM	Vendor Relationship Management