About the Authors

Kenneth A. Bamberger is Professor of Law at the University of California, Berkeley, School of Law (Boalt Hall), and an affiliated faculty member with the Center for the Study of Law and Society. He teaches courses on Administrative Law, First Amendment Law, and Technology and Governance. His research focuses on regulatory decision-making; the roles of public and private actors in governance; business regulation and corporate compliance; and related issues of technology in governance, with a particular focus on information privacy and other forms of risk management.

Emilie Barrau holds the position of legal advisor at the CNIL, the French data protection authority. She has been working in the European and International department since May 2010, primarily on the review of the EU privacy framework. Previously (2004–2010), she worked for BEUC, the European consumer organisation in Brussels, as a legal officer and a European project manager. She was leading the BEUC team on consumer rights’ in the digital environment, following the issues of unfair commercial practices, advertising, data protection and privacy. She holds a Master’s degree in consumer protection and competition law (Université de Montpellier, France) and a LL.M. in International Business Law (Exeter University, UK).

Robin M. Bayley is President of Linden Consulting, Inc., Privacy and Policy Advisors, which she started in 2003 after a career in the British Columbia government. Robin developed policy and legislation and advised ministries on compliance with information and privacy law. She has conducted and reviewed privacy impact assessments and developed personal information sharing agreements. She advises public bodies and private organisations on meeting their legal privacy/data protection obligations while achieving their business goals and has assisted data protection authorities by developing internal processes, public information and complaint tools. Robin has co-authored several articles, chapters and reports on Canadian administration of information and privacy law, video surveillance law, and privacy impact assessments.

Colin J. Bennett is Professor of Political Science at the University of Victoria, BC. He has held Visiting fellowships at Harvard’s Kennedy School of Government,
the Center for the Study of Law and Society at University of California, Berkeley, and the Center for Cyberspace Law and Policy at the University of New South Wales. His research has focused on the comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels. In addition to many scholarly articles and chapters, he has published six books: *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992); *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999, co-edited with Rebecca Grant); *The Governance of Privacy: Policy Instruments in the Digital Age* (MIT Press, 2006 with Charles Raab); *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press, 2008); *Playing the Identity Card: Surveillance, Security Identification in Global Perspective* (Routledge, 2008 co-edited with David Lyon) and *Security Games: Surveillance and Control at Mega-Events* (Routledge, 2011, co-edited with Kevin D. Haggerty). He is currently the co-investigator of a large Major Collaborative Research Initiative grant entitled “The New Transparency: Surveillance and Social Sorting.”

Laurent Beslay works as Co-ordinator on Security and Technology for the European Data Protection Supervisor based in Brussels, since September 2004. His responsibilities include security and technology co-ordination of prior-checks opinions, policy opinions, complaints, inspections, audits and their follow-up. He previously worked, for six years, for the Joint Research Centre of the European Commission, the IPTS (Institute for Prospective Technological Studies) as a project officer in the field of cyber-security. He holds a post-Master’s degree in Global Management of Technological Risks and Crisis (University of Paris, Sorbonne) and a Master’s degree in International Relations.

Tobias Bräutigam is Legal Counsel (Privacy) at Nokia Corporation. He works on various aspects of privacy compliance, such as international data transfers, employee privacy and privacy in consumer services. He also plans and executes awareness-raising campaigns and privacy training throughout the company. He holds a Master’s degree from the University of Freiburg i. Brsg and a PhD from the University of Helsinki. His research focuses on issues of information access, information privacy and comparative law. Learning new things everyday is his goal. He is an Affiliated Research Fellow at the Erik Castrén Institute of International Law and Human Rights, Helsinki.

Amanda Chandler is Global Privacy Manager at Vodafone. Prior to joining Vodafone in June 2003, she worked as a compliance and policy manager with the UK Information Commissioner and then as European Privacy Manager for a US online ad-serving company. Since joining Vodafone, she has been responsible for the implementation of data protection policy and strategy, and played a key role at an operational level in building data protection compliance into business processes across the company, ranging from new products and services to customer services. She works with operational colleagues across the Vodafone corporate family to help build processes and structures to help Vodafone meet its customers’
privacy expectations while at the same enabling its privacy officers to develop as a community of privacy professionals.

**Andrew Charlesworth** is Reader in IT Law in the School of Law and Department of Computer Science at the University of Bristol, where he is the Director of the cross-disciplinary Centre for IT & Law. His post was initially funded by a range of commercial sponsors, and Andrew continues to work with organisations such as Vodafone, Herbert Smith LLP and HP Labs on a range of legal issues. He has considerable experience in the areas of privacy and data protection, including authoring the Data Protection Code of Practice for Higher Education; working on the methodology for the conduct of effective privacy impact assessments in the UK and the associated handbook on PIAs, for the ICO; and ongoing collaborative work with researchers at HP Labs on issues such as privacy in cloud computing, and developing an automated business decision support methodology for PIAs.

**Roger Clarke** is a 40-year veteran of the IT industry. For the last 20 years, he has specialised in strategic and policy aspects of e-business, information infrastructure, dataveillance and privacy, as Principal of Xamax Consultancy Pty Ltd, Canberra. He is a Visiting Professor in the Cyberspace Law & Policy Centre at the University of New South Wales, and a Visiting Professor in the Department of Computer Science at the Australian National University. He has been a board member of the Australian Privacy Foundation since its establishment in 1987, and has been its Chair during 2006–12. He has been a member of the Advisory Board of Privacy International since 2000. He was a member of the Victorian Data Protection Advisory Council in 1996, and of the federal Attorney-General’s Core Consultative Group in 2000, and has performed consultancies for various organisations. In 2009, he was the second person to be awarded the Australian Privacy Medal, following Justice Michael Kirby.

**Stephen Deadman** is the Group Privacy Officer and Head of Legal – Privacy, Security & Content Standards at Vodafone Group where he is responsible for leading Vodafone’s global privacy policy and strategy, and the development and implementation of Vodafone’s global privacy programme. He is also responsible for legal and regulatory guidance to the Group on law enforcement, security, Internet regulation and policy. Since joining Vodafone in 1997, he has managed a number of teams with a particular focus on building the governance mechanisms and processes for addressing the importance of law and regulation in the development of products, services and technologies. In 2002, he founded and chaired Vodafone’s international network of privacy and security law experts and in 2005 formulated and succeeded in the adoption of Vodafone’s global privacy policy. With more than 14 years in the mobile industry, Stephen has worked on many of the emerging privacy issues for the sector including geo-location, mobile advertising, identity management and human rights. A significant portion of his work involves engaging with regulators, policy-makers, civil society, investors, academia and other industry players.

**Paul De Hert** is an international human rights expert. The bulk of his work is devoted, but not limited, to criminal law and technology and privacy law. At
Brussels, Paul De Hert holds the chair of Criminal Law and International and European Criminal Law and Historical introduction to eight major constitutional systems. He is Director of the VUB Research group on Fundamental Rights and Constitutionalism (FRC), Director of the Department of Interdisciplinary Studies of Law (Metajuridics) and core member of the research group Law Science Technology & Society (LSTS) (see: www.vub.ac.be/LSTS). He is an associate professor at Tilburg University where he teaches Privacy and Data Protection in the Master’s programme at the Tilburg Institute of Law and Technology (TILT). He is a member of the editorial boards of several national and international scientific journals such as the *Inter-American and European Human Rights Journal* (Intersentia), *Criminal Law & Philosophy* (Springer) and *Computer Law & Security Review* (Elsevier). He is co-editor in chief of the Supranational Criminal Law Series (Intersentia) and the *New Journal of European Criminal Law* (Intersentia).

**John Edwards** is a New Zealand lawyer specialising in information law. From 1990–1993, he worked for New Zealand’s parliamentary Ombudsmen, reviewing government decisions to withhold information sought under the Official Information Act (New Zealand’s freedom of information statute). In 1993, he assisted the first Privacy Commissioner to set up his office, managing the Wellington office, preparing educational material, and developing complaint investigation processes. Since late 1993, he has been in practice on his own account working for a wide variety of clients in the public and private sector including the Ministry of Justice, the Crown Law Office and the Law Commission. He has been engaged on a temporary basis as solicitor in the State Services Commission, the Department of the Prime Minister and Cabinet, the Inland Revenue Department and the Ministry of Health. He has undertaken many privacy impact assessments and investigations and often provides commentary to the media on information law issues. He has published widely in New Zealand and abroad and has addressed many conferences in New Zealand and elsewhere in the world on privacy matters.

**John Martin Ferris** is the President of Ferris & Associates, Inc., and has more than 40 years of experience in information security and privacy including the life cycle engineering of information systems. He is a member of ANSI Accredited Standards Committee (ASC) X9 and is currently an ANSI ASC X9 liaison to ISO Technical Committee 68 and an ISO TC 68 liaison to the ISO Privacy Steering Committee. His consulting clients have included US agencies, the American Bankers Association and the Financial Services Technology Consortium. Mr. Ferris is retired from the US Department of Treasury where he was responsible for the US Treasury information security program and policies that directed Treasury’s bureaus in compliance with federal security laws, policies and standards. Mr. Ferris holds a BS in mathematics from Drexel University and a MS in computer science from The Johns Hopkins University.

**Anne-Christine Lacoste** is a legal advisor at the Office of the European Data Protection Supervisor (EDPS). She co-ordinates the activities of the EDPS in relation to the Article 29 Data Protection Working Party, drafts official opinions and
follows issues such as transfer of personal data to third countries (transatlantic
dialogue on data protection, passenger name records, binding corporate rules) and
privacy in the context of new technologies. She has completed a degree in law and
a post-graduate degree in International and European law at the Catholic University
of Louvain. She worked for a few years as a researcher at the Department of
Economic and Social Law of the University, on legal assistance programmes of the
European Commission. She joined the EDPS after 10 years at the Belgian Privacy
Commission where she was head of the legal service.

Gwendal Le Grand is the head of the IT experts department at the CNIL, the
French data protection authority, since April 2007. He contributes to the activi-
ties of the Article 29 Working Party (Art. 29 WP) on technology-related issues
such as RFID, behavioural advertising, search engines and social networks. He is
the liaison officer of the Art. 29 WP to ISO/IEC JTC1/SC27/WG5, which devel-
ops privacy standards, and is a member of the ISO Privacy Steering Committee.
He represents the CNIL and the Art. 29 WP within several expert groups of the
European Commission such as the RFID expert group (2007–2009), the data reten-
tion expert group (since 2008) and the Internet of Things expert group (since
2010). Before joining the CNIL, he worked as an associate professor at the École
Nationale Supérieure des Télécommunications (ENST), Paris. He received his PhD
in computer science from the University of Paris 6 in July 2001.

Gary T. Marx is Professor Emeritus from M.I.T. He has previously taught at
the University of California, Harvard University and the University of Colorado
and been a visiting professor at many other schools in the U.S. and Europe. In a
distinctive voice for almost five decades, he has contributed to the fields of race rela-
tions, collective behaviour and social movements, law and society and surveillance
studies. His writing has appeared in academic and popular outlets across discip-
lines and cultures and has been widely recognised with awards, fellowships, many
reprints and translations. He is the author of Protest and Prejudice; Undercover:
Police Surveillance in America; Undercover: Police Surveillance in Comparative
Perspective (with C. Fijnaut); Collective Behavior and Social Movements (with
D. McAdam), among other books. He has written many articles with his students
and 12 introductions to colleagues’ books and served on an array of editorial and
review boards, panels, committees and commissions. Much of his work in recent
decades is at www.garymarx.net.

Emilio Mordini is an MD (University of Rome La Sapienza), specialised in psy-
chiatry and trained as a psychoanalyst. He was a partner of the Psychoanalytic
Institute for Social Research (1986–2001), Professor of Bioethics at the University
of Rome (1994–2006), Secretary of the Bioethical Commission of the Italian
National Research Council (2000–04). In 2002, he founded the Centre for Science,
Society and Citizenship (CSSC), an independent, non-partisan, research centre
based in Rome, the aim of which is to contribute to a better understanding of the
contemporary world by clarifying the social, cultural and ethical factors that shape
technological innovation. He is the scientific secretary of the Italian Technology
Platform on Biometric Technology, and serves on the board of a number of international scientific associations. He has published extensively in peer-reviewed journals, and edited nine books.

Deirdre K. Mulligan is Assistant Professor at the University of California Berkeley School of Information and a Faculty Director of the Berkeley Center for Law and Technology. She teaches and writes on law and policy issues related to information and communication technology. Her research focuses on issues of information privacy, information security, surveillance and the interplay between legal rules and technical systems. She is the Policy Lead for the National Science Foundation’s TRUST Science and Technology Center, Chair of the board of the Center for Democracy and Technology, and Co-chair of Microsoft’s Trustworthy Computing Academic Advisory Board. Her recent publications include “Privacy on the Books and on the Ground”, *Stanford Law Review*, Vol. 63, January 2011, and “New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry”, *Law & Policy*, Vol. 33, No. 4, October 2011, both with Kenneth A. Bamberger.

David Parker is Emeritus Professor of Economics at the Cranfield School of Management, Cranfield University, UK. Previously he was Research Professor in Privatisation and Regulation at Cranfield. He is a former Member of the UK Competition Commission and currently a Member of the UK Government’s Regulatory Policy Committee. David has written extensively on regulation issues and has acted as a consultant on privatisation, regulation and competition in over 20 countries, most recently in the Philippines. He is a member of the Editorial Board of the *Journal of Regulatory Economics* and the Editorial Advisory Board of *Public Money & Management*.

Charles Raab was Professor of Government in the University of Edinburgh, and is Professor Emeritus and Honorary Professorial Fellow. He serves on advisory or editorial boards of many research projects, funding bodies and academic journals, and on governmental expert groups. With the Surveillance Studies Network, he co-authored *A Report on the Surveillance Society* (2006) and an *Update Report* (2010) for the UK Information Commissioner. He has conducted funded research on information policy and regulatory issues, including privacy, data protection, surveillance, police co-operation, identity management, data sharing and e-government, and has written a large number of publications, including (with C. Bennett) *The Governance of Privacy* (2003; 2006). He has co-authored reports for the European Commission, UK and Scottish government agencies, and civil society groups. He was the Specialist Adviser to the House of Lords Select Committee on the Constitution for their Inquiry resulting in *Surveillance: Citizens and the State*, HL Paper 18, Second Report, Session 2008–09. His participation in European research projects includes PRIME (Privacy and Identity Management for Europe) and SIAM (Security Impact Assessment Measure). He is an Academician of the Academy of Social Sciences (AcSS).
Artemi Rallo Lombarte is Chair of Constitutional Law at the Jaume I University of Castellón in Spain. He was also Professor of Constitutional Law and Head of the Constitutional Law Department at the university from 1993 to 1998. Before his return to the university, he was Director of the Spanish Data Protection Agency, in which capacity he wrote his chapter on the Madrid Resolution for this book. He graduated in Law with Extraordinary Prize Honours (1988) and has a Doctorate in Law from the University of Valencia (1990). He has authored numerous monographs, books and scientific articles in specialised national and international magazines. He has participated in national and international research lines and projects on contemporary transformations of the public administration. He was Director General of the Judicial Studies Centre of the Ministry of Justice from 2004 to 2007.

Sarah Spiekermann is a professor for Business Information Systems Engineering at Vienna University of Economics and Business (WU Wien) where she chairs the Institute for Management Information Systems. Before starting her career in Vienna, she completed her “Habilitation” and Ph.D. at the Institute of Information Systems at Humboldt University in Berlin and held Adjunct Professor positions with the Heinz College of Public Policy and Management, Carnegie Mellon University in Pittsburgh and the European Business School (EBS). Her areas of expertise are electronic privacy, RFID, personalisation/CRM, user interaction behaviour in e-commerce and m-commerce environments as well as knowledge management. For more information, see: http://www.wu.ac.at/ec/faculty/spiekermann

Blair Stewart is an Assistant Commissioner with the Office of the Privacy Commissioner, New Zealand. Mr. Stewart worked in legal practice before joining the Office when it was established in 1993. His roles in the Office over the years have included privacy policy, codes of practice, technology and international issues. Mr. Stewart has contributed to international privacy work through the Asia Pacific Privacy Authorities Forum, the International Conference of Data Protection and Privacy Commissioners and as a member of the APEC Data Privacy Subgroup since its inception in 2003. He has placed a special emphasis in his work on developing flexible and effective regulatory and institutional mechanisms for protecting privacy at national and supra-national levels. Since 1996, Blair Stewart has promoted privacy impact assessment as an adaptable tool for decision-makers and regulators dealing with novel and complex technological challenges to privacy. In 2002, Mr. Stewart wrote a Privacy Impact Assessment Handbook which has been influential in New Zealand and elsewhere. He convened international workshops on privacy impact assessment in 2003 and 2007. He holds a B.A. and LL.B.(Hons) from the University of Auckland and has been admitted as a Barrister and Solicitor of the High Court of New Zealand and as a Solicitor of the Supreme Court of England and Wales.

Jennifer Stoddart was appointed Privacy Commissioner of Canada in 2003. Since then, she has overseen a number of important investigations and audits of personal information handling practices in the public and private sectors. She was the
first data protection authority in the world to conduct a comprehensive investigation of the privacy policies and practices of the popular social networking site, Facebook. She also investigated with the Alberta Commissioner a massive data breach at US retail giant TJX, which owns Winners and HomeSense stores in Canada. More recently, she found that Google Inc. contravened Canadian privacy law when it collected personal information from unsecured wireless networks for Google StreetView. In 2011, she concluded that an audit by her Office had found that Staples Business Depot stores had failed to fully wipe customer data from returned devices such as laptops and USB hard drives destined for resale – even though the company had previously committed to addressing the long-standing problem. Commissioner Stoddart also led a number of important investigations on the public sector front, and has conducted audits of, for example, the government’s personal information disposal practices, its use of wireless technology, the Passenger Protect Program, Passport Canada, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and the Royal Canadian Mounted Police’s Exempt Databanks. Throughout her mandate, she has advocated the need to ensure that both PIPEDA and the Privacy Act continue to provide the strongest possible protections for Canadians in an era of constantly evolving risks to privacy. Commissioner Stoddart was previously President of the Commission d’accès à l’information du Québec, an organisation responsible for both access to information and the protection of personal information. She has held several senior positions in public administration for the Governments of Québec and Canada. Commissioner Stoddart holds a Bachelor of Civil Law degree from McGill University, as well as a Master of Arts degree in history from the University of Québec at Montréal and a Bachelor of Arts degree from the University of Toronto’s Trinity College.

Florian Thoma is Chief Data Protection Officer of Siemens, a global electronics and electro-technical company with more than 400,000 employees. He is responsible for ensuring the effective protection of personal privacy rights and compliance with data protection laws and internal regulations and for the worldwide coordination of the Siemens data protection organisation. He serves as member of the IAPP Board of Directors and the IAPP European Advisory Board, and chairs the Workgroup on data protection of BITKOM (the German IT and Telecom Industry Association). He is founder and chair of the non-profit Bavarian Society for Data Protection. Prior to his current position, Florian acted as Siemens lead counsel for the CIO organisation, senior counsel to the in-house IT services provider and chaired the e-commerce, telecoms and data protection practice. He graduated from Regensburg University in 1994.

Adam Warren started his career in the financial services sector. He is currently employed as Research Associate and Lecturer at the Department of Geography, Loughborough University, UK. In 2007, he co-ordinated the project work on privacy impact assessments for the UK Information Commissioner’s Office. His current work includes research into the impact of UK biometric residence permits on foreign nationals, the use of event-based surveillance technologies to predict emerging
infectious diseases and the effectiveness of existing health security practices at UK airports. He has a PhD from the Department of Information Science, Loughborough University.

**Nigel Waters** is a Board member of the Australian Privacy Foundation (www.privacy.org.au) and represents Privacy International (www.privacyinternational.org) at meetings of the APEC Privacy Subgroup and other international fora. He is Principal of Pacific Privacy Consulting (www.pacificprivacy.org.au) and a researcher and visiting lecturer at the Cyberspace Law and Policy Centre, at the University of New South Wales (www.cyberlawcentre.org/ipp). He was Deputy Australian Federal Privacy Commissioner from 1989–1997, and before that Assistant UK Data Protection Registrar. He holds Masters degrees from the Universities of Cambridge and Pennsylvania and from the University of Technology, Sydney.

**David Wright** is Managing Partner of Trilateral Research & Consulting, a Limited Liability Partnership based in London (see www.trilateralresearch.com). He is co-editor and co-author of *Safeguards in a World of Ambient Intelligence* (Springer, 2008) and author of “Should privacy impact assessments be mandatory?”, which appeared in the August 2011 issue of *Communications of the ACM*. He is a partner in a consortium with Vrije Universiteit Brussel (VUB) and Privacy International, undertaking the PIAF (Privacy Impact Assessment Framework) project for the European Commission’s Directorate General Justice, a 20-month project which began in January 2011. He has been a partner in numerous other consortia and European projects dealing with privacy, data protection, security, surveillance, risk, trust, ethics, ambient intelligence and e-inclusion. He has been in four expert groups for the European Network and Information Security Agency (ENISA) dealing with privacy, trust, cloud computing and the Internet of Things. He is a free-lance researcher on the faculty of the Research Group on Law, Science, Technology and Society at the Vrije Universiteit Brussel (VUB), and has published many articles in peer-reviewed journals.
References


References


Department of Finance and Personnel (Northern Ireland), Review of Domestic Rating Data Sharing Privacy Impact Assessment (PIA), Bangor, 2008.


European Network and Information Security Agency (ENISA), Flying 2.0 – Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology, Heraklion, 2010.


European Parliament and the Council, Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.


Information Systems Audit and Control Association, COBIT 4.1, IT Governance Institute, Rolling Meadows, IL, 2008.


International Conference of Data Protection and Privacy Commissioners, “Resolution on the Urgent Need for Protecting Privacy in a Borderless World, and for Reaching a Joint Proposal


References


Office of the Privacy Commissioner of Canada (OPC), Fact Sheet on Privacy Impact Assessment. http://www.priv.gc.ca/fs-fi/02_05_d_33_e.cfm


Office of the Privacy Commissioner of Canada (OPC), Letter in response to the Privacy Impact Assessment (PIA) completed by the Canadian Air Transport Security Authority (CATSA) in anticipation of the deployment of millimetre wave (MMW) screening technology at selected Canadian airport, October 2009. http://www.priv.gc.ca/pia-efvp/let_20100108_e.cfm


Raab, Charles, “Privacy, Social Values, and the Public Interest”, Politische Vierteljahresschrift, Special Issue 46 (2011) on “Politik und die Regulierung von Information”.


Richards, Jonathan, “Top officials to be held to account for data losses”, The Times, 22 April 2008. http://technology.timesonline.co.uk/tol/news/tech_and_web/article3797278.ece


References


References


References

European Cases

BVerfG, 1 BvR 370/07 und 1 BvR 595/07 vom 30.4.2008, “OnlineDurchsuchung”.
Court of Justice of the European Union, Huber v. Germany, Judgment of 16 December 2008, Case C-524/06.
Court of Justice of the European Union ECJ, Opinion of Advocate General Poiares Maduro in Case C-524/06 (Heinz Huber v. Germany), delivered on 3 April 2008.
ECtHR, A.D. and O.D. v. The United Kingdom, Judgment of 2 April 2010, Application no. 28680/06.
ECtHR, Airey v. Ireland, Judgment of 9 October 1979, Series A-32, Application no. 6289/73.
ECtHR, Amann v. Switzerland, Judgment of 16 February 2000, Application no. 27798/95, ECHR 2000-II.
ECtHR, Ashworth and others v. The United Kingdom, Admissibility decision of 20 January 2004, Application no. 39561/98.
ECtHR, Copland v. The United Kingdom, Judgment of 3 April 2007, Application no. 62617/00.
ECtHR, Craxi (no. 2) v. Italy, Judgment of 17 July 2003, Application no. 25337/94.
ECtHR, Dudgeon v. The United Kingdom, Judgment of 22 October 1981, Series A-45, Application no. 7525/76.
ECtHR, Giacomelli v. Italy, Judgment of 2 November 2006, Application no. 59909/00.
ECtHR, Hatton v. The United Kingdom, Judgment of 2 October 2001, Application no. 36 022/97.
ECtHR, Iordachi and others v. Moldova, Judgment of 10 February 2009, Application no. 25198/02.
ECtHR, Liberty and others v. The United Kingdom, Judgment of 1 July 2008, Application no. 58243/00.
ECtHR, Malone v. The United Kingdom, 2 August 1984, Series A-82, Application no. 8691/79.
ECtHR, Messina v. Italy (no. 2), Judgment of 28 September 2000, ECHR 2000-X, Application no. 25498/94.
ECtHR (Grand Chamber), *Hatton v. The United Kingdom*, Judgment of 8 July 2003, Application no. 36022/97.
ECtHR (Third Section), *Hatton v. The United Kingdom*, Judgment of 2 October 2001, Application no. 36022/97.

**US Cases and Legislation**


Index

A
Access Card scheme, 126
Access to information and privacy (ATIP) coordinator, personnel, 162, 421, 465
Accredited Standards Committee (ASC) X9, 307, 314, 319, 486
Alberta Office of the Information and Privacy Commissioner, 7, 29
American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants (AICPA/CICA), 424
ARCI model, 257
Assemblages, 372–373
Assertive scrutiny, 41, 53, 57, 64, 74
Assessable processing, 98, 209
Association of Chief Police Officers (ACPO), 368
Attorney-General’s Department [Australia], 126
Australian Bureau of Statistics (ABS), 126, 156
Australian Communications and Media Authority (ACMA), 128
Australian Government Authentication Framework (AGAF), 126
Australian Government Chief Information Officer (AGCIO), 126
Australian Government Information Management Office (AGIMO), 126
Australian Information Commissioner (OAIC), 6, 122, 144
Australian Law Reform Commission, 126, 129, 143–144, 146, 154
Australian Privacy Foundation, 126–127, 130–131, 133, 138, 147, 157

B
Balancing privacy, 431
Best available techniques (BATs), 357, 480
Better Regulation Commission (BRC), 83–84, 87
Better Regulation Executive (BRE), 83, 85–86, 90–91
Better Regulation Task Force (BRTF), 82–83
Binding Corporate Rules (BCRs), 284
British Standard 10012: 2009, 209, 295
BS 25999, 295
Business continuity management (BCM), 295, 297

C
Cabinet Office Regulatory Impact Unit, 82–83
Cavoukian, Ann, 150, 174, 205
CCTV, 64, 100–101, 109, 208, 368, 370, 372–373, 375
CCTV User Group, 208
Center for Democracy and Technology, 229, 232, 238–240, 243
Centrelink, 123, 126
Certification, 150, 153, 245, 295, 359, 457
Index

F
Facebook, 371
Fair information principles (practices), 21, 134, 379, 436, 473
Federal Data Protection Act (FDPA) [Germany], 277–278
Flaherty, David, 8, 122–123, 150, 243, 246, 418, 437
Freedom of Information (FOI), 23, 106–107, 134, 162, 164, 170, 201, 220, 233, 346, 450, 453, 460
Full-scale PIA, 22, 24, 184, 211, 331, 335, 340, 464, 469, 473
Function creep, 13, 158–160, 201

G
Geotag, 371
Google, 490

I
Immigration Act 2009 [NZ], 18, 23, 192
Impact assessment
  regulatory, 31, 77–96, 400, 418, 450, 453
Impact assessment board [EC], 92, 94
Individual health identifier, 157
Information privacy, 19, 24, 196, 398, 471, 473
Information Privacy Principles (IPPs), 122, 125, 128–131, 133–134, 141, 161, 189–191, 196
Information Security Forum (ISF), 258
Information Systems Audit and Control Association (ISACA), 6, 17, 312, 424
InfoSource, 433
INSEE (French national statistics agency), 100
Intelligence Reform and Terrorism Prevention Act of 2004 [US], 227, 230, 239, 242
Inter Company Agreements (ICA), 280–281
Interface control documents (ICDs), 311
Internal revenue code, 313
Internal Revenue Service, 9, 313
International Conference of Data Protection and Privacy Commissioners, 386, 393, 437–438
International Electrotechnical Commission (IEC), 11–12, 27, 310, 312, 321, 333, 341, 351, 449, 467
International Privacy Principles, 245
International Security, Trust and Privacy Alliance (ISTPA), 310
Internet of Things, 287, 324–325, 345, 401
ISO 14443, 227
ISO 9000:2005, 295
ISO Joint Technical Committee (JTC), 1, 321
ISO Technical Committee (TC), 68, 314

K
Kelly, Nuala O’Connor, 240–242, 245–248
Kroes, Neelie, 5

L
Legislative Council (LegCo) Security Panel [Hong Kong], 158

M
Management Board Secretariat (MBS) [Ontario], 9, 139, 141, 465
Mandelkern Group, 92
Margin of appreciation, 41–42, 57, 59, 65–66, 68, 74
Ministry of Labour and Citizens’ Services [British Colombia], 10
Model applications, 103

N
National Association of Data Protection Officers (NADPO), 207
National Audit Office (NAO) [UK], 82–83, 87–89, 91, 450
National e-Authentication Framework (NeAF), 126
National Environmental Policy Act (NEPA) of 1969 [US], 232, 235–237, 247
National Privacy Principles (NPPs), 128, 131, 147
National strategy to secure cyberspace, 229
“Necessary in a democratic state” test, 54
Necessity test, 55–56, 353
OECD Guidelines, 130, 188, 338, 464, 473
Office for National Statistics (ONS) [UK], 213–216, 219, 469
Office of the Australian Information Commissioner (OAIC), 6, 122, 144
Office of Management and Budget (OMB) [US], 7, 9, 18–22, 24, 30, 77, 226, 228–230, 232, 238, 243
Office of the Privacy Commissioner [New Zealand], 9
Office of the Privacy Commissioner [of Australia], 10
Office of the Privacy Commissioner for Personal Data [Hong Kong], 6, 9
Office of the Privacy Commissioner of Victoria [Australia], 128, 149
Open Europe, 90

Participatory surveillance, 371, 374
Passenger name records (PNR), 4, 113, 458, 461
Payment Card Industry Data Security Standard (PCI DSS), 256, 258, 265
Personal information bank (PIB), 435
Personal Information Protection and Electronic Documents Act (PIPEDA) [Canada], 21, 163
Personally identifiable information (PII), 3, 10, 18–19, 30, 71, 225, 243, 256, 308, 365, 466
PIA consultation group (PCG), 470
PIA process maturity model, 424–425
Privacy Act 1988 [Australia], 125, 135, 143
Privacy Amendment (Private Sector) Act 2000 [Australia], 128
Privacy attributes, 39
Privacy audit, 8, 121, 151–152, 214, 301, 303, 308, 313, 337, 363
Privacy compliance audit, 313
Privacy risk management system (PRMS), 289, 295–303
Privacy Victoria (OVPC), 130, 137–138
Process and Service Descriptions (PSDs), 280–281
Project, 8, 159, 466, 473, 475
Proportionality test, 4, 41–42, 46–47, 53–54, 56, 63, 65–66, 72, 113, 461
Proposed financial system (PFS), 307–313

RACI, 272–273
Radio frequency identification (RFID)
Recommendation, 7, 116, 341, 347–348, 461, 469
Recommendation on RFID, 4, 10, 112, 114, 350, 352, 449
Reding, Viviane, 4
Reducing Regulation Committee (RRC) [UK], 89–90
Regulatory Challenge Unit [UK], 90
Regulatory Policy Committee (RPC), 77, 79, 87–92, 95
Risk Advisory Council [UK], 84
Safer Internet Programme, 294
Security Screening Directive (Alberta), 172
Sensitive information, 14, 26, 28, 55, 165, 170, 286, 300, 332, 352, 389, 470, 473
Small-scale PIA, 211, 331
“Smart” identity card (SMARTIC), 158–159
Spam Act 2003 [Australia], 128
State Services Commission [NZ], 155
Strengths, weaknesses, opportunities and threats (SWOT), 470
Subsidiarity test, 42
SWIFT, 48, 318, 372
System development life cycles (SDLC), 309–312, 314, 321, 463
System of records, 227

T
Telecommunications Act [Australia], 128, 293
Telecommunications Industry Ombudsman (TIO) [Australia], 122, 128
Telecommunications (Interception and Access) Act [Australia], 128
Threshold assessment, 24
Treasury Board of Canada Secretariat, 7–10, 18, 20, 22, 164, 173, 180, 366, 398, 420, 422, 426, 435, 448, 466
Treaty of Maastricht, 92
Treaty of Rome, 92

U
US-VISIT, 227, 238–243, 246, 248