Copyrighted Material

LIST OF CONTRIBUTORS

Orla Lynskey (LLB lingua franca (Dub), LLM (Bruges), PhD (Cantab)), non-practising Barrister-at-Law (Inner Temple) is an Assistant Professor in Law at the London School of Economics where she teaches courses on internet regulation, data protection, and privacy. She studied law at Trinity College Dublin and the College of Europe, Bruges. She holds a PhD in data protection law from the University of Cambridge and was called to the bar at Inner Temple. Prior to entering academia, she worked on antitrust and competition matters at the European Commission and a US law firm in Brussels.

Rosemary Pattenden (BComm, LLB (NSW), DPhil (Oxon)) is Emeritus Professor of Law at the University of East Anglia. She joined the university as a lecturer in 1979 and was promoted to senior lecturer, reader, and finally to professor in 1998. She retired in 2013 and was appointed to an emeritus chair. Rosemary focuses on the law of evidence, criminal appeals and procedure, and the law of confidentiality.

Duncan Sheehan is Professor of Business Law at the University of Leeds. He was previously successively Lecturer and Senior Lecturer in Law and then Professor of Commercial Law at the University of East Anglia where he worked from 2001 to 2015. Duncan's research is in personal property, restitution and breach of confidence.

Richard Stone is Emeritus Professor of Law and Human Rights at Lincoln Law School at the University of Lincoln. He has taught human rights and civil liberties for over thirty-five years, and is the author of *The Law of Entry, Search, and Seizure* (5th edn, OUP 2013) and *Textbook of Civil Liberties and Human Rights* (10th edn, OUP 2014).

http://www.pbookshop.com

Copyrighted Material

Copyrighted Material

1

INTRODUCTION

Duncan Sheehan

http://www.pbookshop.com

The purpose of this book is to examine the legal obligations that professionals owe their clients in respect of confidential information concerning the clients. It is written from the premise that in matters of confidentiality and disclosure of information the same fundamental legal principles apply to all professionals and that any variations in the obligations of different professional groups need to be rationally justified by differences in the nature of the service provided to the client or the information that the professional handles. This chapter will introduce some of the issues raised in the book. We first examine the question of what information or data are and the types that exist. We distinguish information from property and note that information has been equated to property as part of a means to justify confidentiality obligations. The second part of the chapter examines the types of obligation there are and distinguishes privilege, confidence, and privacy, and discusses criminalization. The third part asks who the clients and professionals are, and the fourth looks at disclosure obligations and introduces some of the issues to be covered. **1.01**

The substantive part of the book will first examine different private law causes of action—the wrong of misuse of private information, the related equitable wrong of breach of confidence, and various miscellaneous torts that might be committed. We also look at contractual confidence actions. Because of the overlap with **1.02**

Copyrighted Material

Copyrighted Material

confidence, we examine breaches of fiduciary duty and how some (but not all) professionals may be liable for a breach of fiduciary duty, either because of misuse of information acquired in their professional capacity or because of conflicts between clients where a risk may exist that they will use information for the benefit of a competing client. We examine the private law remedies and selected disciplinary proceedings. The second part of the book mainly examines when disclosure can be justified, or compelled. That includes the question of public interest, which is also relevant to the balancing process under the misuse of private information wrong, but also consent and waiver. Compelled disclosure might be in the course of a trial—for the administration of justice—or in the course of a police or other official investigation. We then examine legal professional privilege, data protection, and public interest immunity, and finally material on collateral use of documents revealed through disclosure, open justice, and restrictions on public reporting of court processes.

A. Information

Information and data

1.03 One important distinction to make at the outset is between information and data. An important sector of the law as it affects professionals is that of data protection, and it is important that it refer to data—not information—protection. Although for the purposes of a breach of confidence or misuse of private information action the distinction is largely blurred, there is a clear distinction. Data are quantitative or qualitative statements or numbers assumed to be factual and not a product of analysis or interpretation. Information is built from data; data are information in latent form,[1] which is yet to be processed.

http://www.pbookshop.com

Types of information: personal, commercial, governmental

1.04 For the purposes of a breach of confidence action, information is 'that which informs, instructs, tells or makes aware'.[2] Information is also a thing.[3] Each piece of information is a definable and ascertainable thing. Information must be ascertainable. In *Corrs Pavey Whiting & Byrne v Collector of Revenue*[4] Gummow J said that the claimant

[1] 'Information can … be conceived of as "data" that has been "processed" in some way': P Roth, 'What is "Personal Information"?' (2002) 20 NZULR 40, 51. The Information Commissioner's Office has produced a booklet, *Determining what Information is Data for the Purposes of the DPA*, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions> (accessed 13 July 2015).

[2] *Commissioner of Police v Ombudsman* [1988] 1 NZLR 385, 402.

[3] R Heverly, 'The Information Semi-Commons' (2003) 18 Berkeley Technology LJ 1127, 1144.

[4] (1987) 14 FCR 434, 443; *FSS Travel v Leisure Systems Ltd* [1999] FSR 505, 512 (Mummery LJ); *Brooks v Olyslager Oms (UK) Ltd* [1999] IRLR 590; *LAC v International Corona Resources* (1989) 148 DLR (4th) 14, 77 (Sopinka J).

Copyrighted Material

Copyrighted Material

must be able to identify with specificity the information in question. Not all information is a thing of value.[5] The fact that the sun is in the sky is not of value to me; everybody else knows it. The confidentiality of the information makes it valuable. Of course, information to be controlled and valuable need not be secret or confidential, but if it is not confidential the rights in the information are of a significantly different character.[6] Absent other defined intellectual property rights such as copyright in the information, its confidentiality and identifiability is critical. That it is identifiable is vital both to the cause of action itself and to the remedy. Things can be traced; if information is a thing, it can be traced and a proprietary remedy made available.[7]

1.05 Personal information is information about an individual or natural person. In common parlance it refers to such things as a person's political and religious beliefs, medical history, mental stability, emotions, sexuality, intimate relationships, genetic makeup, IQ, criminal history, and financial affairs. This is information that the individual can reasonably expect to keep to himself or withhold from others[8] or which, as Wacks puts it, the individual is likely to view as 'intimate or sensitive'.[9] The sensitivity of information depends very much upon the purposes for which it is used.[10] Seen as raw data an individual's name and address are not normally sensitive information, but a list of persons engaged in controversial research involving experimental work on animals[11] or who are thought to be unfit to work with children is. What impact use for a particular purpose has on the sensitivity of information depends upon societal expectations, the personal circumstances of the individual, and that individual's personal sensitivities and culture.[12]

1.06 In *Phillips v News Group Newspapers*[13] Mann J said of confidential commercial information that it need not be information which could be easily sold, or has the same obviously confidential quality as a customer list. It has to be information which relates to commerce (or business) and within that context to have a confidential quality.[14] The following criteria have been suggested. The party claiming confidentiality must believe that the release of the information would be injurious to him or advantageous to another.[15] Commercially sensitive information also comes

http://www.pbookshop.com

[5] JE Penner, *The Idea of Property in Law* (OUP 1997) 111–12.
[6] Copyright, trade mark, patent, etc.
[7] D Sheehan, 'Information, Tracing Remedies and the Remedial Constructive Trust' [2005] RLR 82.
[8] NZ Law Commission, *Privacy: Concepts and Issues* (SP18 2008) paras 2.14–2.22.
[9] R Wacks, *Personal Information: Privacy and the Law* (OUP 1993) 26.
[10] *R (on the application of Robertson) v City of Wakefield Metropolitan Council* [2001] EWHC Admin 915; [2002] 2 WLR 889, [34].
[11] *Imutran v Uncaged Campaigns Ltd* [2001] 2 All ER 385, [8].
[12] P Roth, 'What is "Personal Information"?' (2002) 22 NZULR 40, 42; *Venables v NGN Ltd* [2001] 1 All ER 908.
[13] [2010] EWHC 2952.
[14] ibid [45].
[15] N Moreham, M Warby, and I Christie (eds), *Tugendhat & Christie: The Law of Privacy and the Media* (2nd edn, Sweet & Maxwell 2011) para 4.68; *Thomas Marshall (Exports) Ltd v Guinle* [1979] Ch 227.

Copyrighted Material

Copyrighted Material

in several different varieties, and we examine this in more detail in chapter 4. It could be a client list, or a confidential recipe or work process (which might be patented, or might not). It is information that a corporate body (typically, although it might be an unincorporated business entity) wishes to keep secret so as to allow it to carry on its business. These two categories can overlap in that a sole trader carrying on his business might consider the financial affairs of his business to be personal—they may be transacted through his personal bank account.

1.07 Governmental information relates to any information held by and about the government or another public authority. Much of this is freely accessible. The Freedom of Information Act 2000 allows members of the public to make requests of public authorities for information held about themselves. In *AG v Guardian Newspapers*[16] it was said that the position of the Crown was special and that there needed to be some detriment shown. To the same effect in *Commonwealth of Australia v John Fairfax & Sons*,[17] the Australian government sought injunctions restraining the publication of a book containing alleged secret material relating to the East Timor crisis and the Indonesian invasion in 1975. Mason J held that disclosure of confidential information would only be restrained if it was inimical to the business of government or national security. He said that[18] while it might be sufficient detriment to a private person that disclosure of information would lay his affairs open to discussion and criticism, the same could not be said of the government, particularly in a democracy where open discussion of the government is a public good. It is therefore a necessary condition of relief that the public interest be damaged.

http://www.pbookshop.com

Information and property distinguished

1.08 Property can come in a number of different varieties; however, we commonly use the term as shorthand for private property. The argument has been made that information is property,[19] and historically, as we see in chapter 4, the property justification has been important in explaining confidence. Despite, however, the presence of some property elements, such as information's susceptibility to being bought and sold, other property elements are not present and the property analogy has frequently been misused. The *locus classicus* is *Phipps v Boardman*.[20] That case revolved around the question of whether trustees had misused trust property in buying

[16] [1990] 1 AC 109 (HL); on government information see M Richardson, K Barnett, M Bryan, and M Vranken *Breach of Confidence* (Edward Elgar 2012) 130–36.

[17] (1980) 147 CLR 39.

[18] ibid 52.

[19] AS Weinrib, 'Information and Property' (1988) 39 UTLJ 117; *Suepp v USA* (1980) Sup Ct 763; F Gurry, 'Breach of Confidence' in P Finn (ed), *Essays on Equity* (Butterworths 1985) 110, 122–23 has a list of proprietary parallels. T Aplin, L Bently, P Johnson, and S Malynicz (eds), *Gurry on Breach of Confidence* (2nd edn, OUP 2012) paras 9.74ff. Heverly (n 3) argues information is a particular sort of property, a semi-commons, not private property.

[20] [1967] 2 AC 46.

Copyrighted Material

Copyrighted Material

shares in a company as a result of information acquired as trustees. Their Lordships were split. Lord Hodson, for instance, argued that confidential information could legitimately be regarded as property.[21] Lord Upjohn, in contrast, denied this.[22] He was relied upon in the Court of Appeal in *Douglas v Hello!*[23]

1.09 The analogy with property rights has been taken to extremes. Some commercial cases have suggested that third parties must be dishonest if they are to be liable to the claimant on subsequent revelation of the information.[24] This is similar to the concept of dishonest assistance in a breach of trust. The central case in this area[25] is discussed in *Thomas v Pearce*,[26] and the idea was recently accepted in *ABK Ltd v Foxwell*.[27] Attempts to make analogies with equitable wrongs such as dishonest assistance are conceptually very difficult. It is almost impossible to assist a breach of confidence without knowing the information, which would correspond to receipt. In that case the proper analogy is with knowing receipt, where the test is one of unconscionability.[28] The question of third party liability and the relationship with dishonest assistance is explored further in chapter 6. The application of dishonest assistance mirrors the test where the wrong complained of is that of breach of fiduciary duty.[29]

1.10 There are state-sponsored methods of creating property in the form of copyright, trade marks, and patents.[30] We must treat with some care any suggestion that information that has not been put through this state-sponsored route is property, or that there are property rights in the information.[31] Kohler and Palmer, however, suggest that treating information as property may in some contexts be helpful, although it is not absolutely equivalent with other accepted property assets.[32] Information cannot be stolen.[33] It cannot be converted.[34] These features create problems with seeing information as being property.[35]

http://www.pbookshop.com

[21] ibid 107. See also Lord Goff at 1115.
[22] ibid 127. See Lord Cohen at 102, and Viscount Dilhorne at 89–90.
[23] [2006] WQB 125, [127].
[24] *Thomas v Pearce* [2000] FSR 718.
[25] *Royal Brunei Airlines v Tan* [1995] 2 AC 378.
[26] [2000] FSR 718, 720–22.
[27] [2002] EWHC 9, [82–83].
[28] J Glister and J Lee (eds), *Hanbury and Martin Modern Equity* (20th edn, Sweet & Maxwell 2015) paras 25.013–25.105; *BCCI v Akindele* [2001] Ch 437. Curiously, the heading in *ABK v Foxwell* is 'knowing receipt'.
[29] *Satnam Investments v Dunlop Heywood* [1999] 3 All ER 649, 671.
[30] See generally L Bently and B Sherman, *Intellectual Property* (4th edn, OUP 2014).
[31] *Cadbury Schweppes v FBI Foods* [1999] 1 SCR 142; A Little 'Restitution for Breach of Confidence' [2000] LMCLQ 142.
[32] P Kohler and N Palmer, 'Information as Property' in N Palmer and E McKendrick (eds), *Interests in Goods* (LLP 1998) 1.
[33] ibid 20; *Oxford v Moss* (1978) 68 Cr App R 183; *R v Stewart* [1988] 1 SCR 963.
[34] *R v Stewart* [1988] 1 SCR 963; but see the analogy to conversion drawn in *Seager v Copydex (No 2)* [1969] 1 WLR 809; PBH Birks *An Introduction to the Law of Restitution* (Revised edn, Clarendon Press 1989) 344.
[35] J Lipton, 'Protecting Valuable Commercial Information in the Digital Age: Law, Policy and Practice' (2001) 61 J Technology L and Policy 2.

Copyrighted Material

Copyrighted Material

1.11 Confidential information is excludable. The action of breach of confidence enforces this; however, a property right needs to be exigible against an indefinite group. Smith argues this is not so of confidential information.[36] Property requires rights. In a Hohfeldian sense, if the information is known only to oneself, one may have privileges and powers, but no rights.[37] As more people know the information, the number against whom one has rights becomes larger but can never become indefinite. If it does so the information has ceased to be confidential.[38] Crucially, confidential information cannot be transferred so that the new holder has the same rights as the previous owner. The previous owner still knows the information and so it has not been completely separated from him. Bridge and colleagues discuss the question,[39] arguing that transactions described as sales are actually usually licenses. What is undeniable is that the transferor retains knowledge. The fact that more people know the information has a normative significance. Eventually the information will cease to be confidential.[40] To the extent that rights still inhere in the information they will be indistinguishable from any other intellectual property monopoly. If we see information as being anything that is capable of carrying meaning,[41] it becomes clear that information cannot be per se ownable. The information that the sun is in the sky cannot be owned. This follows naturally from the fact that one person cannot exclude others from the information.[42] Information of this nature cannot be confidential either. Nonetheless, as we see in chapter 7, the fact that information is an identifiable thing means it can be traced and a proprietary remedy awarded where appropriate. Perhaps the best view is that expressed by *Gurry on Breach of Confidence* that the benefit of the confidence obligation as a chose in action is property.[43]

http://www.pbookshop.com

B. Confidentiality Obligations

Confidentiality and privacy distinguished

1.12 We will look in detail at the justifications for confidentiality in chapter 4, but it must be distinguished from privacy which is a related but distinct idea. English law has developed a wrong on misuse of private information which is wider in some respects than confidence, but it has not developed a broader privacy tort.[44] The previous

[36] LD Smith, *The Law of Tracing* (OUP 1997) 368.

[37] See on privileges WN Hohfeld, 'Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1913) 23 Yale LJ 16, 36; P Eleftheriadis, 'The Analysis of Property Rights' (1996) 16 OJLS 31. Contrast A Halpin, 'Hohfeld's Conception: From Eight to Two' [1985] CLJ 435.

[38] Smith (n 36) 369.

[39] M Bridge, L Gullifer, G McMeel, and S Worthington (eds), *The Law of Personal Property* (Sweet & Maxwell 2013) para 25.030.

[40] *Green* v *Folgham* (1823) 1 Sim & St 398, 57 ER 159.

[41] Heverly (n 3) 1149.

[42] M Bridge, *Personal Property Law* (4th edn, Clarendon Press 2015) 3.

[43] Gurry (n 19) para 4.98; T Aplin 'Confidential Information as Property' (2013) 24 King's LJ 172.

[44] *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 AC 406.

Copyrighted Material

Copyrighted Material

taking unwanted photographs or, at least as frequently, by spying on them and taking pictures with long-lens cameras, as happened to the Duchess of Cambridge in September 2012 when *Closer* magazine in France obtained and published topless photographs of her on holiday. Second, the two actions may have different defences in that the defence of public interest in the private information wrong is swallowed largely by the balancing act between articles 8 and 10, informed by the exceptions to privacy allowed in article 8 and the qualifications to article 10. Public interest in its older form may still be of relevance in breach of confidence cases, particularly where commercial information is involved.[46] This is covered in chapter 9 where we also see how different (or similar) the tests are in practice.

1.14 There are many different theoretical justifications and accounts of privacy, covered in further detail in chapter 2. The most famous is probably Warren and Brandeis' conception of the right as one to be 'let alone'.[47] Many notions of privacy rely on notions of control and of excluding the outside world.[48] However, other theorists maintain that privacy is a condition—a state of accessibility to the self.[49] For now the vital point is that privacy should not be equated with secrecy. First, secrecy is relied upon to conceal the truth. It is at least arguable that privacy can be invaded by the circulation of information that is false.[50] The Supreme Court of Canada has said, '[t]he publication of defamatory comments constitutes an invasion of the individual's personal privacy and is an affront to that person's dignity.'[51] Second, it is not only people who have secrets; companies and governments[52] have secrets too. In fact, in law, secrecy is generally associated with the public sphere.[53] Privacy, however, is about the protection of the individual's dignity[54] and personality, and this is entrenched in the article 8 jurisprudence discussed in chapter 2. This means that a company, which cannot feel mental pain, cannot be stripped of dignity. Privacy for a company (if this exists at all) is an intermediate good, not an end in itself.[55] When, as has occasionally happened, a court has intervened to protect a company's privacy,[56] what it has actually done is protect its goodwill.[57] However, the information that an obligation protects need not be personal or intimate. In the business context it may be a trade secret.

http://www.pbookshop.com

[46] As Gurry (n 19) paras 16.59–16.60 points out, the cases on private information show a marked judicial desire to depart from the prior jurisprudence where personal information is at stake.

[47] S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 Harvard L Rev 193, 193.

[48] eg CDL Hunt, 'Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort' (2011) 37 Queen's LJ 167, 181–82.

[49] eg R Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale LJ 421.

[50] Gurry (n 19) paras 5.69–5.72.

[51] *Hill v Church of Scientology of Toronto* [1995] 2 SCR 1130, 1179.

[52] *AG v Jonathan Cape* [1975] 3 All ER 484.

[53] eg Official Secrets Act 1989.

[54] *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63, (2001) 185 ALR 1, [43].

[55] L D'Amato, 'Comment: Professor Posner's Lecture on Privacy' (1978) 12 Georgia L Rev 497, 499–500; see generally chapter 2.

[56] eg *R v BSC, ex p BBC* [2000] 3 All ER 989; see chapter 2.

[57] *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63, (2001) 185 ALR 1, [120–23].

Copyrighted Material

Copyrighted Material

Companies, we will see, ought not to be entitled to privacy, but they are entitled to protect confidential commercial interests. Confidentiality is wider than privacy.

1.15 A third difference is that a secret is always something that is intentionally concealed because disclosure may discredit or otherwise damage the owner of the secret.[58] Privacy may, and often does, protect secrets but it is a state in which A has made some part of himself inaccessible to B because that part of the self is something that A thinks is no concern of B's.[59] Barendt calls this 'social privacy'.[60] Feldman explains, '[w]e all have things we would rather not make accessible to others, from a sense of decency, dignity, or respect for intimacy.'[61]

1.16 Rather than attempt to find an all-embracing definition of privacy, some legal theorists describe the forms that it takes. All of the following in one setting or another have—whether rightly or wrongly is disputed in some cases—been described as aspects of privacy:

1. not to be identified (*anonymity*);[62]
2. not to be subjected to physical interference through, for example, involuntary body searches and drugs testing (*physical or bodily privacy*);[63]
3. freedom from unwanted surveillance by, amongst others, stalkers, paparazzi, busybodies, voyeurs, and agents of the state (*access privacy*);
4. not to have communications monitored or intercepted (*privacy of communications*);
5. not to make known with whom one associates (*relational or associational privacy*);
6. physical space in which to conduct one's personal affairs free from unwanted observation or intrusion (*spatial or territorial privacy*);
7. independence in making decisions about 'quintessentially private' matters such as contraception, abortion, marriage, child rearing, and where to live (*decisional privacy*);
8. control over the collection, storage, retrieval, sharing, and use of personal information (*informational privacy*, which may also encompass data protection, examined in chapter 16).[64]

Directly or indirectly, the goal here is always to prevent unwanted intrusion or circulation of personal information, and this is the division that the

[58] J Wagner DeCew, *In Pursuit of Privacy* (Cornell Press 1997) 48; S Bok, *Secrets: The Ethics of Concealment and Revelation* (OUP 1984) 10.

[59] Wagner DeCew (n 58) 56.

[60] E Barendt, 'Privacy as a Constitutional Right and Value' in PBH Birks (ed), *Privacy and Loyalty* (OUP 1997) 6.

[61] D Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd edn, OUP 2002) 512.

[62] *Valiquette v Gazette* (1991) 8 CCLT (2d) 302.

[63] eg *R v Dyment* (1988) 26 DLR (4th) 399, 514–515; *Henderson v Chief Constable of Fife* 1988 SLT 361, 367.

[64] A Westin, *Privacy and Freedom* (Bodley Head 1967) 7.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

New Zealand Law Commission has made rather than multiplying the types and categorizations of privacy cited above and described in the first edition of this book.[65]

Types of confidentiality obligation

1.17 This book discusses contractual duties of confidentiality and equitable duties arising from a confidentiality relationship or a fiduciary relationship, which can also have confidentiality implications in terms of the construction of information barriers within solicitors' or accountancy firms, for example. As we see in chapter 4, the rationales for fiduciary law and confidence law are such that the principal ought to be able to rely in both cases on the professional not to use or disclose information for his own personal benefit. Some of those confidentiality obligations are derived from article 8 of the ECHR, as mentioned at paragraph 1.18. The right to communicate confidentially with a lawyer is also an aspect of article 6 of the ECHR, which provides for the right to a fair trial. Article 6(1) provides

> In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

In the context of lawyers, the European Court of Human Rights has said that

> [a]n accused's right to communicate with his advocate out of the hearing of a third person is one of the basic requirements of a fair trial in a democratic society … If a lawyer were unable to confer with his client and receive confidential instructions from him without such surveillance, his assistance would lose much of its usefulness.[66]

There are domestic statutory interventions too. The most significant of such intervention is the Data Protection Act 1998, based on a European source—a European Community Directive. There are current moves, discussed in chapter 16, to introduce a reformed European regime by regulation.

1.18 Internationally there are harmonizing measures in specific areas, which include confidentiality requirements, but many are not immediately relevant to professionals except in that they affect the general law. The European Commission proposed, for example, in November 2013 a draft directive on the general protection of trade secrets, and the Council of the EU published its General Approach in May 2014.[67]

[65] NZLC (n 8) para 3.15.
[66] *S v Switzerland* (1991) 14 EHRR 670, 688.
[67] See T Aplin, 'A Critical Evaluation of the Proposed EU Trade Secrets Directive' [2014] IPQ 257.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

Article 7 EU Mediation Directive,[68] however, does have relevance to professionals. It requires mediators to be protected from giving evidence in judicial proceedings, but it seems that because of the lack of mediation privilege in domestic English law, mediation confidences are better protected under the directive than in English law.[69] Article 9 United Nations Commission on International Trade Law (UNCITRAL) Model Law on Conciliation is wider still and binds all the parties to the mediation process to keep all information relating to the proceedings confidential, except as compelled under the law or to implement the agreement.[70] These obligations are qualified by public interest defences, discussed in chapter 9, and by statutory obligations to divulge information—either for the purposes of criminal investigation, or other purposes.[71]

1.19 In law there is also an obligation not to disseminate false personal information that is injurious to another; this is the province of defamation—although as we see in chapter 5, the relationship between privacy, confidence, and defamation has become more complex with the suggestion that truth should not necessarily be a defence to defamation, and the possibility that falsehoods could give rise to a claim in misuse of private information.

1.20 Legal professional privilege is the name given to an area of law that permits a demand for information to be refused,[72] and this is covered in chapter 15. Unlike confidence law, to which it is related in that it is usually said that privileged information must be confidential, it only operates as a shield. Traditionally it allows lawyers to withhold information from the other side and keep back communications that are relevant to the litigation at hand. Such privileges are not available to other professionals such as accountants or journalists. It is not, however, a rule of admissibility. Should a privileged communication—and it is communications and documents that are protected, not information per se—fall into the hands of another, equitable remedies to protect confidences need to be used to enjoin the use of the material. The relationship between privilege and confidence is therefore relevant to chapter 6 on remedies in confidence against third parties.

1.21 A professional may also be subject to professional codes of ethics, but there are some marked differences between the different codes. Some of these are discussed—along with disciplinary sanctions for their breach by the relevant professional bodies—in chapter 8. What a code says about privacy or confidentiality, if relevant,

[68] Directive 2008/52/EC; for comment on the possible gap in protection this leaves see E-M Henke, 'Confidentiality in the Model Law and European Mediation Directive' (GRIN, 2009) 33–34; the directive is implemented in the UK by Cross-Border Mediation (EU Directive) Regulations 2011.

[69] M Bartlet, 'Mediation Secrets in the Shadow of the Law' (2015) 34 CJQ 112; mediation is not covered in detail by this book.

[70] Henke (n 68) 39–40.

[71] Criminal investigations and police powers are covered in chapter 11; See also eg Health and Social Care Act 2012, ss 253–255 giving the Health and Social Care Information Centre power to demand and store confidential information.

[72] See B Thanki, *The Law of Privilege* (2nd edn, OUP 2011).

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

will be taken into account by courts. The Press Complaints Commission Code of Conduct—the terms of which remain the same after the Independent Press Standards Organisation took over in September 2014—have been examined in a number of cases, and this may be relevant where a professional provides information to the press inappropriately or the press somehow intercepts the information.[73]

1.22 Breach of the professional rules may be relevant to the question whether the professional has fallen below the standard of care required by the law in deciding on questions of whether the professional has been negligent in failing to keep the information confidential. In *Harvest Trucking v Davis*[74] Diamond J made useful reference to the Code of Practice of the British Insurance Association in determining whether the intermediary had acted negligently. The code may not be conclusive, however, as demonstrated by the rather more equivocal comments in *Johnson v Bingley*.[75] There are other types of soft law. There is, for example, a large body of guidance in the form of circulars, codes of practice, recommendations, and reports. This may be particularly true in the healthcare setting where, for example, the Department of Health, British Medical Association, and General Medical Council all have issued guidance; and in data protection law, where the Information Commissioner has issued significant guidance. For the most part such guidance has no legal status, but in practice it will be closely followed by public sector professionals because failure to do so will be a breach of their terms of employment and possible non-compliance with administrative law duties. Beyond the public sector, government guidance may set standards of reasonable conduct, but if the guidance is at variance with professional bodies' requirements the individual will have a serious problem. Equally it is important in multidisciplinary teams that the different professional bodies have complementary and not conflicting confidentiality guidance.[76] Recently, in the context of the health service, questions about how confidentiality and information sharing should work within such teams was explored as part of a review chaired by Fiona Caldicott,[77] which came up with a revised list of so-called Caldicott Principles:[78]

1. The use of confidential data needs to be clearly defined and scrutinized
2. Personal data should not be used unless absolutely necessary
3. Only the minimum necessary personal data should be used

[73] See eg *TSE v NGN Ltd* [2011] EWHC 1308, [22] (Tugendhat J); *AAA v Associated Newspapers* [2012] EWHC 2103, [2013] EMLR 2, [54–56] (Nicola Davies J), and upheld [2013] EWCA Civ 554; *Weller v Associated Newspapers* [2014] EWHC 1163, [55–58] (Dingemans J).

[74] [1991] 2 Lloyds Rep 638.

[75] [1997] PNLR 392.

[76] See P Moodie and M Wright, 'Confidentiality, Codes and Courts: An Examination of the Significance of Professional Guidelines on Medical Ethics in Determining the Legal Limits of Confidentiality' (2000) 29 Anglo-American L Rev 39, 62.

[77] Department of Health *Information: To Share or not to Share: The Information Governance Review* (2013).

[78] ibid 20–21.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

Information Commissioner's Office (ICO) states, difficult to see what use data could be put to that would not count as data processing.[85]

1.24 Processing is defined in section 1(1) of the Data Protection Act 1998 as:

> obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:
> (a) organization, adaptation, or alteration of the information or data;
> (b) retrieval, consultation, or use of the information or data;
> (c) disclosure of the information or data by transmission, dissemination, or otherwise making available; or
> (d) alignment, combination, blocking, erasure, or destruction of the information or data.

The use of client-provided information about their finances, for example, to choose appropriate financial investments by an independent financial adviser would involve processing. That processing must be undertaken fairly and lawfully under the first data protection principle, and we examine this and the other data protection principles in chapter 16. Part of the requirement of lawfulness is that the processing not be a breach of confidence, the Human Rights Act, or copyright. The ICO uses the example of medical and banking information as cases where privacy and confidentiality would be expected.[86]

1.25 A proposed European regulation on data protection[87] is currently being developed. This was first announced in January 2012[88] and by proposing a regulation rather than a directive the legislation would be directly effective rather than requiring transposition into national law. The difficulty which the European Commission identified was that although the data protection directive in 1995 was adopted partly as a means of aiding the development of the single market, it had been transposed and enforced differently in different countries so the level of harmonization desired had not been achieved. A regulation would achieve that aim, as well as allowing for updates and changes to the law to reflect changing technologies and expectations.

1.26 Data protection legislation is increasingly important. Indeed, some might consider it the primary means by which information is protected in the modern world; but it is not completely comprehensive. There is, for example, a distinction between information and data. One such distinction is that personal data are by definition in a record. The Act does not seek to control the disclosure of information from

[85] ICO *The Guide to Data Protection* (2010) 25.
[86] ibid 51.
[87] See for discussion eg G Voss, 'One Year and Loads of Data On: An Update on the Proposed EU General Data Protection Regulation' (2013) 16 Journal of Internet Law 1; M Rotenberg and D Jacobs, 'Updating the Law of Information Privacy: The New Framework of the European Union' (2013) 36 Harvard J of Law and Policy 605. This is discussed in detail in chapter 16.
[88] <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm> (accessed 13 July 2015).

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

memory or regulate visual or aural surveillance unless the fruits of the surveillance are reduced to a form that can be processed. Even the coverage of personal data is not total: the definition of personal data does not include every kind of record[89] and anything recorded for domestic purposes falls outside the Act.[90]

The interplay with confidentiality obligations is complex. Currently Data Protection Act 1998 section 1 requires the data to be of living persons, although misuse of private information and professional ethical guidelines may require some degree of post-mortem confidentiality; lapse of confidentiality post-mortem is dealt with in chapter 14. **1.27**

The impact of new technologies

New electronic technologies and the scope they provide for larger and larger databases of information provide significant challenges for professionals and the way in which they work. This began before the publication of the first edition of this book[91] but has mushroomed in the past decade with more and more information being stored online and on databases. It is this trend more than any other that has led to the increasing importance of data protection regimes, and the need for such regimes so far as possible to be technology neutral, so that they do not become significantly outdated quickly as technology develops. In addition, it creates issues for legal professionals in terms, for instance, of the sheer volume of data that might be subject to disclosure in litigation. **1.28**

In the medical context there is a trend to larger and larger databanks. The UK biobank[92] initiative, for example, is a major national health resource and a registered charity. It aims to improve the prevention, diagnosis, and treatment of a wide range of illnesses, such as cancer, heart disease, diabetes, and forms of dementia. The biobank recruited 500,000 people aged between 40 and 69 years from 2006 to 2010 to take part. They provided blood, urine, and saliva samples for future analysis, detailed information about themselves, and they agreed to have their health followed and recorded. The National Health Service (NHS) has also sought to develop a national computer system with the aim of replacing paper medical records with a centralized national electronic database, allowing a patient from Norwich to walk into a hospital in York, for example, and find all their details ready at the click of a button. After the project was abandoned amid some acrimony regarding the cost, comments online in a newspaper[93] argued that its abandonment was welcome because of the number of people in the NHS who **1.29**

[89] Data Protection Act 1998, s 1(1).

[90] ibid s 36.

[91] See eg A Vedder, 'Medical Data, New Information Technologies and the Need for Normative Principles other than Privacy' in M Freeman and A Lewis (eds), *Law and Medicine* (OUP 2000) 441.

[92] See <http://www.ukbiobank.ac.uk> (accessed 13 July 2015).

[93] <http://www.theguardian.com/commentisfree/2011/aug/03/nhs-database-digital-disaster> (accessed 13 July 2015).

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

would have access to a patient's medical records, and the consequent opportunities for breach of privacy or confidentiality. The potential for computer hackers to change someone's medical records was also highlighted, and there have been significant data security issues with other large medical databanks[94] which may give rise to liability under the Data Protection Act 1998, on which see chapter 16. Banks also keep large databases of their customers' finances and transactional history and use this to facilitate Internet banking services, where customers are able to pay bills, set up standing orders and direct debits, and view their transactions online, and there have also been significant issues regarding data security relating to bank databases, such as the theft of data on 27,000 Barclays customers in February 2014.[95]

1.30 On a smaller scale, solicitors and other business professionals keep databases of records about their clients. The American Bar Association adopted in 2012 a model rule that requires attorneys to keep abreast of modern technological developments, including therefore threats to privacy and confidentiality.[96] Indeed, because of the cost of large servers and storage, many organizations are moving to so-called cloud computing networks where software is downloaded that enables the solicitor or other professional to access their material stored on someone else's computer and to access it across the Internet; indeed, this is becoming an everyday occurrence for many of us. Three categories of public cloud computing have been identified:[97]

1. Software as a service: providers offer finished applications (Google™ documents) and data storage. All the user needs is a device with a web browser
2. Platform as a service: again, there is no control over infrastructure but the user can develop his own applications
3. Infrastructure as a service: this allows the user to deploy their own operating systems and configure processing and storage facilities

All, however, provide processing and storage. Customers are often reluctant to abandon their entire network and so may use the network to provide overflow capacity, but smaller firms without big economies may well obtain substantial savings. It is also possible to have private cloud computing where the data are protected by a corporate firewall. It is not merely businesses who make use of the cloud, however. Considerable amounts of medical information—often in the hands of pharmaceutical companies—are placed in the cloud and are extraordinarily useful in healthcare research.[98]

[94] See also B Lo and L Parham, 'The Impact of Web 2.0 on the Doctor–Patient Relationship' (2010) 38 J Law, Medicine and Ethics 17.

[95] <http://www.bbc.co.uk/news/uk-26106138> (accessed 13 July 2015).

[96] ABA Model Rule 1.1, Comment 8.

[97] CS Yoo, 'The Changing Patterns of Internet Usage' (2012) 63 Federal Communications LJ 67, 83.

[98] PM Schwartz, 'Information Privacy in the Cloud' (2013) 161 U Penn LR 1623, 1631–32.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

1.31 Cloud computing still raises security concerns, though, because of the relatively open way that information is transmitted and the possibility for interception of the material, although email routing is often handled differently from data routing under cloud computing in ways said to make the latter more secure.[99] Lawyers in the United States of America (US) have been advised not to send emails to clients' work addresses because the employer may access those emails, for example, and to be wary of cloud-computing networks.[100] Even personal accounts may be seen by employers if accessed from work because attachments may be saved as temporary Internet files on the employer's system. At the very least, lawyers and other such professionals should draw the client's attention to the dangers inherent in electronic communication and the potential lack of privacy as a waiver to possible liability. There is, as we see, a reasonable expectation of privacy with regard to emails, but sensitivity is high and particularly sensitive material should be encrypted.[101] Some NHS services will not normally use email to send test results, although the Caldicott Review of 2013 suggests that if informed consent has been given, information can be sent electronically.[102] Encryption or password protection may only be a partial solution, although it does show that the information contained is intended to be private and confidential; it is also necessary to protect the devices used to connect to the Internet, including mobile devices such as tablets and smartphones. Allen argues that one should never use an unsecure network because everyone else on the network has access to that device.[103]

1.32 There are a number of complications with cloud computing. One is that the law applicable to the data is not necessarily the law one expects, and different countries have different laws. This arises because the server on which the data are stored need not be in the same jurisdiction as the user. This leads to questions about jurisdiction[104] and applicable law. This book primarily concerns English law and is not about the conflicts of law position. Some comment is in order, however. The prima facie position within the EU, as discussed in chapter 16, is that transfer of

http://www.pbookshop.com

[99] Yoo (n 97) 85; on cloud computing see also M Wittow, 'Cloud Computing: Recent Cases and Anticipating New Claims' (2011) 28 The Computer & Internet Lawyer 18; F Wilson and O Bray, 'EU Data Protection Regulators and Cloud Computing Contracts' (2013) 16 Journal of Internet Law 18.

[100] K Crews, 'E-Filing from the Local Coffee Shop: A Practical Look at Confidentiality, Technology and the Practice of Law' (2013) 87 Florida Bar Rev 89; for other practical tips to lawyers see J Allen and A Hallene, 'Protecting your Data in Cyberspace' (2013) 27 Am J Family Law 198; for a more academic treatment see R Bolin, 'Risky Mail: Concerns in Confidential Client–Attorney Email' (2012) 81 U Cincinnati L Rev 601.

[101] L Hill, 'Emerging Technology and Client Confidentiality: How Changing Technology brings Ethical Dilemmas' (2010) 16 Boston University Journal of Science and Technology Law 1.

[102] DoH (n 77) 30; see also D Joseph and M Goldstein, 'Confidentiality' in S Bloch, P Chodoff, and S Green (eds), *Psychiatric Ethics* (4th edn, OUP 2009) 177, 180–81; for more detail on informed consent see chapter 13.

[103] J Allen, 'Data Security in a Mobile World' (2010) 27 GP Solo 4.

[104] Addressed in *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, where the question was whether the claimants could serve out of the jurisdiction.

Copyrighted Material

Copyrighted Material

personal data outside the European Economic Area is forbidden unless certain conditions are met,[105] and this has led, for example, to the EU–US Safe Harbour Arrangement that allow US companies to certify that they hold data in such a way as to satisfy EU law, although the effectiveness of the arrangement has been questioned by Rotenberg and Jacobs.[106] The European Commission argues that the new proposed data protection regulation will help as trust in the EU's coherent regulatory framework will be an important point for investors and a key asset; it will also be clearer whether those providing the cloud-computing services—as opposed to those making use of them—are data controllers, with rather more extensive obligations, or data processors.[107] That said, Schwartz questions the efficacy of national (or regional) regulation, noting the truly international way in which data are processed in the cloud, as a result of the distributed nature of the computing environment.[108]

Criminalization of breaches of confidentiality

1.33 This book is largely, but not exclusively, concerned with private law obligations. Some European jurisdictions, however, criminalize breaches of professional secrecy. In France and Germany, for example, an unjustified disclosure by a professional can lead to a criminal fine.[109] There have also been moves at EU level to criminalize breaches of trade secret law, although the particular proposals discussed by Cornish, Llewellyn, and Aplin was withdrawn by the European Commission in 2010,[110] and the current proposals on trade secret protection do not affect the criminal law of the member states.

1.34 English law does not routinely criminalize breaches of confidentiality or privacy, although there are some offences that may be committed under data protection legislation and the Information Commissioner is empowered to take enforcement action against such breaches.[111] The Law Commission provisionally recommended that there be a criminal offence of unauthorized use or disclosure of a trade secret by analogy with theft.[112] However, this proposal was never taken up, and it is difficult

http://www.pbookshop.com

[105] Data Protection Directive, arts 25–26.

[106] Rotenberg and Jacobs (n 87) 637–40.

[107] Schwartz (n 98) 1641; see also W Kuan Hon, J Hörnle, and C Millard, 'Data Protection Jurisdiction and Cloud Computing: When are Cloud Users and Providers subject to EU Data Protection Law? The Cloud of Unknowing' (2012) 26 Intl Review of Law, Computers and Technology 129.

[108] Schwartz (n 98) 1629.

[109] Art 226-13 French Criminal Code; arts 201–202 StGB; arts 185–186 StGB criminalize defamation, discussed in S Michalowski 'Medical Confidentiality and Medical Privilege—A Comparison of French and German Law' (1998) 5 European J Health Law 89, 89–92. The German criminal offence is more general and does not just cover professionals. See also art 465 Belgian Criminal Code.

[110] T Aplin, WR Cornish, and D Llewellyn (eds), *Cornish, Llewellyn and Aplin: Intellectual Property Law* (7th edn, Sweet & Maxwell 2010) para 8.56.

[111] Data Protection Act 1998, s 40.

[112] Law Commission, *Legislating the Criminal Code: Misuse of Trade Secrets* (Law Comm CP no 150 1997) paras 3.60–3.61.

Copyrighted Material

Copyrighted Material

The first is that a person commits an offence when he fails to comply with an enforcement order issued when the Information Commissioner believes the data controller to have breached one of the data protection principles. This offence has, however, very rarely been prosecuted, and counts as a second order response as the actual enforcement order is the first remedy.[119] The second offence under section 47 is committed by knowingly or recklessly providing false information in response to an information notice.[120] Section 55 of the Act provides for an offence of knowingly or recklessly without the data controller's consent obtaining, disclosing, or procuring the disclosure of personal data. The fact that data protection legislation is backed up by these criminal sanctions suggests that we wish to censure breaches of personal privacy and data protection. Data protection legislation is aimed at a broader group of people than merely professionals. Indeed, the consequences of data security breaches may well be more serious now than when the data protection directive was promulgated, and this explains the need to censure such activity. Where previously a data breach might disclose a user's address, or at worst credit card information, now a data breach might compromise all their personal information. Often the end result is identity theft.[121]

1.38 Where the professional is in the public sector and discloses information, the common law offence of misfeasance in public office may be committed. The elements of the offence are set out in *Re AG's Reference (No 3) of 2003*.[122] The offence is committed when a public officer acting as such wilfully neglects to perform his duty or wilfully misconducts himself to such a degree as to amount to an abuse of the public's trust in the office holder without reasonable excuse or justification. There will be a question whether a professional acts as a public officer, but it is likely that if the professional is acting in an investigative capacity—for example, a forensic accountant working for the Competition and Markets Authority or the National Crime Agency, or a judicial or quasi-judicial role, for example magistrates' clerk, who will be a qualified solicitor or barrister—he will count as a public officer.

1.39 In most cases there is a professional body with the power to censure and to take disciplinary proceedings. It is hard to see the merit in adding another mode of censure, particularly when the professional may be liable to a penalty for breach of data protection law as well as subject to civil liability under confidence or private information law. The New Zealand Law Commission has identified that the criminal

[119] R Jay, *Data Protection Law and Practice* (4th edn, Sweet & Maxwell 2012) paras 21.13–21.14.

[120] An information notice requires a party to provide information to enable the information commissioner to assess whether he, as a data controller, is complying with the data protection principles. See ibid paras 20.19–20.21.

[121] Rotenberg and Jacobs (n 87) 626.

[122] [2004] EWCA Crim 868, [2005] QB 73; in the context of a police officer obtaining and disclosing confidential information from the Police National Computer see *Re AG's Reference No 1 of 2007* [2007] EWCA Crim 760, [2007] 2 Cr App R (S) 86.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

offences that exist mainly protect information on the basis of how or why it was obtained.[123] There is no policy of rendering criminal the disclosure of information just because it is private or confidential. The New Zealand Legislation Advisory Committee, in a paper discussed by the New Zealand Law Commission,[124] suggests a number of questions:

— Will the conduct cause substantial harm to individual or public interests?
— Is public opinion supportive of criminal sanctions?
— Is the conduct best regulated by the criminal law, or are civil law remedies more appropriate?
— Is criminal law simply a 'convenient' tool for tackling the issue?
— How will enforcement and prosecution take place?

It is difficult on the basis of these questions to support a general privacy crime or a specific crime directed at professionals. Civil law and professional disciplinary remedies, dealt with in chapter 8, seem adequate and it is doubtful that public opinion demands a new crime.

C. Who Are the Parties?

Who owes the duty?

Who is the professional?

Professionals come in many different guises.[125] The most obvious might include: solicitors, barristers, accountants, financial advisers, auditors, valuers, quantity surveyors, bankers, and investment bankers; but there are also healthcare professionals—doctors, nurses, psychiatrists, dentists, and others. Professionals are usually engaged by the client not as employees, although increasingly there are in-house professionals who have only one client, their employer. **1.40**

Some professionals, such as doctors, social workers, and teachers, are invariably or almost invariably employed—by a school, hospital, or a local authority. Their clients are not so much their employer but instead those they are presented with in the course of their employment. This will equally be so of what we might call business professionals such as solicitors or accountants who are typically organized in firms of varying sizes and complexity. However, there is often an ideal of service to others embedded in the professional culture of the sector. Professionals are usually required to have degree-level education and a professional training **1.41**

[123] NZLC (n 116) para 7.47; for a summary of the various criminal offences in New Zealand law see paras 2.121–2.162.
[124] ibid para 5.49.
[125] There is very little literature, but see SL Buhai, 'Profession: A Definition' (2012) 40 Fordham Urban LJ 241.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

and accreditation from a professional body, such as the Law Society (Solicitors Regulation Authority), or General Medical Council (GMC), and frequently continuing education requirements. This disparity in knowledge between the client and professional requires that the former trust the latter and for the latter to have an ethos that puts someone else's interests before their own. The previous edition of this work suggested that the existence of such a self-governing regulatory body was not decisive, and indeed it is not. Teachers, for example, have traditionally not had such a body; the General Teaching Council existed for a period but was abolished in 2012. Some of its functions are now carried out by an agency of the Department of Education. The GMC, by contrast, is wholly independent of the DoH, but this does not make teaching any less of a profession whose members have confidential information about their pupils.

1.42 There is significant discussion in this book about the position of journalists. Journalists are in a slightly unusual position in that they do not have clients as such, although they are frequently considered members of a profession and there is, for example, a code of conduct to which they are professionally obliged to adhere.[126] This justifies their treatment in this book. The information they are given is usually provided to them with a view to its contributing to a published story. What is confidential, however, is the identity of the source.[126] This means that the journalist and (if he is not freelance) the media organization for which he works are often third parties and their liability as third parties is covered in chapter 6, although they might also be liable for misuse of private information covered in chapter 2, for example. Sometimes, and we look at this particularly in chapter 12, a person to whom the information relates will seek to discover what information the journalist holds and the identity of the source, who may be a professional or a person working for the professional. Although this might be relevant to criminal investigating authorities, the case law is almost exclusively in the civil law context and so it is largely omitted from chapter 11.

http://www.pbookshop.com

1.43 **Third Parties** As alluded to above, it is not just professionals who owe a confidentiality duty. Professionals' employees who might not themselves be professionals in the sense used in this book nonetheless must observe the same confidentiality obligations and this will be guaranteed by their contracts of employment. If they did not have such obligations, the clients' protection would be seriously compromised; it makes no difference after all from their perspective whether a solicitor or a receptionist publishes confidential information.

1.44 As we will see in chapter 6, interceptors of information and third party recipients aware of the confidentiality of the information will also be held liable in given circumstances. There are groups and bodies who will not be interceptors, third parties,

[126] National Union of Journalists *Code of Conduct* (2011) cl 7; see also Independent Press Standards Organisation *Editors' Code of Conduct* (2014) cl 14. This is the same as the old (now disbanded) Press Complaints Commission code.

Copyrighted Material

Copyrighted Material

or strangers, who may be, by virtue of being entrusted with the information by a professional, subject to data protection rules even if their lack of conscious knowledge of what the data they store amounts to means that they cannot be liable in misuse of private information or confidence. These bodies will be data processors even if they are not classified as data controllers. They may also be liable in negligence, where data security breaches occur.

Who is owed the duty? Clients and 'examinees'

1.45 A client, for the purposes of this book, is the individual whom the professional most immediately serves; this may be because the client employs the professional via an employment contract or because he has engaged their services. Payment by the client is not necessary. Sometimes the state makes the services of a professional available free of charge to the end user (as in the case of the NHS, local authority social services, and state education); at other times, a private sector third party such as an employer foots the bill. Sometimes a third party may engage the professional. The previous edition of this book stated that there were two categories of case.[127]

1.46 The first category is where the third party engages the professional to serve the examinee's interests. Examples include:

1. the doctor retained to treat a child by a parent;
2. the nurse employed by the occupier of premises to attend to persons injured on those premises.

In the first example, the parent has a say about what the professional does and a right to information from the professional, but it is the child who is the true client. If the interests of parent and child clash, the professional must promote the child's best interests. In the second example, the injured person is at liberty to decline the professional's assistance but if that assistance is accepted he is entitled to the same duty of confidentiality as if he hired the nurse himself. The position is more complicated in the case of indemnity insurance if the insurer has a contractual right under the insurance policy to choose the solicitor who acts for the insured and an absolute right to control the conduct of proceedings under the retainer. In these circumstances the insurer's interests will prevail over those of the insured, and in the event of a serious conflict of interest between the insurer and the insured about the disclosure of information, the only course the solicitor can properly pursue is to stop acting for the insured.[128]

[127] For a discussion about the complexities of determining who the social work client is see M Davies, *The Essential Social Worker* (3rd edn, Ashgate 1994) ch 10.

[128] *Groom v Crocker* [1938] 2 All ER 394.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

1.47 The second category is where the third party engages the professional for his own benefit. Particularly in the case of doctors, the true client may be the third party who engaged the professional and not the person examined (the examinee). The GMC refers to doctors with 'dual obligations'.[129] Examples include:

1. the consultant forensic psychiatrist engaged by a court or the Parole Board to form an objective opinion about a defendant's mental state;
2. the psychiatrist asked by local authority social services to assess whether a child has been subjected to sexual abuse;[130]
3. an occupational health professional who carries out a pre-employment health check for a prospective employer;[131]
4. the doctor who examines a personal injury claimant for an insurance company.

As there is no intention to provide a service to the examinee, the professional has no professional relationship with the examinee who has no reasonable expectations of confidentiality vis-à-vis the particular third party,[132] although of course he does so as against other third parties. At the outset of the examination, the professional should tell the examinee that normal rules of confidentiality do not apply,[133] and that he must consent to being seen on this basis. The GMC in its guidance says that only directly relevant information should be disclosed, although in some cases the whole health record may need to be disclosed to government departments in the context of claims for benefits. Solicitors may need to see the whole record to assess relevance for the purposes of litigation. The guidance though is clear that the solicitor, and not the doctor, explains to the patient that he or she needs to see the whole of the medical record.[134]

1.48 Whether such consent can be said to be genuine is a question considered in chapter 13. This though is vital in clinical settings because it is common for examinees to assume that what they say will be treated by the doctor as confidential.[135] The professional should also state that the information will not be used or disclosed for any purpose inconsistent with the purpose of the examination without the examinee's consent unless this is either compelled or permitted by law; for example, where disclosure is in the public interest.[136]

[129] General Medical Council, *Confidentiality: Disclosing Information for Insurance, Employment and Similar Purposes* (2009) para 2; for the general rules see ibid paras 7, 33–35.

[130] *X v Bedfordshire CC* [1995] 3 All ER 353.

[131] *Baker v Kaye* (1996) 39 BMLR 12.

[132] *R v Smith* (1979) 69 Cr App R 378, 384; *Farnsworth v Hammersmith and Fulham LBC* [2000] IRLR 691, [20].

[133] T Gutheil, 'Ethics and Forensic Psychiatry' in S Bloch, P Chodoff, and S Green (eds), *Psychiatric Ethics* (4th edn, OUP 2009) 465. *R v Gayle* [1994] Crim LR 679; *Farnsworth v Hammersmith and Fulham LBC* [2000] IRLR 691, [20]; *R v Davies* [2002] EWCA Crim 85, [33].

[134] GMC (n 129), para 7.

[135] K Rix, 'Privilege and the Prison Inmate Medical Record' (2000) 11 J Forensic Psychiatry 654.

[136] Discussed in chapter 9.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

D. Compulsory Disclosure

1.51 There is now a considerable miscellany of legislation that allows obligations of professional confidentiality to be ignored by officials who need access to information either about a client or about a professional. Major pieces of legislation include the Police and Criminal Evidence Act 1984, which governs police powers of search and seizure, and the Regulation of Investigatory Powers Act 2000, which makes provision for intrusive and directed surveillance and interception of communications by public officials; both pieces of legislation and official powers to seize or use legally privileged or confidential material in the course of an investigation are discussed in chapter 11. Chapter 11 examines police powers to search for and seize documents, the different procedures adopted, and which classes of information and documentation can or cannot be seized and used. It also looks at surveillance powers, and powers granted to, for example, Her Majesty's Revenue and Customs under the Taxes Management Act 1970, and the Secretary of State under the Companies Act 1985. A general survey of powers to require information to be produced and the patterns that they fall into can be found in chapter 10.

1.52 Examples, however, include the GMC's power to force a medical practitioner who is not herself under investigation or 'any other person' to supply information or produce documents to assist the Council or any of its committees, to carry out its functions in respect of professional conduct, professional performance, or fitness to practise.[145] There are exemptions for information that would not have to be disclosed to a court in civil proceedings[146] and information the disclosure of which 'is prohibited … under any other enactment'.[147] Section 20BA of the Taxes Management Act 1970 permits an order to be made by a 'judicial authority' to require documents to be produced where there are reasonable grounds of suspicion that an offence of tax fraud has been, is being, or will be committed. Statutory reporting requirements oblige the professional in some cases to pass on information without a specific request. Reporting obligations are a feature of the medical profession. Under legislation that can be traced back to the nineteenth century, doctors have an obligation to report food poisoning and thirty diseases or disease groups including cholera, plague, TB, measles, mumps, acute meningitis, and smallpox.[148]

1.53 For the purposes of this chapter, the details are relatively unimportant as they will be dealt with in later chapters. What is important is the effect on confidentiality. The previous edition of this book quoted Benn in the *Australian Law Journal*, who said,

[145] Medical Act 1983, s 35A(1). Medical information may also have to be produced under the Health and Social Care Act 2012 to the Health and Social Care Information Centre.
[146] ibid s 35A(6).
[147] ibid s 35A(4).
[148] See GMC (n 129).

Copyrighted Material

Copyrighted Material

> In any given instance, the public interest will seem overriding; yet in the long run protection of the interest of every individual in privacy will have gone by default; the piecemeal erosion of the privilege may never have been halted, to take an overall view of the total consequences. In this respect privacy resembles environmental values; the particular damage rarely seems sufficient to outweigh the promised benefits, but the cumulative consequences may be disastrous.[149]

This is true and provides a warning, but too much can be made of this. Balancing is at the heart of the approach to the law in privacy where the courts apply an intense focus to balance the rights and interests at stake under articles 8 and 10. The need to balance privacy and the public interest in justifying these powers is therefore nothing new. Indeed, in modern law the right to respect for privacy can provide a trump for those subjected to demands for information under these statutory requirements. A professional should never surrender confidential information until and unless required to do so. The consequences of voluntarily divulging confidential client information would at the very least be to damage the relationship with the client, even were legal or professional disciplinary consequences not to follow. If the professional is required to do so, the client then has a choice whether to challenge the requirement or not.

1.54 In this situation, one possibility is simply to say that the public or other authority has simply overstepped its powers, but more interestingly for our purposes the client may wish to argue that the power used is incompatible with the ECHR. The court in these cases has power where the provision is in primary statutory form, and where the court cannot under section 3 Human Rights Act 1998 find a compatible interpretation, to issue a declaration of incompatibility under section 4. It cannot strike down primary legislation, but the executive's and Parliament's reaction has tended to be positive to declarations under section 4, as Cram observes.[150] Parliament has as a result of such declarations repealed or amended statutes and in some cases *ex gratia* compensation schemes have been set up. Some cases have involved article 8 rights; for example, *R (on the application of CG) v Commissioner of Police for the Metropolis*,[151] which concerned the right of police to keep DNA evidence indefinitely of those arrested. The Supreme Court decided that section 64(1A) Police and Criminal Evidence Act 1984 could be read compatibly with the ECHR and decided not to issue a declaration of incompatibility, because the section need not be read so as to require indefinite retention; the European Court reversed this, holding the provision was incompatible with article 8. Clients can therefore have some confidence that courts will seek robustly to uphold their article 8 rights when faced with challenges to the legality of orders

http://www.pbookshop.com

[149] S Benn, 'The Protection and Limitation of Privacy' (1978) 52 ALJ 686, 691.

[150] I Cram, 'Judging Rights in the United Kingdom: the Human Rights Act and the new Relationship between Parliament and the Courts' (2006) 12 Review of Constitutional Studies 53, 77; see more recently on courts' interpretation of statutes to be human rights-compliant C Crawford, 'Dialogue and Rights: Compatible Interpretations under Section 3 Human Rights Act 1998' (2014) 25 KLJ 34.

[151] [2011] UKSC 21, [2011] 1 WLR 1230.

Copyrighted Material

Copyrighted Material

to produce documentation containing confidential information, although challenges have not always been successful. In some cases article 6 may also be engaged and legal professional privilege, as we will see in chapter 15, is in part a way of creating equality of arms between the parties by encouraging candour with a party's legal representative. *R v A*[152] is an example of a case where incompatibility with article 6 was argued. It was argued that section 41 of the Youth and Criminal Justice Act 1999 precluded a fair trial by prohibiting a defendant from questioning a rape complainant about her previous sexual history—in particular, previous consensual sex with the defendant himself. The House of Lords, using section 3, read into the statute, on the basis of a jurisdiction to imply additional provisions,[153] a residual power to admit evidence required to ensure a fair trial was possible.

1.55 Sometimes the requirements of confidentiality—although not of privilege—are overridden by the exigencies of the court process. The Civil Procedure Rules (CPR) provide for the parties to disclose all material relevant to the dispute at hand after the initiation of proceedings[154] and in some cases orders for disclosure can be made prior to the start of litigation; this is examined in chapter 12,[155] which also examines the similar processes in criminal trials. The justification of these pre-trial disclosure obligations is to enable there to be a fair trial. The rules regarding criminal investigations and powers to demand information in the course of such an investigation are dealt with in chapter 11.

1.56 However, the court is alert to the fact that the information is provided to the other litigant and to the court for a particular purpose, and the CPR also retain a rule that where material is later sought to be used for a collateral purpose permission must be sought first. This is covered in chapter 17 and has parallels with the rule that information disclosed for a particular purpose should be treated as otherwise confidential in the general law. Privacy, secrecy, and confidentiality concerns have also given rise to the practices of anonymizing witness statements, and protecting witnesses' identity, but also anonymizing cases to protect the interests of associated parties including children, and even in some cases claimant's identities. These privacy concerns must be weighed against the common law and article 6 principle of open justice. There is a sense that in some cases privacy concerns have been taken too far and there are moves, particularly in the family courts, to improve transparency. Chapter 17 also examines the extent to which, despite concerns for open justice, non-parties can be denied access to material for privacy or confidentiality reasons and the extent to which non-parties can be denied access to the proceedings as they take place in court or chambers, or the extent to which reporting is possible. This is particularly topical when we consider official secrets in the

http://www.pbookshop.com

[152] [2001] UKHL 25, [2002] 1 AC 45.
[153] ibid 68, discussed Cram (n 150) 70–72.
[154] CPR r 31.17.
[155] See also *Norwich Pharmacal Co v Commissioners of Customs and Excise* [1973] 2 All ER 943.

Copyrighted Material

Copyrighted Material

broadest sense of the phrase and the attempt to restrict all knowledge of a terrorist trial in 2014. The Court of Appeal refused to allow the complete secrecy requested in the first case, but did allow the media to be barred from considerable parts of the trial; indeed as seen from the decision the court's judgments were reserved and kept back in full.[156]

http://www.pbookshop.com

[156] *Guardian News and Media v AB & CD* 12 June 2014 <http://www.judiciary.gov.uk/wp-content/uploads/2014/06/guardian-v-ab-cd.pdf> (accessed 13 July 2015); for the 'open judgment' on the decision see *Guardian News and Media v Erol Incedal* [2014] EWCA Crim 1861. He was acquitted in March 2015 of most charges; <http://www.bbc.co.uk/news/uk-32067725> (accessed 13 July 2015).

Copyrighted Material

Copyrighted Material

Part III

DATA PROTECTION AND LEGAL PROFESSIONAL PRIVILEGE

http://www.pbookshop.com

Copyrighted Material

Copyrighted Material

in which issues of LPP most often arise) during judicial and quasi-judicial proceedings,[4] civil or criminal. In the late twentieth century, responding to the growing reach of government and the powers of public officials to compel disclosure of information, the judiciary in England and elsewhere in the common law world[5] reinvented LPP as a common law right[6] that may be invoked in any situation in which disclosure of information is mandatory. This development was accompanied by judicial pronouncements that LPP is a 'fundamental' condition of justice,[7] not merely a procedural but an important 'substantive' right[8] and, at common law, 'absolute',[9] meaning that it is without true exceptions and, unlike public interest immunity privilege (PII),[10] no balance has to be struck between competing public interests. 'If the privilege attaches to a document, then it is immune from production however strong the countervailing arguments may be.'[11] Even a court's need for evidence is subordinated to preserving confidentiality.[12]

15.02 In *B v Auckland District Law Society* Lord Millet described LPP as 'a right to resist the compulsory disclosure of information'.[13] In one respect this description is misleading. The focus of LPP is not information as such; the aim is to protect *communications*. A communication for present purposes may be defined as the transmission or exchange of information or opinions by any means. First to be protected were the written and oral communications between lawyers and their clients concerning litigation.[14] During the nineteenth century the litigation stipulation was dropped: LPP could be claimed for any communication between a client and a lawyer made for the purpose of enabling the lawyer to give or the client to receive legal advice.

> If the privilege were confined to communications connected with suits begun, or intended, or expected, or apprehended, no one could safely adopt such

http://www.pbookshop.com

[4] *Parry-Jones v Law Society* [1969] Ch 1 (CA), Law Reform Committee, *Sixteenth Report* (1967) 1.

[5] *Baker v Campbell* (1983) 153 CLR 52 (HCA), *Descoteaux v Mierzwinski* [1982] 1 SCR 860 (SCC).

[6] *R v Derby Magistrates' Court* [1996] AC 487, 507 (HL). For statutory protection of lawyer–client communications see paras 10.25 and 10.33.

[7] *R v Derby Magistrates' Court* [1996] AC 487, 507 (HL), *R (on the application of Morgan Grenfell & Co Ltd) v Special Commissioner of Income Tax* [2003] 1 AC 563 (HL) [7].

[8] *R (on the application of Morgan Grenfell & Co Ltd) v Special Commissioner of Income Tax* [2003] 1 AC 563 (HL) [31].

[9] *Three Rivers District Council v Governor and Company of the Bank of England* (No 6) [2004] UKHL 48, [2005] 1 AC 610 [25] (henceforth referred to as *Three Rivers (No 6)*).

[10] Paras 9.75 and 12.34.

[11] *Rockefeller & Co v Secretary for Justice* [2000] 3 HKC 48, 69 per Keith JA.

[12] *Three Rivers (No 6)* (n 9) [25]. The Supreme Court of Canada, on the other hand, has held that LPP may give way to some other compelling public interest such as public safety, see *R v McClure* [2001] 1 SCR 445; *Smith v Jones* [1999] 1 SCR 455 (SCC). For more about this public safety exception see paras 15.74 and 15.104 below.

[13] [2003] 2 AC 736 (PC) [67].

[14] G Hazard, 'An Historical Perspective on the Lawyer–Client Privilege' (1978) 66 Cal L Rev 1061, Note, 'Developments—Privileged Communications' (1985) 98 Harvard LR 1501.

Copyrighted Material

Copyrighted Material

precautions as might eventually render any proceedings successful, or all proceedings superfluous.[15]

15.03 The nineteenth century also saw the privilege expand to include communications with third parties made in aid of litigation.[16] As a result, at common law there are now two distinct subcategories of LPP:[17] litigation privilege (LP) and legal advice privilege (LAP). LP requires the immediacy of litigation whereas LAP does not.[18] Increasingly, the LP label has been restricted to litigation-related communications *with third parties*.[19] LAP then encompasses lawyer–client communications, whether or not related to litigation. This way of distinguishing LP and LAP is not universally used by judges,[20] but it is the one adopted in this book.

Instrumental rationales

15.04 LPP serves both the private interests of clients and the wider public interest. Although each of the subcategories of LPP has a different immediate purpose, since the eighteenth century[21] the overarching rationale of both has been to enhance the administration of justice and encourage legal compliance through the use of lawyers.[22] This rule of law rationale[23] is paradoxical because LPP also hinders courts achieving justice by suppressing relevant—and sometimes highly probative—evidence. On balance, the courts have concluded that justice is best served by protecting the confidential communications generated by the lawyer–client relationship.

15.05 The particular justification for the LAP subcategory of LPP derives from the law's complexity, which makes it desirable that individuals and organizations have access

http://www.pbookshop.com

[15] *Greenough v Gaskell* (1833) 1 My & K 98, 103, 34 ER 618 *per* Lord Brougham. The authorities on this extension were reviewed by Lord Carswell in *Three Rivers (No 6)* (n 9) [90]–[92].

[16] *Wheeler v Le Marchant* (1881) 17 Ch D 675, 684 (CA).

[17] *Anderson v Bank of British Columbia* (1876) 2 Ch D 644, [12]–[14]. No legislation distinguishes the two forms of LPP by name.

[18] *Three Rivers (No 6)* (n 9) [65].

[19] B Thanki, *The Law of Privilege* (2nd edn, OUP 2011) para 1.10.

[20] In *Dadourian Group Int. Inc v Simms* [2008] EWHC 1784 (Ch) [86], Patten J explains LP in terms of 'a communication between a client and his lawyer or between one of them and a third party which comes into existence after litigation is commenced or contemplated'. See also *Tesco Stores Ltd v OFT* [2012] CAT 6 [35]. The Police and Criminal Evidence Act 1984, s 10(1)(b) appears to have been drafted on the assumption that LP refers to 'communications between a professional and his client … in connection with or in contemplation of legal proceedings'. To complicate the situation further, some judges refer to the two subcategories as LP and LPP (instead of LAP), eg *D (A Child)* [2011] EWCA Civ 684, [12].

[21] Prior to the eighteenth century, see J Wigmore, *Treatise on the Anglo-American System of Evidence in Trials at Common Law* vol 8 (McNaughton rev. 3rd edn, Little, Brown & Co 1961) para 2290. LPP was seen as a means of protecting the lawyer's reputation which would have been damaged by being forced to breach an oath of secrecy to the client.

[22] *Blank v Canada* [2006] 2 SCC 39 [31]; A Zuckerman, *Zuckerman on Civil Procedure* (3rd edn, London 2013) para 16.19.

[23] *Carter v Northmore, Hale, Davey & Leake* (1995) 183 CLR 121, 127, 129 (HCA), *Three Rivers (No 6)* (n 9) [34].

Copyrighted Material

Copyrighted Material

the privilege against self-incrimination but do not mention LPP.[502] The courts have accepted[503] that they may order disclosure of communications passing between a lawyer and client.[504] LPP must be breached only to the extent that the communication is relevant to locating the missing child's whereabouts.[505]

Innocence at stake

15.103 English case law[506] treats LPP as paramount and, unless waived, as enduring forever once its definitional elements have been established.[507] It is available to a privilege-holder without a recognizable interest in maintaining the confidentiality of the communication, although in these circumstances it is conceivable that a court might decide that the privilege has been waived.[508] Treating LPP as absolute[509] may prevent a criminal defendant establishing her or his innocence[510] or, conversely, from being punished for the death of the client, if ownership of the privilege passed to the defendant on the client's death.[511] In the first scenario, upholding a claim of LPP may prevent a fair trial, in violation of article 6.[512] Denying LPP, on the other hand, would *not* infringe article 8 because article 8 permits rights to be denied in a proportionate manner for 'the protection of the rights and freedoms of others' and 'for the prevention of crime'.[513] To avoid a conflict with article 6, which takes precedence over a common law rule, English law may have to recognize an innocence at stake exception to LPP.

15.104 The need for this exception has been recognized in Canada where solicitor–client privilege may be set aside to ensure that a criminal defendant can make full answer and defence,[514] a right protected by section 7 of the Canadian Charter of Rights and Freedoms. To avoid damaging public confidence in the confidentiality of

http://www.pbookshop.com

[502] Family Law Act 1986, s 33; Child Abduction and Custody Act 1985, s 24A. See also ch II-2.
[503] Presumably on a necessary implication basis, although this has not been stated.
[504] *Re H (child abduction—whereabouts order to solicitors)* [2000] 1 FCR 499, 503.
[505] *Re B (abduction disclosure)* [1995] 2 FCR 601.
[506] Cf *Swindler and Berlin v US* (1998) 118 SCt 2081 (noted by H Ho (1999) 115 LQR 27).
[507] *General Mediterranean Holdings v Patel* [2000] 1 WLR 272.
[508] Under some circumstances waiver is objectively determined. For a discussion of waiver and its many forms see para 15.76.
[509] *R v Derby Magistrates' Court, ex p B* [1996] AC 487, 507 (HL). But see *General Mediterranean Holdings v Patel* [2000] 1 WLR 272, 291, 296; *Linstead v East Sussex Brighton & Hove* [2001] PIQR P 25.
[510] *R v Derby Magistrates' Court* [1996] AC 487 (HL) (a murder trial in which access by the defence to material protected by LPP that was of substantial relevance was denied). This case was decided before the incorporation of the ECHR into English domestic law.
[511] *R v Jack* (1992) 70 CCC (3d) 67 (disclosure, which was permitted in this case, assisted the prosecution of the husband by whom the client had been murdered). See also 14.05.
[512] Access to evidence is a prerequisite of a fair trial: *Jespers v Belgium* (1981) 27 DR 61, paras 57–58; *Edwards v UK* (1992) 15 EHRR 47. Cf *McGinley v UK* (1998) 27 EHRR, para 86. Article 6 also contains an implied equality of arms principle: *DeHaes v Belgium* (1997) 24 EHRR 11, para 53.
[513] Article 8(2).
[514] *R v McClure* [2001] 1 SCR 445, *R v Brown* [2002] 2 SCR 185. Contrast *Carter v Northmore Hale Davy & Leake* (1995) 183 CLR 121,125 (HCA) where an exception was proposed and rejected for a communication that 'may establish the innocence of [an] accused or … materially assist his defence'.

Copyrighted Material

Copyrighted Material

lawyer–client communications, the Canadian innocence at stake exception is narrowly confined. The defendant must convince the court of a genuine risk of wrongful conviction without access to the privileged material.[515] To do this requires the defendant to show that the material relates to a core issue and that the defence does not have access to it in an admissible form from another source.[516] The Canadian innocence at stake exception does not involve an ad hoc balancing of competing interests, an approach the House of Lords rejected in *R v Derby Magistrates' Court, ex p B*,[517] and is likely to be satisfied only in the rarest of circumstances.[518]

15.105 Before recognizing a similar exception to LPP, English courts would have to grapple with a number of issues:

1. Should it apply to all crimes or only serious ones?
2. Should the prosecutor (who is not in jeopardy) benefit from the exception?
3. What happens if the privilege-holder can also claim self-incrimination?[519]
4. To what extent, if at all, should the exception apply if the privilege-holder is a co-defendant?[520]
5. If, in the interests of avoiding a miscarriage of justice, a privileged communication has to be disclosed, how can dissemination of the privileged material be minimized?[521]

15.106 The Canadian innocence at stake exception presupposes the criminal defendant is aware of the privileged communication's existence. What if this is not the case? English courts need also to consider relaxing the lawyer's legal and ethical duties of confidentiality to permit this to be revealed. The case for allowing this is particularly strong where the client is either dead or, as in *R v Derby Magistrates' Court, ex p B*, has been acquitted and cannot be retried.[522] In these situations, the only likely consequence of lifting the veil of confidentiality is to damage the privilege-holder's reputation.

http://www.pbookshop.com

[515] In *R v Creswell* 2000 BCCA 583, the doctrine was extended to communications relevant to establishing a valid abuse of process argument. See also *R v Castro* 2011 BCCA 507.

[516] G Murphy, 'The Innocence at Stake Test and Legal Professional Privilege: A Logical Progression for the Law … But Not in England' [2001] Crim LR 728. For the case for an innocence at stake exception see also Mahoney, n 381 above.

[517] [1996] AC 487 (HL).

[518] CBA, Ethics and Professional Responsibility Committee, *Frequently Asked Questions about Solicitor–Client Privilege and Confidentiality*, November 2010, 5, available at: <http://www.cba.org> (accessed 3 October 2015).

[519] A privilege against self-incrimination is inherent in article 6, see *Saunders v UK* (1996) 23 EHRR 313.

[520] In *R v Dunbar* (1982) 68 CCC (2d) 13, 16 the Ontario Court of Appeal suggested that 'an accused ought not to be required to disclose privileged information, the disclosure of which might assist a co-accused to the detriment of the accused who is required to disclose the privileged communication'.

[521] This issue is explored in chapter 17.

[522] [1996] AC 487 (HL). The privilege-holder had been acquitted of the offence and, at the time, the double jeopardy principle prevented a retrial. The law on retrials has since changed.

Copyrighted Material

Copyrighted Material

16

DATA PROTECTION AND FREEDOM OF INFORMATION

Orla Lynskey

http://www.pbookshop.com

Copyrighted Material

Copyrighted Material

This chapter considers how data protection rules apply to professionals who process the personal data of their clients and how those professionals can avail of, or be subject to, freedom of information law. The law governing personal data processing in the UK is heavily influenced by EU law: the Data Protection Act 1998 (DPA) implements the EU Data Protection Directive (the EU Directive),[1] and the EU Charter of Fundamental Rights[2] has been successfully invoked before the courts in order to strengthen the rights of individuals.[3] Moreover, at present the EU is currently in the process of adopting a General Data Protection Regulation[4] which, unlike the Directive, will not require national implementing legislation such as the DPA as it will enter directly into the domestic legal order. **16.01**

A. The Structure and Scope of Data Protection Law

The DPA is broad in scope as a result of the expansive way in which central concepts are defined and interpreted. **16.02**

In determining whether the DPA applies, the first step is to ascertain whether the information concerned constitutes 'data'. Unlike the EU Directive, which does not define data, the DPA defines 'data'[5] as information which: **16.03**

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;
(b) is recorded with the intention that it should be processed by means of such equipment;
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
(d) does not fall within paragraph (a), (b), or (c) but forms part of an accessible record; or
(e) is recorded information held by a public authority and does not fall within paragraphs (a) to (d).

An 'accessible record' is defined as a 'health record, an educational record or an accessible public record',[6] while a 'relevant filing system' is defined as a set of

[1] 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.
[2] EU, Charter of Fundamental Rights of the European Union [2000] OJ C364/01 and [2010] OJ C83/389.
[3] *Google Inc v Vidal Hall and Ors* [2015] EWCA Civ 311.
[4] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final.
[5] S 1(1) DPA.
[6] S 68 DPA.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

information, which although not automatically processed, is 'structured, either by reference to individuals or by reference to criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible'.[7] In *Durant v FSA*[8] LJ Auld specified that a manual filing system must be 'on a par' with a computerized filing system.[9] Therefore, if a professional processes hard copies of personal data, rather than digitized personal data, the data protection rules will only apply if the files are stored in a manner which enables the easy identification of files relating to a particular individual or individuals.

16.04 Not all 'data' are 'personal data' for the purposes of the DPA. Personal data are data which relate to a living individual who can be identified from those data alone, or from those data in conjunction with other information which the controller possesses or is likely to possess in the future.[10] The definition of personal data encompasses expressions of opinion about an individual and indications of others in respect of that individual.[11] Therefore, in addition to the requirement that the information must be data, two additional elements must be present: the data must (1) 'relate to' (2) an 'identified or identifiable' individual. In *Durant* the Court of Appeal interpreted the 'relate to' condition narrowly in an attempt to limit this broad definition of personal data. It suggested that as the DPA was intended to give effect to the requirements of article 8 of the European Convention on Human Rights (ECHR), data only 'relate to' an individual if the information concerned is 'biographical in a significant sense' or if it affects the privacy of an individual.[12] *Durant* has, however, subsequently been confined to its facts in *Edem*[13] and therefore a broad definition of personal data, in line with the EU Directive[14] and the Opinion[15] of the Article 29 Working Party,[16] prevails. As personal data relate to only 'identified or identifiable' individuals, anonymized data are excluded from the scope of the DPA, although the extent to which personal data can ever be said to be fully anonymized is disputed.[17]

http://www.pbookshop.com

[7] S 1(1) DPA.
[8] [2003] EWCA Civ 1746.
[9] ibid [46].
[10] S 1(1) DPA.
[11] ibid.
[12] *Durant* (n 8) [28].
[13] See *Edem v IC & Financial Services Authority* [2014] EWCA Civ 92.
[14] Art 2(a) (n 1).
[15] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data', adopted on 20 June 2007, WP136.
[16] Art 29 of the EU Directive provides for the creation of a 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data' (the 'Article 29 Working Party'). This is an independent body, composed of a representative of each of the national data protection authorities amongst others, which acts in an advisory capacity.
[17] This is acknowledged by the Article 29 Working Party which states that 'case studies and research publications have shown how difficult it is to create a truly anonymous dataset while retaining as much of the underlying information as required for the task'. See Article 29 Working Party, 'Opinion 5/2014 on Anonymisation Techniques', adopted on 10 April 2014, WP216, 3.

Copyrighted Material

Copyrighted Material

Part IV

OPEN JUSTICE AND PRIVACY

http://www.pbookshop.com

Copyrighted Material

Copyrighted Material

17

OPEN JUSTICE, PRIVACY, AND LIMITING USE OF DOCUMENTS DISCLOSED IN LITIGATION

Duncan Sheehan

http://www.pbookshop.com

In an adversarial legal system the parties to proceedings are entitled to have access to documents belonging to opponents and third parties including records containing confidential and other personal information. This chapter examines the measures that exist in law to preserve as far as possible the confidentiality of the information that has had to be disclosed either prior to trial or during proceedings in a court of law. **17.01**

A. Control of Documents

Limited disclosure and circulation

When a party to litigation is required to allow inspection of confidential documents in civil litigation, the court may limit production of the confidential documents by imposing restrictions as to where copies of the documents may be kept or read and by whom.[1] In intellectual property law disputes such restrictions are imposed so as protect the parties' trade secrets.[2] In other cases access to medical and counselling **17.02**

[1] P Matthews and H Malek (eds), *Disclosure* (4th edn, Sweet & Maxwell 2011) para 15.23.
[2] *Mackay Sugar Cooperative Association Ltd v CSR Ltd* (1996) 137 ALR 187.

Copyrighted Material

Copyrighted Material

records have been restricted to the applicant's legal and professional advisers[3] or, if the applicant is not legally represented, to his medical advisers.[4] Reasons for imposing restrictions on disclosure of documents about someone other than the party receiving disclosure also include that there is a risk of harassment[5] and to protect the parties' privacy.[6] It was said in *Elliott v MEM* that

> [i]t is not in dispute that the defendants' medical adviser should see all records, however sensitive, so that he can give proper advice on all the information known to the plaintiff's medical adviser. Justice demands no less. But I see no reason why the disclosure of sensitive records should go further than is necessary to secure that end. Documents which the medical adviser considers relevant will of course be disclosed to the defendants' legal advisers … But the indiscriminate disclosure of all the plaintiff's medical records to the defendants' solicitors would, in my view, threaten a legitimate interest of the plaintiff in maintaining the confidentiality of her medical records, without securing any compensatory advantage or benefit to the defendants.[7]

17.03 In some cases it is not unknown for access to documents to be limited to counsel who cannot pass the document on to their client. This causes difficulty because it might be that the evidence shows that there is little chance of litigation succeeding and decisions to discontinue should be made by the client, not his advisers. This can be embarrassing for counsel and lead them to refuse to examine material.[8] However, the article 8 right to respect for privacy of the subject of the document may make such a restriction unavoidable in England.[9]

17.04 Confidentiality clubs or confidentiality rings are often considered in cases where commercial rivals disclose information to one another.[10] The issue is that when, for example, confidential pricing information has to be divulged, it may be impossible for a competitor to entirely put that out of their mind in setting their own prices. There is therefore a link to the question of collateral use, considered below. Confidentiality clubs operate to restrict access to commercially sensitive documents to certain individuals only. The question arose in the decision of *Roussel Uclaf v ICI (No 2)*[11] where it was said,

[3] *Steele v Moule* [1999] CLY 326; *Re B* [2002] All ER (D) 167. Contrast *Premier Profiles Ltd v Tioxide Europe Ltd* 29 September 2002 [29]; If there are legal advisers, the legal advisers must be given access to the documents: *Hipwood v Gloucester Health Authority* (1995) 24 BMLR 27.

[4] Senior Courts Act 1981, ss 33(2)(b)(iii), 34(2)(b)(iii); County Court Act 1984, ss 52(2), 53(2).

[5] *Church of Scientology v DHSS* [1979] 3 All ER 97. Contrast *B v B* [1991] 2 FLR 487.

[6] *M v L* [1997] 3 NZLR 424.

[7] *Elliott v MEM Ltd* 11 March 1993; deciding when privacy rights come out paramount can lead to difficult cases and on its face astounding advice to crime victims. It may be best to advise the victim of sexual offences not to see a counsellor because the notes of such confidential discussions with a professional may be disclosable to the defence to allow for a fair trial under art 6.

[8] *Grofam Pty Ltd v Macauley* (1994) 121 ALR 22, 37 (Ryan J).

[9] As in eg *Re X* [2002] EWCA Civ 525, denying the birth parents access to the identity of proposed adopters of children.

[10] *Mears Ltd v Leeds City Council* [2011] EWHC 40; *Porton Capital Technology Funds v 3M UK Holdings Ltd* [2010] EWHC 114 (Comm); *Church of Scientology of California v DHSS* [1979] 1 WLR 723.

[11] [1990] FSR 25.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

> [e]ach case has to be decided on its own facts and the broad principle must be that the court has the task of deciding how justice can be achieved taking into account the rights and needs of the parties. The object to be achieved is that the applicant should have as full a degree of disclosure as will be consistent with adequate protection of the secret. In so doing, the court will be careful not to expose a party to any unnecessary risk of its trade secrets leaking to or being used by competitors. What is necessary or unnecessary will depend upon the nature of the secret, the position of the parties and the extent of the disclosure ordered. However, it would be exceptional to prevent a party from access to information which would play a substantial part in the case, as such would mean that the party would be unable to hear a substantial part of the case, would be unable to understand the reasons for the advice given to him and, in some cases, the reasons for the judgment.[12]

17.05 In *IpCom GmBH v HTC Europe Ltd*[13] Floyd J set out a number of considerations relevant to the inclusion or exclusion of individuals in a confidentiality club. In that case the respondents argued that the information was valuable commercial information to which access should be restricted. The considerations were:

1. That the proceedings were at interim stage and it was unclear whether there would be a full trial. Allowing full inspection could inflict unnecessary detriment on HTC and others.
2. The lack of clarity as to the usefulness of the documents, which might be found to be of background relevance only.
3. The interests of third parties, party to some licensing agreements and concerned to maintain their own confidentiality interests through non-disclosure to IpCom.
4. The size of the receiving company—although this was not explicitly suggested, a larger organization[14] would be able to put information barriers (see chapter 4) in place, avoiding the issue above of a competitor's pricing strategy affecting its own. Frohwitter and Schoeller, who were part of IpCom's internal management team, were denied access therefore on the basis that they could not 'unlearn' the information and might not in reality be able to avoid its subsequent use. As an external lawyer bound by a code of ethics, Sedlmaier was allowed access.
5. Whether it was necessary in the interests of justice for the parties to have access to the documents. It was decided it was not.

17.06 Confidentiality rings are also sometimes used where judicial or quasi-judicial decisions have confidential elements. This has recently caused friction between the European Commission and the English courts. In *Emerald Supplies Ltd v BA*[15] the claims were by indirect purchasers against British Airways for freight overcharges made to a freight forwarder who had then passed through those overcharges. Having decided to fine a number of carriers, the European Commission failed

[12] ibid 29–30; *Warner-Lambert Co v Glaxo Laboratories Ltd* [1975] RPC 354.
[13] [2013] EWHC 52 (Pat) [31–33].
[14] Also referred to in *Mears Ltd v Leeds City Council* [2011] EWHC 40, [50] (Ramsey J).
[15] [2014] EWHC 3513.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

proceedings are concluded.[221] Importantly, section 12 of the 1960 Act does not itself protect the identity of the child (or anyone else). FPR 12.73 supplements the Children Act 1989 by providing for a list of persons to whom disclosure of proceedings related to the Act may be made, but prohibits communication to the wider public of information relating to proceedings held in private on pain of contempt. FPR 14.14 provides similar guidance for cases under the Children and Adoption Act 2002. The January 2014 Practice Guidance in the family courts and Court of Protection provides a rubric to be added at the start of the judgment, stating that the judgment was delivered in private and naming the conditions on which publication is permitted. It is contempt to fail to abide by that.

17.70 The High Court has jurisdiction to add to the restraints under the Children Act 1989 and Administration of Justice Act 1960.[222] Such applications for reporting restrictions orders are to be considered by balancing the article 8 and article 10 rights of the parties. In *Re J (A Child)* Munby P sets out a series of arguments in favour of transparency.[223] In that decision he stated that the naming of the professionals would not necessarily make it likely that J would be identified, and that he was concerned to permit legitimate discussion by the parents. He decided that:

> The balance between the public interest in discussing the workings of the system and the personal privacy and welfare interests of the child is best and most proportionately struck by restraining the naming of the child while not restraining the publication of images of the child. The effect of this is that (a) the essential vice—the identification of the child—is in large measure prevented, (b) internet searches are most unlikely to provide any meaningful 'link' in the searcher's mind with the particular child, and (c) the public debate is enabled to continue.[224]

Given that a picture is said to be more privacy-invading than a simple statement of what happened, it is surprising that the pictures were allowed to be posted.

In *A Council v M*,[225] M had forced her adoptive daughter A to artificially inseminate herself to add another child to the family. The question at issue was not whether M—as the defendant in a criminal trial—should have her identity withheld but how to protect the children. A previous reporting restrictions order had in fact been breached by M who had written a piece which appeared on a website. Peter Jackson J concluded that the consequences of publicity and M's identification for the younger family members would at best be harmful and at worst disastrous, saying '[i]f these youngsters are identified, the effect on them would be long-lasting and profound.' By contrast, an order preventing the identification of a criminal

[221] *Re J (A Child)* [2013] EWHC 2694, [2014] 1 FLR 523, [21] (Munby P), citing *Clayton v Clayton* [2006] EWCA Civ 878, [2006] Fam 83; see also *Re P (A Child)* [2013] EWHC 4048 (Fam).
[222] *Re J (A Child)* [2013] EWHC 2694; [2014] 1 FLR 523, [22].
[223] ibid [25–40].
[224] ibid [82].
[225] [2012] EWHC 2038.

Copyrighted Material

http://www.pbookshop.com

Copyrighted Material

defendant would not preclude the reporting of the trial itself.[226] He came to this conclusion after a careful balancing of the parties' article 8 and article 10 rights using the 'intense focus' approach set out in *Re (S)*[227] and discussed in chapter 2. The opposite result was arrived at in the case of *Re Trinity Mirror plc*.[228] In that decision the Court of Appeal overturned an order under section 11 of the Contempt of Court Act 1981 preventing the naming of a defendant in order to protect the children involved. The Court of Appeal found the Crown Court in fact lacked jurisdiction to make the order, but went on that the importance of free reporting of criminal trials cannot be overemphasized and that no order barring identification was possible, but that work should be done with the children to help them to cope with the identification of the defendant.[229]

Postponement of reporting

17.71 Under section 4 Contempt of Court Act 1981 the court may order the postponement of publications of a fair report of its proceedings where appropriate to do so in the interests of the administration of justice. When the court exercises its discretion under section 4(2) the test has three stages:

1. Is there a not insubstantial risk of prejudice?
2. Would the order eliminate the risk, and are there less restrictive means of dealing with it?
3. The judge must then balance the competing public interests of administration of justice and open justice.

Longmore LJ in *ex p The Telegraph Group Ltd*[230] commented that even if there is no other way to remove the alleged risk of prejudice, the degree of risk involved may be tolerable and making no order may still be justifiable. On the facts of that case he was concerned that even fair and accurate reporting[231] of the trial might create a head of steam in the form of resentment. The facts involved a police officer who was being tried for the murder of an unarmed man in the bedroom of his flat after a bungled police raid. Another three officers were accused of misconduct in public office. Since the first officer intended to blame the other three as part of defence, the Court of Appeal agreed that reporting of the first trial should be restricted so as not to prejudice the second. The section is in fact regularly invoked in such cases of sequential trials, so the conduct of the first does not prejudice the second.

http://www.pbookshop.com

[226] ibid [85–86]; *A Local Authority v W* [2005] EWHC 1564 (Fam) where the identification of the defendant in a trial for knowingly infecting another with HIV would make one of her children's (who was likely to have been infected also) lives impossible; *Re A (A Minor)* [2011] EWHC 1776 (Fam).
[227] [2005] 1 AC 593.
[228] [2008] EWCA Crim 50; [2008] QB 770.
[229] ibid [33–34].
[230] [2001] 1 WLR 1983 (CA) 1991.
[231] ibid 1988.

Copyrighted Material