The Battle for Rights – Getting Data Protection Cases to Court

Megan Richardson*

Abstract

This article compares the legal protection of privacy and personal data principally in common law jurisdictions. It points out that the growth of privacy law in these jurisdictions has traditionally centred on the ability of individuals to bring claims to court, with claims largely dealt with as a matter of common law (i.e. judge-made law). However, the absence of a generally accepted principle that individuals should be free to bring a claim in court for a breach of a statute has worked to limit the development of (statutory) data protection norms in the common law world. Nevertheless, the situation now appears to be changing with some recent cases.

Keywords: Privacy; data protection; common law; judicial enforcement; comparative law

1. Introduction

In his 1872 masterwork Der Kampf ums Recht, or The Battle for Right as it was known in England,¹ the German legal sociologist Rudolf von Jhering argued that the ideal environment for the creation of law is one in which aggrieved individuals voice their grievances publicly, and lawmakers including judges respond with the development of legal standards in sympathy with their concerns. Law is thus the product of a constant struggle by individuals for the recognition of legal rights. In words later echoed to a considerable extent by the American jurist Oliver Wendall Holmes Jr,² von Jhering said that ‘[t]he life of the law’ is based on the idea of ‘restless striving and working’.³ Or as Holmes eloquently put it in his own masterwork The Common Law in 1881, ‘the life of the law has not been logic; it has been experience’.⁴ Von Jhering may have restricted his comments to private law, taking the benevolent view that ‘the realisation in practice of

---

¹ Professor of Law and Co-Director of the Centre for Media and Communications Law, The University of Melbourne. Thanks to the anonymous referees as well as Karin Clark, Martin Vranken and especially Lee Bygrave for very helpful comments on earlier drafts, and to the editors of the Oslo Law Review for their thorough editing of the manuscript.

² See Konrad Zweigert and Kurt Siehr who note more generally that Jhering was influential in American legal realism, in part due to the publication of his work in English: ’Jhering’s Influence on the Development of Comparative Legal Method’ (1971) 19 American Journal of Comparative Law 215, 223–225.

³ von Jhering (n 1) 2.

public law and criminal law is assured, because it is imposed as a duty on public officials'. However, his logic may be extended to any law whose 'practical realisation depends on the assertion by individuals of their legal rights', including where public officials have wide discretion rather than a specific 'duty' to give effect to the law for the individual's protection. In these instances, as in others where 'the realisation of the law depends upon the ability of individuals to bring claims, it can be argued that the individuals concerned should have the power directly to vindicate their legal rights.

In any event, this was the position taken by the framers of the Bürgerliches Gesetzbuch (BGB) who, in 1896, responded to von Jhering and others who maintained that law should reflect modern concerns, including protection against 'attacks on personality'. Section 823 II of the BGB stated that a person harmed as a result of another's breach of a statutory provision adopted for his or her protection is entitled to bring a claim for damages in court. After the BGB came into force the provision became an early platform for the development of personality rights in Germany in the early 1900s, even before the inclusion of rights to dignity and personality in the post-second world war German Constitution, which prompted a more expansive reading of the provisions of the BGB to flesh out personality rights in accordance with the new constitutional standards.

A number of jurisdictions in the common law world have adopted versions of section 823 II of the BGB in ways tailored to personality rights. For example, the New York legislature, after the failure of the plaintiff's privacy claim in the 1902 case of Roberson v Rochester Folding Box Co, enacted sections 50 and 51 of the New York Civil Rights Law in 1903. These sections, which continue in force today, impose criminal liability on those who without consent use a person's name or likeness for advertising or trade purposes (the circumstances of the Roberson case) and further specify that a person harmed can bring a civil action for damages. Thus, even without much by way of common law protection of privacy in New York, there is some statutory protection available to privacy through sections 50 and 51 of the Civil Rights Law including a right to bring claims to court. Moreover, this protection has Withstood (to an extent) the broad reading given by the US courts, especially from the 1960s onwards, of the right to freedom of

---

5 von Jhering (n 1) 71.
6 ibid (of course he identified this especially with what he termed 'private law').
7 Thus von Jhering spoke of the 'idealism' of 'the man who looks upon himself as his own end, and esteems all else lightly when he is attacked in his personality'. See The Struggle for Law (n 1) 100-101.
8 Subject to a qualification that 'the obligation to compensate only applies in instances of fault'. See Martin Vranken, Fundamentals of European Civil Law (2nd ed, Federation Press 2010), 291.
10 ibid.
11 Roberson v Rochester Folding Box Co, 171 NY 538, 64 NE 442 (NY 1902).
speech and the press under the First Amendment to the Bill of Rights in the US Constitution.¹³

Norway provides an example of a mixed system with some common law features. As noted in Lillo-Stenberg and Sæther v Norway,¹⁴ plaintiffs can rely on sections 3–6 of the Damages Compensation Act of 1969 in conjunction with section 390 of the Penal Code of 1902 to bring civil claims for legal protection of privacy.¹⁵ Although Norwegian courts have also developed their own non-statutory precedents in favour of privacy,¹⁶ the above statutory provisions have often been relied on in cases involving privacy claims, including the Lillo-Stenberg case. It was only because of the particular circumstances of the latter case (involving celebrity performers engaged in a spectacular celebration of their marriage in a publicly accessible area) that the Norwegian Supreme Court held that the publication of unauthorised photographs of parts of the celebration (but not the actual marriage ceremony) in the magazine Se og Hør was not an unlawful violation of the plaintiffs’ privacy. When the case came before the European Court of Human Rights, the latter accepted that an appropriate balance had been reached between the rights to private life and freedom of expression under Articles 8 and 10 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) taking into account the margin of appreciation afforded to national law.

Nevertheless, common law jurisdictions have not, as a general matter, accepted that individuals should be entitled to bring an action under a statute adopted for their protection. Rather, developments of privacy law in common law jurisdictions have mainly been focused on common law (i.e. judge-made law), which itself is premised on the central idea of individuals bringing claims to court. While this approach has worked reasonably well for aspects of privacy law, it has led to a relative lack of development of

¹³ However, note Chanko v American Broadcasting Co, Inc 2014 NY Slip Op 30116(U) and on appeal 122 AD 3d 487 (2014), regarding the reality television programme ‘NY Med’ filmed in The New York and Presbyterian Hospital without patients’ consent. Claims for violation of privacy included claims under §§ 50 and 51 New York Civil Rights Law, statutory rules on physician–plaintiff confidentiality, and the tort of intentional infliction of emotional distress. The claims were struck out on the basis that the show depicted a ‘pixilated image of plaintiffs’ decedent, who was not identified’ (despite evidence from the plaintiffs that the decedent was recognised by his wife and family while viewing the episode months after his death).

¹⁴ Lillo-Stenberg and Sæther v Norway Appl. no. 13258/09 (Judgment, 16 January 2014).

¹⁵ Unlike their more generally worded German counterparts, the focus of these sections is privacy: s 390 Penal Code (Straffeloven, 22 May 1902, no 10) stating that ‘[a]ny person who violates another person’s privacy by giving public information about personal or domestic relations shall be liable to fines or imprisonment for a term not exceeding three months’, ss 3–6 Damages Compensation Act (Skadeerstatningsloven, 13 June 1969, no 26), adding that ‘a person who has ... infringed the privacy of another person shall, if he has displayed negligence or if the conditions for imposing a penalty are fulfilled, pay compensation for the damage sustained’.

¹⁶ See e.g., Lee Bygrave and Ann Aarø, ‘Norway’ in Michael Henry (ed.), International Privacy, Publicity and Personality Laws (Butterworths 2001), 333, 340. The authors also note a number of other statutory provisions of relevance to privacy protection, including s 121 Penal Code dealing with breaches of confidence.
data protection norms in these jurisdictions, although the situation appears now to be changing.

2. The Common Law Approach

In common law jurisdictions, in contrast to the broad freedom accorded to common law doctrine developing through judicial resolution of individual grievances, statutes are given a restricted role. Thus in the UK and Australia, it is said that a statute, being the provenance of the legislature, must manifest an intention to allow private claims to be brought before the courts. Indeed, where a statute provides its own mechanism for enforcement – as for instance with the appointment of a public official or body to oversee its operation – the assumption is against private claims (except to the extent provided for under the statute). The classic statement is still held to be that of Lord Tenterden CJ in *Doe d Bishop of Rochester (Murray) v Bridges* in 1831: ‘[w]here an Act creates an obligation, and enforces the performance in a specified manner, we take it to be a general rule that performance cannot be enforced in any other manner’. In the US there is sometimes said to be no tort of breach of statutory duty – although this statement may go too far, for a court may take a statutory standard into account in assessing liability for the common law tort of negligence or in fashioning other torts based on the statutory ‘policy’. Nevertheless, if a statute provides its own mechanism for enforcement, the inclination is often (with some variations) against this.

These approaches have limited the development of rights over personal data in common law jurisdictions. For instance, section 5 of the US Federal Trade Commission Act of 1914 (as amended in 1938) broadly prohibits ‘unfair or deceptive acts or practices’ in

17 By ‘data protection norms’ I mean legal rules that specifically regulate the processing of personal data (i.e., data that relates to identifiable natural/physical persons) with a view to safeguarding, *inter alia*, the personality interests of the data subjects. While data protection norms can be seen as a subset of privacy law, their aims embrace more than a concern for privacy. See generally Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International 2002) ch 7.


20 See W. Page Keeton et al, *Prosser and Keeton on the Law of Torts* (5th ed, West Publishing 1984), 222 (‘perhaps the most satisfactory explanation is that courts are seeking, by something in the nature of judicial legislation, to further the ultimate policy for the protection of individuals which they believe the legislature must have in mind’).

21 See Richard Stewart and Cass Sunstein, ‘Public Programs and Private Rights’ (1982) 95 *Harvard Law Review* 1193 for a detailed discussion and argument that courts should be more willing to provide remedies in the face of legislative silence in order to foster legislative objectives of e.g. security of entitlements and advancement of public values.

22 15 USC §§ 41–58.
trade. This is often billed as a consumer data protection provision. Yet it has been treated as offering a relatively limited base for the development of consumer data protection norms. The courts have held that enforcement of section 5 vests in the Federal Trade Commission. This is on the basis that ‘[o]n careful examination of the Act and its legislative history ... Congress did not contemplate or intend ... a private right of action’ and ‘the social ends to be fostered [by the statute] and the administrative means of achieving those objectives, are inseparably interwoven into a unified and comprehensive statutory fabric’, with the legislative balance ‘[taking] into account not only consumer protection but also the interests of the businesses affected, with particular concern for tempered enforcement, the orderly development of commercial standards, and freedom from multiplicitous litigation’. The FTC is entitled to bring cases to court but rarely does so, leaving this as the last option for situations where it cannot itself resolve the matter. Moreover, its preference is usually to resolve matters through a process of negotiated compromise rather than the pronouncement of relevant legal norms. Commentators have noted that ‘the FTC has asserted itself as a strong watchdog in this domain based on its broad authority to regulate “unfair and deceptive trade practices” pursuant to Section 5 of the Federal Trade Commission Act’. However, the FTC hardly operates as a vehicle for the stringent vindication of data protection rights, due to its conciliatory approach.

Not all US states have emulated the federal approach under the FTC Act. California, for instance, has a number of statutory protections of personal data which allow for individual claims. These include the protection of a person’s name or likeness from unauthorised use in advertising under section 3388 of the California Civil Code; the protection against ‘unfair competition’ under section 17200 et seq of the California Business and Professional Code; the protection of medical records under section 56 of the California Confidentiality of Medical Information Act; and rules on ‘personal information privacy’ dealt with under section 1798.81 et seq of the California Civil Code.

---

25 To take a recent example, under the terms of a draft consent order with Craig Brittain, founder of IsAnybodyDown, Brittain agrees to refrain from publishing more nude photographs or videos of people without consent, but without admission of liability or award of damages or compensation to those whose privacy has been affected: see (2015) 80 Federal Register no. 25, 6714.
26 The California Civil Code § 3344 prohibits the non-consensual use of another’s name, voice, signature, photograph, or likeness for advertising, selling, or soliciting purposes, and creates a cause of action for persons injured by such actions.
27 The California Business & Professional Code § 17200 et seq prohibits ‘any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising, ...’ and creates rights of action for ‘a person who has suffered injury in fact and has lost money or property as a result of the unfair competition’.
28 California Civil Code § 56 et seq provides for confidentiality of medical information, creates rights of action for a person ‘who has sustained economic loss or personal injury’, and permits the award of nominal statutory damages under § 56.36.
Several substantial class actions relying on these provisions have been brought in California in recent years. A high profile example is the *Fraley v Facebook* class action launched after the social network’s change of terms of service to facilitate its sponsored stories advertising programme. The plaintiffs’ claims included breach of customers’ publicity rights and unfair competition. After Facebook failed in its attempt to have the claims struck out summarily, a settlement was arrived at, requiring payment of damages and clear notification of Facebook terms. Adobe has been another target. And more recently, current and former employees of Sony Entertainment have brought several class actions against the company after a major 2014 hack of the company resulted in the release of their personal data, including sensitive health information, on the internet. The claims against Sony include, *inter alia*, breach of the Confidentiality of Medical Information Act and the personal information privacy standards of the California Civil Code. Thus, it seems that California is developing as a centre for what might be called data protection law – much in the same way as it earlier developed as a locus of common law and statutory claims around the protection of privacy and publicity.

Dealing with privacy and publicity rights as a matter of common law may be a reasonable option for plaintiffs given the inherent flexibility of common law doctrines. Samuel Warren and Louis Brandeis argued in their seminal article on *The Right to Privacy* published in 1890 that the law should move further to acknowledge the right to privacy in response to claimants’ demands in a way that, some have suggested, was influenced by von Jhering. Yet, they were talking about a new common law (rather than statutory) privacy tort which would build on and supplement previous common law developments. In this respect, they were following Holmes who in the 1880s treated

---

29 California Civil Code § 1798.81.5 (as amended in 2014) provides that ‘[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure’. Other provisions require data breach notification and state that a customer injured by a violation of the title may institute a civil action for damages.

30 See *Fraley v Facebook, Inc*, 830 F Supp 2d 785 (2011). The court rejected the defendant’s motion for summary dismissal and allowed the claims to proceed to trial based on the right of publicity and unfair or deceptive acts or practices under the California Business and Professional Code, with the result that the parties settled.

31 In *re Adobe Systems Privacy Litigation*, 014 US Dist. LEXIS 124126. The court allowed a class action to proceed against Adobe after a 2013 hack of Adobe’s servers which involved the theft of customers’ personal information including credit cards, login ids, passwords and expiration dates. Taking a liberal view of the US Supreme Court’s pronouncements on the threshold requirement for standing in a class action in *Clapper v Amnesty International USA*, 133 S Ct 1138 (2013), the California court accepted that there was ‘threatened injury ... certainly impending to constitute injury in fact’ sufficient to meet the threshold requirement.


the common law as a principal site of the development of legal rights in response to new social circumstances. It was a powerful argument at the turn of a century when social changes included the widespread use of the portable camera, the ‘yellow press’, and modern advertising techniques, leading to some public consternation about the consequences for privacy. The plaintiffs’ claims, bolstered by Warren and Brandeis’ arguments, inspired the development of a number of privacy torts in various US states. These torts were subsequently catalogued by Prosser as torts of, respectively, publication of private facts, intrusion on seclusion, false light publicity, and appropriation of name or likeness (the latter a precursor to what would later become a publicity right).

Might the common law produce a set of data protection norms? In some ways common law developments have been quite well geared to modern conditions of weak computerised information-security systems combined with powerful communication networks. For example, in the pending Sony litigation in California, one of the claims rests on negligence, which is framed in terms of a lack of due care in guarding employees’ and former employees’ personnel files from malicious hacking and internet publication. Comparable claims have already succeeded in other US cases, including in Remsburg v Docusearch, Inc in New Hampshire where an internet-based investigation and information service was held liable for negligence for retrieving and passing on

35 See Holmes (n 4).
36 See Robert Mensel, ‘Kodakers Lying in Wait: Amateur Photography and the Right of Privacy in New York, 1885–1915’ (1991) 43 American Quarterly 24. The problem was not just amateur photography: for a photograph taken of an actress without her consent as part of a commercial publicity stunt mounted by the theatre, see Manola v Stevens & Myers, unreported, in June 1890, noted in Warren and Brandeis (n 33), 195.
37 Warren and Brandeis (n 33) observed that: ‘The press’ is ‘overstepping in every direction the obvious bounds of propriety and decency’: 195–196. Even so, they did not anticipate the new photojournalistic practices that would follow the commercialisation of the half-tone block from about 1890 onwards, ushering in the pictorial newspaper and magazine press. See Howard Cox and Simon Mowatt, Revolutions From Grub Street: A History of Magazine Publishing in Britain (Oxford University Press 2014), ch 2.
38 The development of display advertising was another consequence of the commercialisation of half-tone block technology: see Cox and Mowatt, ibid. But advertisers were also updating their techniques to take into account the new insights from psychology, drawing on the work of Walter Dill Scott, John Watson and Edward Bernays (nephew of Sigmund Freud) in the early 1900s, including the powerful impact of personal associations when it comes to selling goods and services: see Matthew McDonald and Stephen Wearing, Social Psychology and Theories of Consumer Culture: A Political Economy Perspective (Routledge 2013), 3–4.
39 Nor were Warren and Brandeis the only ones to note this: see, for instance, Roscoe Pound, ‘Interests of Personality’ (1915) 28 Harvard Law Review 343, 362–363 (‘the demand which the individual may make that his private personal affairs shall not be laid bare to the world and be discussed by strangers’ is ‘a modern demand’).
41 Corona v Sony Pictures (n 32): Sony owed a legal duty to Plaintiffs and the other Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard their PII stored on its Network: [4]; Forster v Sony Pictures (n 32), framing the duty of care to include ‘among other things, maintaining and testing SPE’s security systems and taking other reasonable security measures to protect and adequately secure the personal data of Plaintiffs and the class from unauthorized access’: [86].
social security and address details of a woman to a stalker who murdered her.\textsuperscript{42} American privacy scholars have identified \textit{Remsburg} as ‘an important step forward in recognising and remediying modern information privacy harms’.\textsuperscript{43} European scholars might consider this a step beyond privacy protection as it is focussed on the protection of personal information rather than privacy as such, although it still clearly falls short of a European-style right of data protection.\textsuperscript{44} Certainly, there are limits to the use of negligence as a common law data protection doctrine, premised as it is on a duty of care owed by the defendant to the plaintiff, and there have been only a few cases.\textsuperscript{45}

In the UK as well, most of the development of personality rights has also been around the common law, and if anything its historical character has determined even more the shape of the development than in the US where there is more open adherence to Holmes-inspired legal realist ideas. Thus, what in the US is called a right of publicity is in the UK dealt with under a more traditional common law doctrine of passing off, although the latter is construed broadly to include unauthorised personal endorsement cases.\textsuperscript{46} Similarly, the protection of privacy has until recently been largely dealt with as a matter of the equitable action for breach of confidence,\textsuperscript{47} a doctrine that has also come to be broadly construed. It extends, for instance, to cases involving the misuse of information obtained with knowledge or notice of confidentiality rather than being confined to cases where the information was imparted in a relationship of confidence.\textsuperscript{48}

---

\textsuperscript{42} \textit{Remsburg v Docusearch, Inc}, 149 NH 148 (2003).


\textsuperscript{44} In line with the decision of the German Federal Constitutional Court in the Population Census Act case of 1983 identifying a right to ‘informational self-determination’, as guaranteed by articles 1 and 2 of the Basic Law: \textit{Volkszählungsurteil} (Population Census Act judgment) (1983) 65 BVerfGE 1, translated by Donald Kommers, \textit{The Constitutional Jurisprudence of the Federal Republic of Germany} (Duke University Press 1989), 332, 334. See also Paul de Hert and Serge Gutwirth, ‘Data Protection and the Case Law of Strasbourg and Germany’ in Gutwirth et al (eds.), \textit{Reinventing Data Protection} (Springer 2009) 3, underlining the ‘real objective’ of data protection regulation as one of protecting individual citizens against ‘unjustified collection, storage, use and dissemination of their personal data’, being an objective that goes beyond simply ‘echoing a privacy right with regard to personal data’: ibid, 4. See too Bygrave (n 17).

\textsuperscript{45} Richards and Solove (n 43) write that ‘[h]ardly any other cases have reached a conclusion similar to that in Remsburg … [and] there have been scant attempts in tort law to explore the path that Remsburg has sketched out’: 1923.


\textsuperscript{47} Other doctrines such as negligence and intentional infliction of emotional distress might also be used on limited occasions, see, eg., \textit{Swinney v Chief Constable of Northumbria Police Force} [1997] QB 464 (negligence); \textit{James Rhodes v OPO} [2015] UKSC 32 (intentional infliction of emotional distress – although the claim did not succeed in that case and the tort was construed narrowly). However, the UK courts have resisted the idea of extending the tort of negligence by reference to obligations imposed by Article 8 ECHR, see \textit{Smith v Chief Constable of Sussex Police} [2009] 1 AC 225.

\textsuperscript{48} See for instance \textit{Douglas v Hello! Ltd} [2006] QB 125 (a case which involved the unauthorised taking and publication of photographs of a private wedding party; the plaintiffs were successful, unlike the plaintiffs in the \textit{Lillo-Stenberg} case mentioned above (n 14), although the circumstances were rather different); \textit{Campbell v MGN, Ltd} [2004] 2 AC 457 (a case involving the unauthorised taking and publication of photographs showing celebrity model Naomi Campbell, who had denied drug addiction, attending a
Human Rights Act of 1998, giving effect to the ECHR, English courts have identified a new tort of ‘misuse of private information’, but they have treated this as an offshoot of the breach of confidence doctrine rather than framing it as a breach of a statutory duty prescribed by the Act.

Interestingly, breach of confidence has also developed as a source of rights in cases that are not solely or necessarily about privacy. Such cases include *Douglas v Hello!* (in which one of the plaintiffs – OK! Magazine – had tendered for the exclusive rights to cover a celebrity wedding) and *Imerman v Tchenguiz* (in which the plaintiff objected to the defendants’ surreptitious access of his computer hard drive in his office to find evidence for a family law dispute). In both cases the claims based on breach of confidence succeeded. Indeed, in *Imerman* the court seemed prepared to hold that accessing the hard drive might in itself entail a breach of confidence rather than in more conventional terms premising the breach on the (potential) subsequent misuse of the information. As the court put it, ‘[i]t is of the essence of the claimant’s right to confidentiality that he can choose whether, and, if so, to whom and in what circumstances and on what terms, to reveal the information which has the protection of the confidence’. Such expansive reasoning suggests that this doctrine, which in the US has largely now dwindled to a narrow doctrine based on special relationships of confidence, could evolve in the UK.
into something quite significant by way of a common law data protection right, despite the constraints of the doctrine’s focus on confidential, not just personal, information.\footnote{Of course it depends on what is meant by ‘confidential’. However, the courts have broadly construed this to encompass information that retains a degree of confidentiality, even if available to a limited audience, drawing the line only ‘once it has entered what is usually called the public domain (which means no more than that the information in question is so generally accessible that, in all the circumstances, it cannot be regarded as confidential)’: Guardian Newspapers (n 48), Lord Goff at 281-2.}

3. The Turn to Statute

Until recently, courts in the UK have made little of the data protection statute drafted to comply with the standards set down in the European Union Data Protection Directive of 1995.\footnote{Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.} The latter prescribes (in Articles 22 and 23) that individuals should have a right of action in cases where they are harmed as a result of a breach of its standards. Similarly, the UK Data Protection Act of 1998, which transposes the Directive, allows for cases to be brought by aggrieved individuals.\footnote{See ss 7–15 and especially p 13 (‘Compensation for failure to comply with certain requirements’), 14 (rectification, blocking, erasure and destruction), and 15 (jurisdiction and procedure).} Nevertheless, the courts suggested in early cases under the Act that little significance would be accorded to the statute despite the readiness of plaintiffs to invoke it. In one early case, Durant v Financial Services Authority,\footnote{Durant v Financial Services Authority [2004] FSR 28.} the Court of Appeal construed the meaning of ‘personal data’ in the Act as importing a requirement that the data should be of a private character. In other cases it was simply said that the statutory data protection claims added nothing to the other claims of misuse of private and confidential information.\footnote{For instance Campbell v MGN Ltd (n 48), Baroness Hale at 494 (the data protection claim ‘adds nothing to the claim for breach of confidence’); Douglas v Hello! (n 48), Lord Phillips for the Court at 174 (‘[i]t is not necessary for us to consider the Data Protection Act … in the light of our conclusions as to privacy and confidence’); Imerman v Tchenguiz (n 52), Lord Neuberger at 627 (‘[r]esolution of the issues of confidentiality and its breach in the context of ancillary relief proceedings make it unnecessary to resolve the specific question of breach of statutory duty’).} Further, at least until recently, little was made of the right to data protection in Article 8 of the EU’s Charter of Fundamental Rights of 2000,\footnote{Article 8(1) of the Charter provides that ‘everyone has the right to the protection of personal data concerning him or her’ and Article 8(2) specifies that ‘[s]uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law …’. Article 7 provides for the right to private life in similar terms to Article 8(1) ECHR.} now part of EU constitutional law under the Lisbon Treaty of 2009. Thus, while important data protection cases have come out of other European jurisdictions, with questions referred to the European Court of Justice on issues such as the implications of European data protection standards for general monitoring of internet users for copyright infringements;\footnote{Case C-70/10 Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs (SABAM) [2011] ECR I-0000; and Case C-360/10 Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) v Netlog [2012] ECR I-0000.} data retention;\footnote{Joined Cases C-293/12 and 594/12 Digital Rights Ireland Ltd and Seitlinger and others [2014] ECR I-0000.} and the so-
called right to be forgotten,\textsuperscript{63} we have seen less attention paid to these matters in English courts. Yet, the position may be changing, as shown by some recent cases.

One such case is \textit{Rugby Football Union v Viagogo},\textsuperscript{64} decided in 2012. The Supreme Court dealt with the defendant’s argument that a preliminary discovery (or ‘Norwich Pharmacal’) order requiring release of the identities of persons involved in illegal ticket scalping using the Viagogo website would breach the Data Protection Act without taking the restrictive \textit{Durant} line of insisting that the information should also be ‘private’.\textsuperscript{65} Further, the court noted the right to data protection in the Charter.\textsuperscript{66} More recently, in the \textit{Vidal-Hall v Google} case,\textsuperscript{67} Tugendhat J granted leave to serve the defendant out of jurisdiction for claims including breach of the Data Protection Act brought by the plaintiffs after they discovered that Google had bypassed their Apple Safari security measures to access their personal information and engage in targeted advertising. The judge treated the data protection claim as distinct from the misuse of private information claim (with the ‘private’ information detailed in a secret annex to the judgment).\textsuperscript{68} For the first time it was suggested that a data protection claim may give more protection to personal information than one for misuse of private information.\textsuperscript{69}

The decision was recently upheld by the Court of Appeal,\textsuperscript{70} which went further by suggesting that the Data Protection Act in its present terms falls short of the right to data protection embodied in the Charter. Specifically, it noted that section 13(2) of the Act limits recovery of non-pecuniary loss to cases where (i) the claimant also suffers pecuniary or material loss or (ii) the contravention relates to the processing of personal data for ‘special purposes’ (journalism, artistic, or literary purposes – none of which

\textsuperscript{63} Case C-131/12 Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECR I-0000.

\textsuperscript{64} Rugby Football Union v Viagogo Ltd [2012] 1 WLR 3333.

\textsuperscript{65} The Supreme Court held that the order complied with the Data Protection Act, comparing the case to the Court of Appeal’s recent decision in \textit{Golden Eye (International) Limited v Telefonica} [2012] EWCA Civ 1740 (permitting a similar order on evidence that the claimants’ copyrights had been infringed by the individuals’ file-sharing activities).

\textsuperscript{66} The Charter was raised in the Court of Appeal in the \textit{Viagogo} case where an application was made to amend the notice of appeal to state that ‘[t]he learned judge should have had regard to the fact that the order sought [for identification of those involved in illegal ticket scalping using the Viagogo website] involved an interference with the fundamental rights of individuals under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and in the light of that fact should only have made the order if satisfied that it was both necessary and proportionate for the protection of the claimed rights of the RFU: Rugby Football Union v Viagogo Ltd [2012] FSR 11. Nevertheless, it was held that the order was necessary and proportionate.


\textsuperscript{68} There was also a breach of confidence claim but it was concluded that obtaining service out of jurisdiction for a purely equitable claim was not covered by the UK rules.

\textsuperscript{69} The judge commented that ‘[n]ot all the information that can be deduced or inferred by a person viewing a screen which shows targeted advertisements will be private information. Far from it. For example, if lawyers’ screens might show advertisements from which it could be inferred that they were lawyers, then that would, in most circumstances, not disclose information that was private (although it might be personal)’: Vidal-Hall (n 67), Tugendhat J at [118].

\textsuperscript{70} Google Inc v Vidal-Hall & Ors [2015] EWCA Civ 311.
were thought to apply in the case at hand). The qualifications are not found in Article 47 of the Charter, which states that ‘everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article’.\(^71\) The Court bluntly concluded that ‘what is required in order to make section 13(2) compatible with EU law is the disapplication of section 13(2), no more no less’.\(^72\) In future English cases we may expect to see further explication of the right to data protection now supported by the Charter.\(^73\)

4. Final Reflections

All in all, the UK appears to be becoming more European in its approach to data protection, especially as more cases get into the courts. We can expect this trend to continue at least as long as the UK remains subject to European data protection standards as well as the constitutional framework of the EU Charter, including its Article 8 right to data protection. The trend may take the UK even further away from other common law jurisdictions and not only the USA. For instance, Australia has so far seen little development of its data protection standards in part due to the limited scope allowed for those whose interests are affected to bring claims in court for breach of the statute.\(^74\) Other avenues might be explored, including relying on breach of confidence following the lead of the English Court of Appeal in *Imerman*;\(^75\) adopting the American approach of treating negligence as a standard that takes into account obligations imposed under statute (including a data protection statute);\(^76\) and developing a body of consumer data protection law to the extent that applicable consumer protection

---

\(^71\) ibid, [79].

\(^72\) ibid, [105].

\(^73\) Note also the ongoing proceedings in the English ‘right to be forgotten’ case *Mosley v Google Inc*, where the plaintiff seeks an order under the Data Protection Act requiring Google to block access to video footage posted on the internet showing him engaging in private sexual activity (after his successful case against News of the World (p 49)). In preliminary proceedings on an application brought by Google to strike out the claim, Mitting J allowed it to go forward to trial: *Mosley v Google Inc* [2015] EWHC 59.

\(^74\) Although s 98 of the Privacy Act 1988 (Cth) specifies the right to obtain an injunction under the Act (and provision is also made for enforcement or review of a determination of the Privacy Commissioner in ss 55A and 96), there is no general right to bring a claim before a court for a breach of the Act. As noted in *Austen v Civil Aviation Authority* (1994) FCR 272, ‘[i]t would appear that a deliberate decision was made by Parliament not to give a right of action in tort for breach of a privacy principle: see The Law Reform Commission Report No 22, Vol 2, par 1085’. The cited report of the Law Reform Commission states that ‘it is not appropriate that all breaches of privacy standards should give rise to an action in tort’ and ‘the question whether a breach of any particular standard should give rise to tort liability should be resolved in the context of framing that standard’, further noting that its own recommendation was a new statutory tort regarding the publication of sensitive facts. The recommended tort was not enacted. The same goes for later recommendations of the Law Reform Commission made in 2008 and in 2014, for a statutory privacy tort.

\(^75\) The Australian courts have already followed the UK courts’ lead in treating breach of confidence as a privacy doctrine: see *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 (obiter comments of Gleeson CJ and Gummow and Hayne JJ); *Giller v Procopets* (2008) 24 VR 1; *Wilson v Ferguson* [2015] WASC 15.

\(^76\) See too *Doe v Australian Broadcasting Corporation* [2007] VCC 281 (negligence liability premised on the defendants’ breach of s 4 of the Judicial Proceedings Reports Act 1958 (Vic) which makes it an offence to publish information identifying a rape victim).
legislation allows this and permits claims in court. Judges might also, as in one recent Australian case, consider data protection values in the exercise of judicial discretion.

At best, however, these techniques can only go so far in framing data protection norms in the absence of the ability of courts to deal directly with the terms of a data protection statute at the instance of those whose rights are directly involved. Moreover, ideally the development of data protection norms, concerned as they often are with conduct that transcends national borders, should be a cross-jurisdictional effort. As von Jhering noted in the 19th century, the life of the law is ideally ‘a common life; a system of reciprocal contact and influence’. Until recently that has been true of many common law jurisdictions (although to a lesser extent in the US), but whether it will continue into the future is a matter of speculation.

---

77 For instance, in Australia relying on s 18(1) Australian Consumer Law (set out in schedule 2 of the Competition and Consumer Act 2010 (Cth)) (‘A person must not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive’) and ss 232–236 of the same legislation (providing for, inter alia, actions for injunctions and damages on application by any person).

78 Dallas Buyers Club LLC v iiNet Limited [2015] FCA 317, Perram J at [84]–[86].