PRIVATE LAW RIGHTS IN THE DIGITAL AGE: THE ROLE OF THE COURT?

Lord Colin Tyre
Judge,
Supreme Courts of Scotland

Introduction

During the last 30 years, information and communications technology has developed at an increasingly rapid and bewildering pace. The internet has transformed our way of life and there is no sign that we have reached a plateau in its capabilities. When an organisation such as a court service enters into a contract for the provision of a new IT system, the only certain thing is that by the time you get it, you will no longer want what you thought you wanted when you ordered it.

The law has struggled to keep pace with these developments. Legal rules and principles devised before the digital age cannot always be applied to electronic information gathering and communication. Special new rules may quickly be superseded by further technological advances. As a consequence, the courts find themselves required to resolve disputes which simply could not have arisen quite a short time ago.

The focus of this session is on private law rights in the digital age. In this paper I will consider some of the difficulties that have arisen in relation to the exercise and protection of private law rights, and examine the ways in which these have been addressed by the courts. I shall offer some brief observations on the continuing role of the courts in developing the law in response to technological change. Because Scotland is a relatively small jurisdiction, many of these issues have not yet come up for decision there. I shall therefore be drawing to a large extent upon English case law, as well as that of the European Court of Justice and the European Court of Human Rights.

What private law rights are affected?

I begin by identifying the rights upon which this paper will focus.

Right to privacy

The first is the right to privacy. This right is enshrined for all members of the Council of Europe in Article 8 of the European Convention on Human Rights, which requires respect for private and family life. As has been recognised, the

values embodied in Article 8 are equally applicable in disputes between an individual and the state and in disputes between an individual and another individual or a non-governmental body such as a newspaper or social media company.[1] Rights to privacy did not, of course, begin in the UK with accession to the Human Rights Convention. But in relation to cases not involving interference by the state, the courts in England and Wales have found it necessary to identify the common law right that is encapsulated in Article 8, it having been decided that there was no common law tort of invasion of privacy.[2] The solution adopted was to develop the law of breach of confidence to create a right of action for misuse of private information. It is also worth noting that in the first recital to the new General Data Protection Regulation,[3] the protection of natural persons in relation to the processing of data is asserted to be 'a fundamental right'.

The general right to respect of private life and the more specific right to protection of personal data are also safeguarded by Articles 7 and 8 of the EU Charter of Fundamental Rights.

Breach of confidence

There remains in addition a distinct right of action for breach of confidence. Information may be confidential without being private, and vice versa.

Freedom of expression

Another important private law right is the right to freedom of expression, protected by Article 10 of the Convention. This right frequently comes into conflict with the Article 8 right of another person. Article 10 itself recognises that the right to freedom of expression must be exercised responsibly and subject to such restrictions as are necessary in a democratic society for, among other things, protecting the reputation or rights of others. But, once again, the right not to be defamed by another does not rest solely upon Convention rights but has been part of national law in the jurisdictions of the UK for hundreds of years.

Challenges to private law rights in the digital age

Privacy

There are a number of aspects of information and communication technology which pose particular risks of interference with private law rights. The most obvious is the advent of 'big data': the ability of computers to carry out searches,

[1] *Campbell v MGN Ltd* [2004] 2 AC 457, Lord Nicholls of Birkenhead at para 17.
[2] *Wainwright v Home Office* [2004] 2 AC 406.
[3] Regulation (EU) 2016/679

process enormous quantities of data and suggest patterns whose identification would be beyond human capabilities. Another is 'persistence': the problem that once information has been published, it remains out there, discoverable indefinitely. Such features may, without control, be subject to inappropriate exploitation by both public and private data processors.

State interference

Perhaps most controversial of all is the conflict between personal privacy rights and the exercise by the state of electronic gathering of information. In the UK, this conflict is far from having been resolved. It can at least be said that the state's exercise of information gathering powers has become more transparent than it was. This may be partly due to the activities of whistle-blowers – it was only recently that the UK expressly admitted the existence of Government Communications Headquarters (GCHQ), its information gathering and processing centre – but it is also due to the work of the Investigatory Powers Tribunal, which investigates and decides cases involving complaints that public authorities or law enforcement agencies have unlawfully infringed privacy rights or other human rights. This tribunal has evolved means by which sensitive security issues can be raised and determined in open court, for example by dealing with them on the assumption that the allegations by the complainant are true, without asking the law enforcement authority to confirm or deny this, and giving a ruling in principle before any necessary examination of the facts takes place in a closed hearing. This in turn has resulted in a much greater degree of disclosure by the UK Government of its intelligence-gathering practices, in the form of Codes of Practice with which the law enforcement agencies have undertaken to comply.

That does not of itself solve the problem if the practices openly disclosed are contrary to European law. Especially controversial is the retention of bulk data, which may be collected openly or covertly. Bulk data includes both bulk personal data, ie biographical details including commercial and financial activities, communications and travel, and also bulk communications data, which might include the location of mobile and fixed line phones from which calls are made or received (though not the content of the communications), or the location of a computer used to access the internet (though not the precise browsing history). In the case of *Digital Rights Ireland*,[4] the Court of Justice declared invalid a 2006 Directive[5] requiring e-communication service providers to retain bulk data for a period of between six months and two years for use by member states in the investigation, detection and prosecution of serious crime. The UK Government

[4] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Ireland* (Case C-293/12) [2015] QB 127

[5] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

responded to this decision by rushing through emergency legislation, the Data Retention and Investigatory Powers Act 2014 ('DRIPA'), which restored the right to require e-communication service providers to retain data for 12 months use by a range of public authorities, and for a range of purposes extending well beyond the investigation and prosecution of serious crime. The 2014 Act, however, had a 'sunset' clause in terms of which it ceased to have force at the end of 2016.

The validity of DRIPA was in turn challenged as being contrary to Articles 7 and 8 of the Charter of Fundamental Rights.[6] The challenge was brought by, among others, David Davis, a Conservative MP, and Tom Watson, a Labour MP; Mr Davis later had to withdraw as a claimant on being appointed as Minister responsible for Brexit. The claimants were especially concerned about provisions of DRIPA which permitted recovery of data relating to privileged communications between lawyer and client. The first instance court upheld the challenge, and disapplied DRIPA in so far as it failed to comply with EU law.
On appeal, the Court of Appeal referred the case to the Court of Justice for a preliminary ruling. The case was heard along with a reference from Sweden, and the Court's ruling was issued on 21 December 2016.[7]

The Court forcefully affirmed the line that it had taken in *Digital Rights Ireland*, holding that EU law precluded national legislation that prescribed general and indiscriminate retention of data. Protection of the fundamental right to respect for private life required that derogations should apply only in so far as is strictly necessary. Because the data, taken as a whole, was liable to allow precise conclusions to be drawn concerning the private lives of the persons concerned, the interference had to be regarded as particularly serious. Only the objective of fighting serious crime was capable of justifying it. The Court further considered that it was essential that access to data should, except in cases of urgency, be subject to prior review carried out by either a court or an independent body. Clearly the Court's views were not unduly influenced by the terrorist atrocities that had occurred in various member states since it gave its judgment in *Digital Rights Ireland*.

The case is now back with the Court of Appeal. Although DRIPA expired at the end of 2016, the decision of the Court of Justice remains of major importance, because on 29 November 2016, a new law, the Investigatory Powers Act 2016, received Royal Assent. This Act, gleefully nicknamed the Snooper's Charter by the media, is intended to provide a state-of-the-art regime for the exercise of investigatory powers by public authorities in the UK. Already, however, it is being asserted by opponents of wide-ranging powers that the 2016 Act suffers

[6] *Davis & Others v Secretary of State for the Home Department* [2016] 1 CMLR 48; [2015] EWCA Civ 1185
[7] Joined Cases C-203/15 *Tele2 Sverige AB v Post-och Telestyrelsen* and C-698/15 *Secretary of State for the Home Department v Watson & Others*

from the same flaws as its predecessor and consequently also falls foul of the rulings of the Court of Justice. The new Act has not yet been brought into force. The UK Government is consulting on the terms of various draft Codes of Practice to accompany the legislation, but a notable absentee is a Code of Practice dealing with bulk data retention. Matters are on hold pending the judgment of the Court of Appeal.

Nor is the departure of the UK from the European Union likely to change the position to any great extent. Although judgments of the Court of Justice will no longer have binding effect in the UK, and the UK Parliament will be free to pass legislation departing from judgments issued before the effective date of Brexit, that does not mean that the UK will be at liberty to go its own way. It will still require to share data with EU member states, and will not be able to do so unless it can provide 'a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order'.[8]

Another contentious issue which interferes even more directly with private law rights is what is referred to in security jargon as CNE (computer network exploitation) or, as everybody else would call it, hacking. The extent to which UK intelligence agencies hack into computers was the subject of an application to the Investigatory Powers Tribunal by a number of internet service providers in *Privacy International* and *Greennet Ltd*.[9] One consequence of the bringing of the case was that the intelligence agencies publicly acknowledged for the first time that certain hacking activities were carried on, but some activities, such as leaving vulnerabilities in a target computer, were still 'neither confirmed nor denied'. One of the principal issues in the case was whether warrants permitting hacking of categories of targets not identified by name contravened long-standing legal protections against general warrants. The Tribunal held that it did not, and an attempt by the claimants to have that decision judicially reviewed has been unsuccessful, the High Court having held that decisions of the Tribunal are not subject to judicial review.[10] The new Investigatory Powers Act 2016 now provides expressly for warrants to be granted for 'targeted equipment interference', so the Tribunal may have to give the matter further consideration.

Non-state interference

I have been dealing so far with interference with the privacy rights of individuals by the state. The digital age has also created opportunities for interference by individuals and by non-state entities. An interesting recent example is provided

[8] *Schrems v Data Protection Commissioner* (Case C-362/14), para 96
[9] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs; Greennet and Others v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIP Trib 14_85-CH
[10] *R (Privacy International) v Investigatory Powers Tribunal* [2017] EWHC 114 (Admin)

by the English Court of Appeal case of *Vidal Hall v Google Inc.*[11] The claimants were three Apple computer users who had been annoyed to discover that when they used the Safari internet browser, advertisements which were obviously targeted at them personally were appearing on their computer screens. This, it was alleged, could only mean that Google was collecting private information about their browsing history, contrary to its publicly stated position that this would not be done unless a Safari user expressly consented to it.

The case came before the court as an application by the claimants for leave under the English rules of civil procedure to serve the writ on Google in California. The legal issue to be decided, which was whether misuse of private information was properly classified as a tort under English law (it was), is perhaps not of as much general interest as some of the other matters arising from the court's judgment. It was confirmed that breach of confidence and misuse of private information were two separate grounds of action with different legal foundations. The court also noted that the Data Protection Directive[12] conferred a right to recover damages for distress (in addition to financial loss) – a right which had deliberately not been transposed into UK national legislation. In these circumstances, it was held that Article 47 of the Charter of Fundamental Rights (right to an effective remedy) was engaged, and the court was bound to disapply the national provision to contrary effect.

A further issue raised was whether the browser-generated information (or BGI for short) fell within the definition of 'personal data'. Google argued that the BGI taken on its own was anonymous: the individual could not be identified from it alone, and Google kept it separate from other data such as email account details. The court did not have to decide this issue but considered that it was sufficiently arguable to allow the case to proceed. Leave was granted to serve the writ in California.

A somewhat different form of breach of data protection legislation was at issue in the case of *Mosley v Google Inc.*[13] The background to the case will be familiar: Max Mosley, the former president of the Fédération Internationale de l'Automobile, successfully sued the publisher of the News of the World for breaching his privacy by printing photographs of him engaged in sexual activity. Some of the images remained available on the internet, and could be accessed using search engines. They turned up as 'thumbnails', ie reduced file size images, produced by a Google search. When Mr Mosley discovered this, his solicitors served notices under the Act on Google requiring it to cease processing the images. Google refused for various reasons, including that it was not a data controller. Mr Mosley sued again; this time he sought damages under the UK

[11] [2016] QB 1003
[12] Directive 95/46/EC of 24 October 1995
[13] [2015] 2 CMLR 689

Data Protection Act for distress caused by Google's processing of his personal data. By now, it had been established by the judgment of the Grand Chamber in the *Google Spain* case[14] that an internet service provider such as Google was indeed a data controller, so that defence was not available. Instead, Google argued unsuccessfully that it fell within an exemption for caching information as an intermediary (as it would do, for example, with regard to an email sent by one person to another), or, alternatively, that what Mr Mosley was looking for amounted to a general monitoring obligation, which member states were not entitled to require. Once again the judge did not have to determine these issues but merely decide whether the case had a real prospect of success. He decided that it did, and that the questions were of general public interest, and the case proceeded.

Defamation and freedom of expression in the digital age

The conflict between freedom of expression and the right to protection of one's reputation is not a new one. It is fully recognised in the Convention on Human Rights. In the UK, the Human Rights Act 1998 includes a provision[15] which ensures that a court may not, as a general rule, grant an order (such as injunction or, in Scotland, interdict) restricting the Convention right to freedom of expression without having given the person against whom the order is to be granted an opportunity to be heard.

The digital era has created new challenges for the law of defamation. It has brought worldwide publication within the reach of anyone with a computer or a smartphone, and this, together with the disinhibiting effect of comparative anonymity, has enabled defamatory material to be created and shared which previously, due to editorial control, would never have seen the light of day. The author is, of course, liable for defamation in the usual way, if he or she can be identified and is worth suing. But our jurisdictions have had to address the issue of the liability of intermediaries: web-hosting services; facilitators of online message boards and comments on articles; and, most controversially of all, search engines. The balance between legitimate protection of reputation and suppression of free speech has proved to be a difficult one to strike.

In the UK, the current response is a mixture of home-grown and EU-inspired solutions.[16] Under section 1 of the Defamation Act 1996 (which is not specific to digital communication), a person has a defence if he shows that he was not the author, editor or publisher of the statement complained of; that he took reasonable care in relation to its publication; and that he did not know, and had

[14] *Google Spain SL v Agencia Española de Protección de Datos* (Case C-131/12)
[15] Section 12
[16] For a recent discussion, see the Scottish Law Commission Discussion Paper No 161 on Defamation (2016)

no reason to believe, that what he did caused or contributed to the publication of a defamatory statement. A number of internet service providers have successfully argued that they were not the author, editor or publisher of material complained of. In *Metropolitan International Schools Ltd v Designtechnica Corp*[17] Eady J held that the snippets appearing in response to a Google search did not constitute 'publication' because of the practical difficulty of controlling what appeared in response to a user's search terms. In *McGrath v Dawkins & Others*,[18] Amazon was held not to be the publisher of allegedly defamatory comments in book reviews, but the judge allowed the question of whether reasonable care had been taken to go to trial.

A separate protection for 'information society services' is afforded by the Electronic Commerce (EC Directive) Regulations 2002. The defence available depends upon the degree of involvement of the intermediary. 'Mere conduits', such as services transmitting but not storing emails, attract complete immunity. Providers of caching services, where information is stored for efficient onward transmission, obtain immunity if various conditions are met. Web-hosting service providers are protected from civil and criminal liability if they show that they did not have actual knowledge of 'unlawful' information, that they were not aware of facts or circumstances from which it would have been apparent to them that the information was unlawful, and that on becoming aware they acted expeditiously to remove or disable access to the information. The Court of Justice has ruled, in the context of trade mark infringement, that this defence is available to a search engine provided its role is 'merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores'.[19]

Further specific protection for website operators has now been provided in England and Wales (but not Scotland) by section 5 of the Defamation Act 2013. An operator has a defence to an action for defamation if it shows that it did not post the statement complained of. This defence is however defeated if the claimant shows that it was not possible to identify the poster; the claimant gave the operator a notice of complaint; and the operator failed to respond promptly to the complaint. These basic provisions are fleshed out by regulations specifying,[20] among other things, how to complain, how the operator must respond initially, what the operator must do if the original poster does not react, and so on. The purpose is to strike the desired balance between protection of the person complaining and freedom of speech, but the procedure is so prescriptive that one suspects that many operators will adopt the simpler course of removing the contentious material, to the potential detriment of free speech.

[17] [2011] 1 WLR 1743
[18] [2012] EWCA 83
[19] *Google France v Louis Vuitton Malletier* [2010] ECR I-2417.
[20] The Defamation (Operators of Websites) Regulations 2013

Continuing uncertainties

Inevitably with so many different attempts to address the issue of defamatory online material, there are anomalies and uncertainties. It is not clear, for example, whether liability attaches to a hyperlink to a webpage containing defamatory material; in Canada it has been held that it will only do so if the text indicates adoption or endorsement of the hyperlinked text.[21] On other matters, different jurisdictions have reached varying decisions. In New Zealand the High Court refused to strike out a claim that Google was a publisher of snippets and hyperlinks to allegedly defamatory website material.[22] In a case with somewhat bizarre facts, the Supreme Court of South Australia held that Google was a publisher of snippets and of defamatory autocomplete search results in circumstances where they were not taken down within a reasonable time after a complaint had been made.[23]

And it may not even suffice to take a defamatory statement down promptly after complaint. In *Delfi v Estonia*,[24] a large internet news portal published an article critical of a ferry company and a member of its board. This attracted comments many of which contained personal threats and humiliating and defamatory statements directed against the board member. The Grand Chamber of the European Court of Human Rights upheld the judgment of the Estonian Supreme Court that the internet portal was the publisher of the comments which because of their content did not attract article 10 protection. The news portal was professionally managed, was run on a commercial basis, and sought to attract comments on news articles published. Moreover, the portal exercised a substantial degree of control over the comments which were published, and its role was more than that of a passive service provider. The obligation to remove such comments without delay following publication (even before receipt of a complaint) did not amount to a disproportionate interference with Delfi's freedom of expression.

Other private law rights

Protection of reputation against defamation is not the only situation in which the article 10 right to freedom of expression can come into conflict with the interests of others. Some examples are hate speech, revenge porn, and other abuses of social media which do not actually amount to defamation. One solution, which has been adopted to some extent in Scotland, is to criminalise certain types of activity of this kind. But this is a risky strategy. The choice of activity to be criminalised tends to be influenced by popular pressure, and if not carefully

[21] *Crookes v Wikimedia Foundation Inc* [2011] SCC 47
[22] *A v Google New Zealand Ltd* [2012] NZHC 3252
[23] *Duffy v Google Inc* [2015] SASC 17
[24] (2016) 62 EHRR 6

thought through can lead to breach of article 10 rights. I note that the newly-enacted Digital Economy Act 2017 (which does apply to Scotland) includes, following a late amendment in the House of Lords, an obligation on the Government to issue a code of practice to providers of social media platforms such as Facebook, containing guidance as to what action to take against use of their platforms by individuals for the online bullying, insulting or humiliation of others. No sanctions are specified. Whether this constitutes an effective means of reducing online abuse of freedom of speech, and consequent protection of article 8 rights, remains to be seen.

The role of the courts

The picture that emerges from this brief survey is a complex one in which both the legislature and the judiciary have participated in the response of the law to digital technological change. In some areas, notably interception of private communications for purposes of national security – or indeed broader purposes – governments will prefer to regard the development of the law as a matter for them and not for the courts. But they have not had it all their own way. The courts are bound to apply supra-national law such as rulings of the two European Courts and the underlying Conventions and Treaties, and it will be apparent from what I have said that, in the UK at least, such challenges have often been successful. If nothing else, they have compelled disclosure by the UK Government of the extent to which it would wish to interfere – and does interfere – with privacy rights for purposes going beyond what many would regard as core protection such as the prevention of terrorism. They have exposed, for example, the extent to which the government would wish, if it could, to override safeguards such as legal professional privilege and journalists' confidentiality. But the participation of the courts has extended beyond shedding light on executive practices; the Court of Justice in particular has taken a hard line on the acquisition and retention of bulk data, and has undoubtedly had an influence on the development of national law on this controversial subject. When the UK Government returns its attention to bringing the Investigatory Powers Act 2016 into force, it will have to give consideration to the consequences for this new legislation of the judgment of the Court of Justice in the Watson reference, and in particular for the production of a code of conduct regarding retention of bulk data. It will be surprising if the matter does not end up back before the courts, who will once again have to examine the relationship between national legislation and the fundamental rights guaranteed by the Convention and the Charter.

In matters not involving national security, the courts have an equally important role to play. Once again fundamental common law rights, as well as Convention and Charter rights, will be invoked and will have to be protected where

appropriate. Even where the legislature has attempted to provide solutions by micro-management, as is the case with the liability of website operators, this can never be a complete solution. Search engines perform a valuable social function – indeed it might be argued that in the internet age they are an indispensable utility – but experience has shown that they can be manipulated to produce damaging interference with privacy rights. Developing technology will constantly test the proper interpretation of expressions such as publisher and publication. Just as the courts have had to apply concepts created many years ago for printed media to digital dissemination of information, comment, abuse, deliberate misinformation, and everything else, so they will continue to have to apply concepts created for the technology of the day to the technology of two, five or ten years into the future, which will be just as challenging.

New dangers?

I offer one further – and controversial – matter for consideration. The subject of 'fake news' has come to the fore in the course of the last year, most notably because of the alleged influence of inaccurate information disseminated online during the 2016 US presidential election. The expressions 'fake news', and its associate 'alternative facts', have given rise to light-hearted comment in the traditional media, but they are a very serious matter indeed. When a substantial part of the population receives its diet of news of current affairs by means of Twitter, in which complex issues are reduced to a few words that make misrepresentation virtually inevitable, there arise concerns that the democratic process could be overwhelmed by extremist propaganda, as has happened in the not too distant past.

My question is simply this: is any private law right of individuals engaged by the promulgation and repetition of non-defamatory but false factual assertions? If so, what would be the foundation of such right? Is article 8 of the Convention sufficiently broad to encompass an interference with personal life consisting of telling lies to the world at large? Probably not: it would normally be difficult to establish 'victim' status. Is there, then, a need for a new form of *actio popularis*, recognising a public interest vested in an individual to challenge the publication of misinformation and prevent it from exerting a malign influence? In the UK, the Supreme Court has demonstrated its readiness to depart from the old concept of title to sue to a more flexible notion of sufficient interest.[25] Or would this represent a wholly unjustifiable interference with freedom of expression, falling outside any of the categories listed in Article 10 where such freedom may legitimately be restricted?

[25] See eg *AXA General Insurance Ltd v HM Advocate & Others* [2012] 1 AC 868

Recent experience has shown that the courts are sometimes called upon to tackle issues that politicians, mindful of possible press reaction (including reaction from purveyors of fake news), are hesitant to address. Nor does there appear to be sufficient appetite on the part of the social media providers such as Facebook and Twitter to do anything unless and until legally obliged to do so. The problem seems to be growing. One day someone is going to ask a judge to take action to prevent the repetition of an item of non-defamatory fake news. What will the answer be?