right to do the act complained of, but as the supply of items (the films) the necessarily contemplated use of which by the cinema proprietor would inevitably fall within the public performance right in relation to those items. In those circumstances, if there had not been an express grant one would surely have been implied. That can be seen from the comments of Whitford J in *CBS v Ames*:

> "In my judgment, in the context of [*Falcon v Famous Players*], it is quite plain that a person who hires out a film to a cinema proprietor can sensibly be said to be purporting to grant authority for the showing of the film … The decision in [*Falcon*] I think went against the defendants because they plainly purported to grant the right to show the film."

In *Amstrad* itself, Lord Templeman said of *Falcon*: "the hirer sold the use which was only capable of being an infringing use". That statement is firmly rooted in the factual context of *Falcon*. Hiring out a film to a domestic customer would not have carried an implied grant of the right to perform in public.[337]

It would seem to follow that if, instead of the film in *Falcon* having been rented to the cinema by the film company who made it, a copy had been provided to the cinema by some avowedly illegitimate source, such a source would also have "sold the use which was only capable of being an infringing use". In that situation, disavowal of any right to make the grant would presumably have been no obstacle to the implication of a purported grant, if the implication is made necessarily from the objective nature and circumstances of the transaction. If that is right, it is unnecessary to resort to notions of "sanction, approve, and countenance" in order to find authorisation in such circumstances.

2–218 **Supply of records for private performance** Similar judicial observations have been made about sale of records. The first was by Buckley LJ in 1913, in *Monckton v Pathe Freres*:

> "The seller of a record authorises, I conceive, the use of the record, and such user will be a performance of the musical work."

[337] See *CBS v Ames* [1982] Ch. 91, discussed below, for an unsuccessful attempt to hold a business that lent out records to private customers liable for authorising home taping of the rented records.

This is a potentially confusing statement,[338] since mere private performance of a work (as opposed to public performance) requires no permission under UK copyright law. As stated by the Gregory Committee in 1952[339]:

> "It is no infringement to sing a copyright song or to play a piece of copyright music or a gramophone record in private,[340] neither is it an infringement to listen in private to a wireless programme of copyright music."

In *CBS v Ames*[341] Whitford J said:

> "… there is no doubt that anybody purchasing a record would immediately assume that he was being authorised to play it, but no more than that."

Again no permission under copyright was required to play a record in private and Whitford J's statement should not be read as suggesting that it was. The point of the statement was to emphasise what such a sale does *not* authorise (in that case home taping of rented records, which would infringe the reproduction right). However, these statements as to what right is impliedly granted by a sale or supply have significant implications for digital works, as discussed below.

Supply of records for public performance Staying with the analogue world for the moment, different considerations arise where records are supplied for use in public places. If *Falcon* had concerned the hire of a record to the cinema for the express purpose of being played to the audience in the interval, then the hire of the record would have carried the same implication as did the hire of the films. 2–219

What then would have been the position if the supplier hired 50 records to the cinema, leaving the cinema to decide which to play? The contemplated use (public performance) would have been the same. But the nexus between the agreement to supply and the performance would be thinner, since the cinema

[338] Thus the reference to Buckley LJs' observations by Lord Templeman in *Amstrad* [1988] R.P.C. 567 at 1053F "In [*Monckton*] a performance of the musical work by the use of the record was bound to be an infringing use and the record was sold for that purpose" is puzzling. Only a public, not a private, performance would have infringed and the purpose for which a record is sold in ordinary circumstances is private use and consumption (see *Thompson v Warner Brothers Pictures Ltd* [1929] 2 Ch. 308 CA per Russell LJ at 336 and Lawrence LJ at 331). *Monckton* (decided in 1914) concerned ordinary sales, not sales for the purpose of public performance. Confusion may have arisen because it was not until *Thompson v Warner Brothers*, 15 years after *Monckton*, that it was settled that the author's sole right to make or authorise the making of mechanical copies newly created by the 1911 Act did not, as argued by the plaintiffs in that case, carry with it a sole right to sell or otherwise exploit (including by any kind of performance) the mechanical recording. In any event Buckley LJ's comments were obiter (*Thompson* at 336), since the infringement actually found in *Monckton* was secondary infringement by sale with relevant knowledge.

[339] Gregory Committee October 1952 Cmd.8662 [125]. And see *Thompson v Warner Brothers Pictures Ltd* [1929] 2 Ch. 308 CA.

[340] This held true regardless of whether the sheet music and lyrics from which the song was sung or played, or the vinyl record which was played, were themselves licensed or not under the reproduction right. Matters are less simple in the digital era. While it remains true that the public performance right is not engaged by playing a work in private, a private performance can potentially engage the reproduction right due to the temporary copies made in the memory of the user's device in order to play the work. See section 2.14.1.

[341] *CBS Inc v Ames Records and Tapes Ltd* [1982] Ch. 91.

proprietor would have had the control over which records (if any) to play. In the same vein, would it make any difference if the supplier had hired the gramophone as well as the records?

2–220 **Juke boxes** Such issues arose with juke boxes. Typically, a company would rent a juke box and a supply of records to, for instance, a restaurant for the use of its customers. In this situation the nexus is yet thinner, since (within the constraints of the selection of records supplied) what is played depends not on the supplier's customer, but on the supplier's customer's customers.

In *Vigneux v Canadian Performing Right Society*[342] Vigneux hired the juke box and records to a restaurant for the use of its customers at a fixed weekly rental, visiting once a week to collect the rental and change the records as necessary. The Privy Council, perhaps surprisingly focusing more on the hire of the machine than the selection and supply of the records,[343] found there was no authorisation:

> "They had no control over the use of the machine; they had no voice as to whether at any particular time it was to be available to the restaurant customers or not. The only part which they played in the matter was, in the ordinary course of their business, to hire out to [the restaurant] one of their machines and supply it with records, at a weekly rental of 10 dollars … Vigneux supplied the machine in the ordinary course of business, at a fixed rental; they had no interest beyond that."

In *Winstone v Wurlitzer*[344] the Supreme Court of Victoria commented on *Vigneux*:

> "The only control moreover referred to by their Lordships was control over the use of the machine, which was the means of giving the performance complained of. No consideration was apparently given to the question of control over the content of the performances, that could be given by means of the machine. And it would seem relevant to the question whether Vigneux … granted or purported to grant [the restaurant proprietor] and his customers the right to do the act complained of, to know whether or not they controlled the selection of the records that were to be placed in the 'juke box' from time to time, and so determined what musical compositions could, if and when it was put into operation by [the restaurant's] customers, be performed thereon. Actually … it was not clear just what the position was in this regard."

[342] *Vigneux v Canadian Performing Right Society Ltd* [1945] A.C. 108 PC. The finding of no authorisation was obiter and apparently not argued. In Australia, the supplier of a juke box and records who operated on a profit-sharing arrangement was found liable for authorisation (*Winstone v Wurlitzer Automatic Phonograph Co of Australia Pty Ltd* [1946] V.L.R. 338.

[343] Whitford J in *CBS v Ames* [1982] Ch. 91 commented: "I find it somewhat curious that no reference was made in this judgment to the fact that Vigneux, in addition to supplying the equipment for playing the records, also supplied the records, and could quite plainly only anticipate that any records they were supplying would be taken as records which it was open to customers to have played on the insertion of an appropriate coin. On any basis the case against Vigneux was very much stronger than the present case. It was a case of supplying both records and the equipment which could perform and would perform what would be a limited repertoire of records." The suggestion that the Privy Council judgment made no reference at all to the supply of records is not correct. However they clearly focused more on the hire of the machine.

[344] *Winstone v Wurlitzer Automatic Phonograph Co of Australia Pty Ltd* [1946] V.L.R. 338.

These passages could suggest that authorisation may in some circumstances be easier to establish where copies of the work itself are supplied, rather than devices or facilities capable of being used to infringe copyright in third party works (as to which see below). However, it does not follow that awareness of the likelihood that customers will choose to make copies of the work supplied amounts to authorisation.

2–221 **Lending records and sale of blank tapes** Thus in *CBS v Ames* the defendant company owned a chain of retail record shops. The plaintiff companies sold records to it. The defendant instituted a record lending library scheme. Customers who joined were charged an initial membership fee and a further fee for each record borrowed. Members were also offered discounts on purchases, including 5% on blank tapes. Non-member customers were offered the same purchase discounts if they bought sufficient quantities of goods. Initially there were no warning notices against infringement. Later the defendant, at the request of the plaintiffs (through the MCPS), displayed warning notices in the shops and affixed warning stickers to the record sleeves and tape covers. It also introduced a form signed by all library members containing a warning.

2–222 The plaintiffs alleged that the defendant was liable for authorising infringement by members of the lending library, on the basis that it knew that infringement would take place and was seeking to take commercial advantage of it. Their case was that the scheme was embarked on

> "in the full knowledge of the fact that the record companies would object, in full knowledge of the fact that it would be detrimental to the interests of the record companies, and in full knowledge that substantially all the people hiring would be home taping."

The defendant's proprietor, Mr Ames, accepted that at all times he realised that records borrowed from his library might be home taped, as indeed records purchased might be by friends of the purchaser, but said that he did not start the library scheme in order to make money out of home taping.

2–223 Whitford J found that at no time had Mr Ames, whom he found to be a frank and fair witness,[345] expressly sanctioned, approved or encouraged home taping. He also rejected the assertion that the whole of the scheme was set up by Mr Ames to enable him to make money from members of the public who he must have known would only be borrowing records to make tapes from them. Mr Ames did accept that he knew that there would be likely to be some home taping of the library records.

The judge also found that up to the time of the intervention of the MCPS intervention the defendant was indifferent to the possibility or indeed the probability that a proportion of borrowers would home tape. Since the MCPS intervention warning notices and stickers had been displayed and applied.

Whitford J held (in a passage cited by Lord Templeman in *Amstrad*):

[345] As will be seen in the internet cases discussed below, the court's assessment of the good faith (or lack thereof) of the person alleged to have authorised infringement may in practice strongly influence the court's decision.

All satellite radio receivers had memory buffers containing a rolling 4 to 10 seconds of the most recent transmitted content. This buffer provided smooth listening, avoiding any interruptions dues to momentary interruptions in transmission.

Some models also had an automatic extended buffer. This buffer stored 44 to 60 minutes of programming on the channel to which the subscriber chose to listen. It enabled live pause and replay. The content stored in the buffer was lost if the subscriber turned off the receiver or changed channel.

Other models also had a block recording feature. If the subscriber engaged this feature then up to 10 or 100 hours of broadcast content were automatically copied and stored for later replay.

The Federal Court of Appeal had to consider whether the service provider authorised the copying that took place in the extended and block recording buffers.[352]

2–229 The Court summarised as follows the principles under Canadian law as enunciated in the *CCH Canadian Ltd v Law Society of Upper Canada*[353] decision:

- Where a person authorises the use of equipment that may be used lawfully but may also be used unlawfully to infringe copyright, it must prima facie be presumed that the person authorised only the lawful use of the equipment.
- That presumption is not rebutted by a notice warning a person who is permitted to use equipment that certain uses could infringe copyright.
- The presumption may be rebutted if the person authorising the use of the equipment is, by virtue of its relationship with the user of the equipment, in a position to control the use of the equipment such that it may be said to have sanctioned, approved or countenanced any infringement resulting from the use of the equipment.

2–230 The Court said that the satellite radio service providers might be said to authorise their subscribers to use all features of the radio receivers with which they were supplied. It was appropriate that they be given the benefit of the prima face presumption against authorisation of the use of the receiver to infringe. The question was whether that presumption had been rebutted. That turned on the degree to which the service providers controlled the use of the receivers supplied to their subscribers.

It was important that the subscriber could not prevent the copying of broadcast content without turning the receiver off or, if the receiver had a block recording

[352] As to the 4–10 seconds buffer, the Federal Court of Appeal declined to interfere with the Copyright Board's determination that this buffer did not amount to a copy of an entire work or a copy of a substantial part of a work. The relevant works for this aspect of the case were musical works. For UK cases see the discussion of temporary copies in section 2.14.1.

[353] *CCH Canadian Ltd v Law Society of Upper Canada* [2004] 1 S.C.R. 339; 2004 SCC 13. The articulated scheme of presumption and rebuttal does not correspond with UK law. The case concerned provision of a photocopier for unmonitored self-service use by patrons of the Law Society library. The Court found that the Law Society was not liable for authorisation. It did not exercise control over patrons who might commit infringement, nor over the works that patrons chose to copy, their purposes of copying or the photocopiers themselves. Contrast the Australian case of *University of New South Wales v Moorhouse* (1975) 133 C.L.R. 1.

feature, by disengaging it. Because the copying was automatic, the only control that could be exercised over copying initiated by the subscriber rested with the satellite service providers. They alone knew what was being broadcast and when, and what broadcast content was subject to copyright. They alone had chosen to supply their subscribers with receivers that precluded them from exercising any choice as to what was copied in the extended buffer once the receiver was turned on, and any choice as to what was copied when the block recording feature, if any, was engaged.

Although not all broadcast content was subject to copyright, in practical terms the use of a satellite radio receiver as it was intended to be used would always result in the making of infringing copies because of the technological choices made by the satellite radio service providers.

The presumption against the authorisation of an infringing act was rebutted by the degree of control exercised by the satellite radio service providers over their broadcast content and the features included in the radio receivers supplied to their subscribers.

2–231 The more interesting aspect of the Canadian judgment relates to the block recording buffer. This was not completely automatic, in the sense that the subscriber had the choice whether to use it or not. Nonetheless it was provided as an ordinary feature of the service. Analysed in *Amstrad* terms, it would not be difficult to conclude that, by supplying both the content and the feature together, the service provider was purporting to grant the subscriber the right to copy the supplied content by means of the supplied feature.

There was some discussion in the judgment of whether copyright notices which warned the subscriber against certain impermissible uses (such as public performance) could be relied upon to justify the conclusion that the service provider purported to have the authority to allow uses that were not warned against in the notice, i.e. private copying. While the Court declined to draw that inference, it did comment that

> "the satellite radio providers could not realistically have advised their subscribers against making infringing copies, because the copying was automatic in the case of a receiver with an extended buffer, and in the case of a receiver with a block recording feature when it was engaged."

2–232 **Remoteness from the allegedly authorised infringement** Authorisation of a user's automatic copying by loading into RAM or buffer memory does have limits. If the seller is too remote from the end user who loads the supplied copy of the work into memory when using the supplied device, then the seller will not be taken to have authorised the end-user's copying. *Philips v Salton*,[354] a post-*Amstrad* decision, is an example.

The case concerned a coffee making machine containing control software which, when the machine was used, would automatically be copied temporarily in the machine's microcontroller. One of the parties to the litigation was a Hong Kong company which was said to have designed, or had designed on its behalf, the allegedly infringing software. The two companies in the supply chain between it and the UK, who were themselves defendants, alleged that it had authorised: (a)

[354] *Philips Domestic Appliances and Personal Care BV v Salton Europe Ltd* [2004] EWHC 2092 (Ch).

Over a century ago *De La Bere v Pearson Ltd*[22] illustrated the pitfalls of giving personal advice. A newspaper advertised that its City editor would answer inquiries from readers of the paper desiring financial advice. The paper published a reader's question asking for the name of a good stockbroker, together with a reply recommending someone who the editor ought to have known, if he had made proper inquiries, was an undischarged bankrupt. The reader dealt with the stockbroker and lost his money.

The case was brought in contract, the consideration for the contract being said to be either the publication of the reader's question or the addressing of the inquiry. The newspaper was found liable. That was described by Lord Devlin in *Hedley Byrne* as a "just result". Nowadays, given the development in negligence liability since *Pearson*, it would probably be unnecessary to force the facts into the straightjacket of contract theory.

5–012 **No new principles** Interactivity does not give rise to any new legal principles. *Patchett v SPATA*[23] was the first case on negligence liability for incorrect information on a website to reach the English courts. The Master of the Rolls observed, in response to the suggestion that special considerations applied to representations on websites, that the mere fact that the representations were contained on a website did not support the conclusion that a duty of care is owed:

> "As ever, all depends on the circumstances. Some websites are interactive and it may be possible … to conclude in particular circumstances that a duty is owed."[24]

Scott Baker LJ in the same case said:

> "I too would like to emphasise that no different legal principles apply to misrepresentations on a website than to those anywhere else in the public domain."[25]

(c) Mass advice

5–013 The second factor exacerbating the potential for online liability is that the lower cost of providing information electronically permits wider and easier dissemination of the information. The result is that it becomes economic to provide, electronically, the sort of information and quasi-advice that previously had to be custom-made and delivered personally by professional advisers. This may parallel the developments in the market for goods which preceded the imposition of manufacturers' liability for defective goods in *Donoghue v Stevenson* in 1932.

5–014 **World at large** In *Candler v Crane, Christmas & Co*,[26] a case concerning liability for accounts, Lord Denning commented:

[22] *De La Bere v Pearson Ltd* [1908] 1 K.B. 280.
[23] *Patchett v Swimming Pool & Allied Trades Assoc Ltd* [2009] EWCA Civ 717.
[24] *Patchett v SPATA* [2009] EWCA Civ 717 at [40].
[25] *Patchett v SPATA* [2009] EWCA Civ 717 at [42].
[26] *Candler v Crane, Christmas & Co* [1951] 2 K.B. 164.

> "… a scientist or expert (including a marine hydrographer) is not liable to his readers for careless statements in his published works. He publishes his work simply for the purpose of giving information, and not with any particular transaction in mind at all. But when a scientist or an expert makes an investigation and report for the very purpose of a particular transaction, then, in my opinion, he is under a duty of care in respect of that transaction."

Thus there is no general liability for mere information made available to the world at large. The courts have resisted imposing liability for pure economic loss "in an indeterminate amount for an indeterminate time to an indeterminate class".[27]

5–014A **Foreseeable reliance by limited class** However *Patchett v SPATA*[28] demonstrates that where information is made available to the world, if it will foreseeably be relied upon by a limited class of persons then a duty of care to those persons may be capable of arising (although in that case, the majority of the Court of Appeal held that on the facts it did not do so). The more recent case of *Taberna v Selskabet* (discussed below) reinforces the point.

5–015 **Incorrect information about membership of trade association** *Patchett v SPATA* concerned incorrect information on the defendant trade association's website. The claimants were looking for a contractor to build a swimming pool. Mr Patchett went to the trade association website, which provided a drop-down list of association members, from which he selected the contractor that he ultimately employed. Association membership was said to provide a number of advantages, including having been fully vetted by SPATA with checks on their financial record and experience in the trade, and membership of SPATA's SPATASHIELD bond and warranty insurance scheme. The website also stated that SPATA supplies an information pack and members' lists, which give details of suitably qualified and approved installers in the customer area.

The contractor got into financial difficulties, ceased trading and did not complete the works. It transpired that the contractor was only an associate member of SPATA, not a full member. Only full members underwent checks and vetting and were covered by the SPATASHIELD scheme. While the drop-down list on the website gave no indication that there were two types of member, the information pack would have revealed the true position.

5–016 While the claimants' claim for negligent misstatement failed (on a 2:1 majority), it did so on the specific point that (according to the majority of the Court of Appeal) it was to be expected that a user of the website would obtain the information pack, so that the requirement that the recipient of the representations would act without independent enquiry was not satisfied. Apart from that point, it is possible that the Court of Appeal would have held that a duty of care arose (Smith LJ, dissenting, thought they would have done[29]). The Master of the Rolls (one of the majority) had this to say:

[27] *Caparo Industries Plc v Dickman* [1990] 2 A.C. 605 at 621 per Lord Bridge.
[28] *Patchett v Swimming Pool & Allied Trades Assoc Ltd* [2009] EWCA Civ 717.
[29] *Patchett v Swimming Pool & Allied Trades Assoc Ltd* [2009] EWCA Civ 717 at [51].

Further, in the *SABAM* CJEU cases, the starting point for filtering was works in respect of which the rightsholders claimed to hold rights (see para.5–339 above). It is difficult to see how in *Rapidshare III* notifying a list of infringed works would render the monitoring obligations less general than those considered in those cases.

5–348 In the English case of *Mosley v Google* Mitting J, declining to grant summary judgment to the defendant search engine,[458] held that since it was common ground that existing technology permitted Google, without disproportionate effort or expense, to block access to individual images, as it could do with child sexual abuse imagery, the evidence might well satisfy a trial judge that Google could do so without impermissible monitoring.

5–349 In *X v Twitter Inc*,[459] a decision of the New South Wales Supreme Court, Pembroke J made an order requiring the defendant (who did not appear in the proceedings) to prevent further publication of "information contained in or referred in" certain tweets, as well as an order directed to future tweets from particular users. In the absence of evidence from Twitter, the judge accepted that there must be a mechanism to filter information on the Twitter service and did not consider it unreasonable or inappropriate to make orders imposing a requirement for the application of some degree of filtering or checking to ensure that the information did not get posted or, if it was posted, was removed.

5.6.6 Account termination and identity provision injunctions

(a) Account termination

5–350 The CJEU in *L'Oreal v eBay* commented that if the operator of the online marketplace did not decide, on its own initiative, to suspend the perpetrator of the infringement of intellectual property rights in order to prevent further infringements of that kind by the same seller in respect of the same trade marks, it could be ordered by means of an injunction to do so.

5–351 An injunction terminating an internet access account goes further. It is more invasive of fundamental rights (in particular the right of freedom of expression) than one terminating a specific service such as a seller's account on an online auction platform. A general purpose internet connection has substantial non-infringing uses—all the more so if the connection is used by others, for instance within a household.

5–352 The Danish Supreme Court, in a case brought by the International Federation of the Phonographic Industry, held in February 2006 that an ISP given notice of illegal filesharing could be required, if necessary by injunction, to disconnect the service of the customer in question.[460] The Court relied heavily on the InfoSoc Copyright Directive art.8. The Finnish courts have granted similar orders

[458] The case was conducted on the footing that Google's search engine activity could be within the art.13 caching exemption (see paras 5–117 and 5–192 above).

[459] *X v Twitter Inc* [2017] NSWSC 1300 at [35] to [37].

[460] (2006) 11(9) E.C.L.R. 243; IFPI press release: *https://web.archive.org/web/20130902082957/http://ifpi.org/content/section_news/20060215.html* [Accessed 21 November 2019].

requiring ISPs to disconnect P2P file sharers.[461] In January 2014, the Provincial Court of Barcelona ordered an ISP permanently to cease providing internet access to a user who had infringed by peer to peer sharing 5,100 music tracks.[462]

5–353 In *X v Twitter Inc*[463] (above), the Australian court made an order requiring Twitter to suspend certain users' existing accounts and future accounts opened by those users.

(b) Identity provision

5–354 **McFadden** In September 2016, the CJEU delivered its judgment in *McFadden*, concerning the liability of a shop with a free Wi-Fi facility for copyright infringement by its users.

The Court considered what obligations an injunction to prevent copyright infringement might legitimately impose on the proprietor of the shop; in particular whether some specific kinds of obligation are prohibited under the EU Charter of Fundamental Rights.

The German referring court was considering the possibility of granting an injunction requiring the shop to prevent third parties making a particular copyright work available to the public from a P2P platform. On the facts, although the shop could decide what technical measures to take to comply, in practice the only measures that it could take were to terminate or password-protect the internet connection or to examine all communications passing through it.

5–355 The CJEU held, for each type of possible measure:

- Monitoring all the information transmitted was impermissible as contrary to the prohibition on general monitoring obligations in the Electronic Commerce Directive art.15.
- Terminating the internet connection completely would cause a serious infringement of the freedom to conduct business. It would categorically prevent an internet access provider from pursuing that activity in order to remedy a limited infringement of copyright without considering the adoption of measures less restrictive of that freedom. In those circumstances, such a measure would not strike a fair balance between the fundamental rights concerned.
- Securing the connection by password protection was not an impermissible measure. Such a measure did not damage the essence of a service provider's freedom to conduct business in so far as it was limited to "marginally adjusting one of the technical options open to the provider in exercising its activity".

[461] See M. Norrgård, *Blocking Web Sites—Experiences from Finland* (1 February 2012). Available *https://ssrn.com/abstract=1997103* [Accessed 7 October 2019] or *http://dx.doi.org/10.2139/ssrn.1997103* [Accessed 7 October 2019].

[462] See *https://torrentfreak.com/court-orders-spanish-isp-to-disconnect-music-pirate-140120/* [Accessed 7 October 2019].

[463] *X v Twitter Inc* [2017] NSWSC 1300 above at [37].

proportionate from the perspective of users, such as a URL-based notification system of the type mentioned in *Newzbin2* as being open for consideration where there was substantial non-infringing use.[473]

The judge recorded in his second judgment that he had considered the proportionality of the proposed orders from the perspective of individuals affected by them who were not before the Court and, having undertaken that exercise, was satisfied that the orders sought were proportionate for similar reasons as in *20C Fox v BT*[474] (at [199]–[200]). He considered that the present case was, if anything, a stronger one for the making of such orders for the reasons indicated in the first judgment.[475]

5–367 There was no doubting in *Dramatico* the notorious history of The Pirate Bay, reinforced by material on its website revelling in a display of contempt for copyright and for take-down notices. Indeed, AG Szpunar in the later CJEU *Pirate Bay* case considered that the behaviour of the site operator was relevant to the assessment of proportionality.[476] Nevertheless, for a sharing site a blocking injunction at the site level heavily engages the separate fundamental rights of the site's actual and potential users, especially where there is potential for substantial non-infringing uses.

(c) Scope expansion

5–368 In *Newzbin2*, the scope of the injunction sought was widened between the first and second judgments, on the basis of evidence of steps that Newzbin2 was expected to take to enable users to circumvent the injunction. In *Dramatico*, the order included IP address blocking, on the basis of evidence that otherwise the BT Cleanfeed system could be circumvented and that The Pirate Bay's IP address was not shared. In both cases, the Court considered that the extended scope was proportionate. In *Cartier v BSkyB*, IP address blocking was extended to shared IP addresses, with the safeguards discussed above at para.5–313.

Desire to achieve effectiveness and to prevent circumvention, where neither goal may be fully achievable, has the potential to stimulate a cycle of increased scope and complexity. Cory Doctorow in his article "Lockdown: the Coming War on General Purpose Computing" identified a similar effect: "Each regulation begets a new one, aimed at shoring up its own failures".[477]

Such a cycle carries a risk of taking the court into areas that it may be ill-equipped to remedy or police. One example could be said to be the order in *Cartier v BSkyB* (a trade mark site blocking case) regarding notification of shared IP addresses (para.5–313 above), with its provision for the claimant's solicitors to certify the existence of "unlawful activity".

[473] In an Italian case the Rome Court of Appeals overturned a site blocking order issued by the Rome Public Prosecutor against ISPs in relation to a video site. One of the grounds is reported to have been that a whole site order was too broad and that individual URLs should have been specified. ("Italian Court Orders ISPs to Unblock Torrent Site Filmakerz.org" *Softpedia* 3 April 2014.

[474] *20th Century Fox Film Corp v British Telecommunications Plc* [2011] EWHC 1981 (Ch).

[475] The question of proportionality is dealt with shortly in the second judgment (*Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 1152 (Ch) at [12]), referring back to [21]–[29] and [75]–[81] of the first judgment ([2012] EWHC 268 (Ch)).

[476] *Stichting Brein v Ziggo* (C-610/15) Opinion of AG Szpunar, 8 February 2017 at [76]).

[477] C. Doctorow, "Lockdown: The Coming War on General Purpose Computing" at *http://boingboing.net/2012/01/10/lockdown.html* [Accessed 7 October 2019].

(d) Process

Some significant process issues have arisen out of the cases, although the safeguards gradually introduced (para.5–308 onwards above) have gone some way to ameliorating these. 5–369

Nevertheless, the lack of judicial supervision of new internet addresses notified for blocking remains a matter of potential controversy. In the Australian decision of *Roadshow Films v Telstra*,[478] the judge rejected a scheme for ongoing notification, holding that whether the terms of any injunction should be varied to refer to additional domain names, IP addresses or URLs is a matter for the court to determine in light of evidence and should be dealt with by way of further order. The order contained a procedure for obtaining such variations. Subsequent Australian site blocking orders have contained similar provisions, as has the first Canadian site blocking order (*Bell Media Inc v GoldTV.biz*).[479]

(e) Routine

As observed by Arnold J (see para.5–258 above) it is the duty of the court not simply to rubber stamp terms agreed by the parties. In *Popcorn Time*,[480] Birss J discussed when it was and was not appropriate for applications to be dealt with on paper without an oral hearing. Where the factual circumstances were the same as in cases that had previously been considered in reasoned public judgments and the ISPs did not oppose either the order or the fact of it being on paper then the court might consider that a hearing was not necessary. Similarly there was no objection to grouping multiple different and independent websites in the same application where the issues raised were the same for each website. 5–370

However, where the nature of the target sites raised new and different issues from those previously considered the claimants must ensure that they draw the court's attention to any new factors. If the matter raises substantive new issues it would be unlikely to be suitable to be dealt with on paper.

(f) Representation of target site

The court's starting position is that the target site should be notified of the application unless there is good reason not to do so, since (as Arnold J observed in *Dramatico*) the site operators would be adversely affected by the order. However, there is no report so far of a refusal of relief on the basis that the target site ought to have been notified of the application in advance or made a party. The normal form of order now provides for the target site to have liberty to apply to vary or discharge the order (see para.5–317 above). 5–371

The absence of the target site at the hearing places a premium on the accuracy, fairness and objectivity of the evidence and submissions of the rightholders; and

[478] *Roadshow Films Pty Ltd v Telstra Corp Ltd* [2016] F.C.A. 1503.

[479] *Universal Music Australia Pty Ltd v TPG Internet Pty Ltd* [2017] F.C.A. 435; *Roadshow Films Pty Ltd v Telstra Corp Ltd* [2017] F.C.A. 965; *Foxtel Management Pty Ltd v TPG Internet Pty Ltd* [2017] F.C.A. 1041; *Television Broadcasts Ltd v Telstra Corp Ltd* [2018] F.C.A. 1434; *Bell Media Inc v GoldTV.biz* [2019] F.C. 1432.

[480] *20th Century Fox Film Corp v Sky UK Ltd* [2015] EWHC 1082 (Ch).

(i) Permanence

5–377 The injunction available under s.97A and contemplated by art.8(3)[486] is a final injunction. Final injunctions are normally permanent and, subject to provision for liberty to apply in the event of material change of circumstances, is the form in which most of the ordinary s.97A blocking orders have so far been granted.

However, the football live streaming blocking orders have been limited to the duration of the football season. The *Cartier v BSkyB* trade mark blocking order contained a sunset clause based on the particular facts of that case—see para.5–317 above). The *Matchroom* boxing order[487] was limited to two years.

5–378 One of the factors that contributed to the ECJ decision in *SABAM v Scarlet* was that the injunction in that case required the ISP to install a filtering system for an unlimited period. While it seems unlikely that permanence would of itself render a blocking injunction disproportionate, permanence does appear to be a factor that ought to be taken into account when considering whether the terms of the injunction considered as a whole are proportionate.

The fewer the mechanisms for supervising the administration of the injunction on an ongoing basis and the broader the terms of the injunction, the more likely is permanence of an injunction to be an issue of concern. So the broader the scope of the injunction (e.g. extending to sites whose sole or predominant purpose is said to be to enable or facilitate access to the original site) and the less there is any court oversight of evolving matters such as ongoing notification to the ISP of URLs and IP addresses (or, in the case of live streaming orders, matches and events), the more likely it is that the proportionality of a permanent injunction could come into question.

5–379 There is also possible concern with an accumulation of notified and blocked IP addresses building up over an indefinite period of time if at some point they are no longer used by or under the control of the target site and ought to be available for use by others.[488]

5–380 The Australian copyright site blocking orders mentioned above contain both time limitations (three years) and a provision that should the applicants have a good faith belief that any target address has permanently ceased to enable or facilitate access to a Target Online Location, or has permanently ceased to have the primary purpose of infringing or facilitating the infringement of copyright, then the applicants must within 15 business days of forming such a good faith belief notify each respondent of the fact in writing, in which case the respondent is relieved of the obligation to block the target address.

5–381 In *APC v Auchan Telecom*,[489] the Paris Tribunal de Grande Instance granted copyright blocking injunctions against several ISPs and search engines. It held that in order to limit the measures to those that were strictly necessary to protect the rights in issue and also to avoid their becoming obsolete the injunction should be limited to 12 months. The Court had found that it had no power to make an

[486] *20th Century Fox Film Corp v British Telecommunications Plc* [2011] EWHC 2714 (Ch) at [35].
[487] *Matchroom Boxing Ltd v British Telecommunications Plc* [2018] EWHC 2443 (Ch).
[488] See Open Rights Group report of June 2018 (*http://www.openrightsgroup.org/press/releases/2018/nearly-40-of-court-order-blocks-are-in-error-org-finds* [Accessed 7 October 2019]).
[489] *APC v Auchan Telecom* (RG: 11/60013) 28 November 2013 Paris Tribunal de Grande Instance; Paris Court of Appeal 15 March 2016 (No.040/2016).

evolving order, but the plaintiffs could return to court to seek an updated order.[490] The orders were upheld on appeal to the Paris Court of Appeal.

(j) Transparency

5–382 There is an argument (especially in the light of the CJEU comments in *Constantin Films v UPC Telekabel* above (para.5–220) regarding access by users to the court process) that given the significant public interest aspects of a site blocking injunction there should be transparency over the ongoing notification of IP addresses and URLs, so that the block list should be available for public scrutiny. That is not the practice in the English cases.

A counter argument would be that it is undesirable to provide a public list of locations where infringing content may be found. As noted above (para.5–320), live streaming injunctions have designated some aspects of the initial order (including the identities of the target streaming servers) confidential in order to deter circumvention.

(k) Cross-border issues

5–383 The CJEU judgment in *SABAM v Scarlet* concludes with a point that will come to the fore should a site blocking injunction be sought against an intermediary with users in more than one country. A blocking injunction against a domestic fixed-line internet access provider is unlikely to raise such issues.[491] But an injunction against a mobile internet access provider could do so, as would an injunction against any intermediary whose customers or users were located in more than one country. The CJEU said this when considering the impact on the fundamental rights of users:

> "that injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned." [52]

[490] The same court made an order in similar terms a year later in respect of The Pirate Bay. *Société Civile des Producteurs Phonographiques (SCPP) v Orange* 4 December 2014 Paris Tribunal de Grande Instance.
[491] In one case it has been reported that an Austrian site blocking injunction in respect of The Pirate Bay had effects in Slovakia because a Slovakian ISP used a datacentre in Vienna for its DNS server. See *https://torrentfreak.com/austrian-pirate-bay-blockade-censors-slovak-internet-accidentally-151203/* [Accessed 7 October 2019].

social media sites blocked due to user posts insulting Ataturk[34]) and Egypt (YouTube ordered to be blocked for a month over presence of "Innocence of Muslims" video.[35]

Generally, details of such activities[36] can be found in surveys at the websites of organisations such as Amnesty International,[37] Human Rights Watch,[38] the Freedom Forum,[39] Index on Censorship,[40] Reporters sans Frontieres,[41] ARTICLE 19,[42] the Committee to Protect Journalists[43] and the OpenNet Initiative.[44]

Similar technical methods have been used to implement copyright and trade mark site blocking orders in the UK and elsewhere (see Ch.5).

The examples below are some instances in which claims under local laws enforcing cultural or other deeply held values have been asserted against internet content emanating from other countries.

6–021 **Language** France has well-known legislation, the Loi Toubon, designed to preserve the use of the French language in public places. Two pressure groups, Defence of the French Language and Future of the French language, sued the French branch of a US college, the Georgia Tech Lorraine International School, because its website was written only in English. In 1997 the action was dismissed on a technicality.

In 2014, it was reported that some retailers' English-only websites were no longer available in Quebec due to failure to comply with Quebec's French Language Charter.[45]

6–022 **The *LICRA v Yahoo!* Nazi memorabilia case** In 2000, a French court, in the case of *League against Racism and Anti-Semitism and Union of French Jewish Students v Yahoo! Inc*,[46] assumed jurisdiction over the US company Yahoo! Inc and ordered it to prevent access to Nazi memorabilia offered for sale by individuals on its yahoo.com online auction site, contrary to French law. Yahoo!

[34] In *Yildirim v Turkey* (3111/10) 18 December 2012, Turkey's blocking of Google Sites was held to have violated ECHR art.10. A similar finding was made in relation to blocking of YouTube in *Cengiz v Turkey* (48226/10 and 14027/11) 1 December 2015. An order to block Twitter was quashed by Turkey's Constitutional Court in 2014 (*http://www.reuters.com/article/us-turkey-twitter-ban-turkeys-twitter-ban-violates-free-speech-constitutional-court-idUSBREA311BF20140402* [Accessed 10 October 2019]).

[35] "Egypt Court Orders YouTube Ban" (*https://uk.reuters.com/article/uk-egypt-youtube/top-egypt-court-orders-temporary-youtube-ban-over-prophet-mohammad-video-idUKKCN1IR0FH* [Accessed 10 October 2019]).

[36] The Report of the UN Special Rapporteur on freedom of expression dated 6 April 2018, addressing the regulation of user-generated content, is also a useful source.

[37] See *http://www.amnesty.org* [Accessed 10 October 2019].

[38] See *http://hrw.org/doc/?t=internet* [Accessed 10 October 2019].

[39] See *http://www.freedomforum.org* [Accessed 10 October 2019].

[40] See *http://www.indexoncensorship.org* [Accessed 10 October 2019].

[41] See *http://www.rsf.fr* [Accessed 10 October 2019].

[42] See *http://www.article19.org* [Accessed 10 October 2019].

[43] See *http://www.cpj.org* [Accessed 10 October 2019].

[44] See *https://opennet.net/* [Accessed 10 October 2019].

[45] See *https://nationalpost.com/news/canada/retailers-forced-to-block-english-only-websites-in-quebec-or-face-sanctions-from-language-police* [Accessed 10 October 2019].

[46] English translations of the decision of 22 May 2000 and 20 November 2000 are at *http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm* [Accessed 10 October 2019] and *http://www.cdt.org/speech/001120yahoofrance.pdf* [Accessed 10 October 2019] respectively. The two

contended that the Court had no jurisdiction and that compliance with the order was impossible since it could not reliably exclude access to the site from France.

The French court found that it had jurisdiction on several bases: first, that the mere display of the items offended against French law; secondly, that although (as Yahoo! argued) some aspects of the auction site could be regarded as aimed at the US, that was not true of Nazi memorabilia, which would be of interest to anyone (including French people); thirdly, there was obvious harm to the particular plaintiffs; and fourthly, that the yahoo.com site was in any event targeting France, since it used geographical IP address filtering to serve up French language banner advertisements to users who appeared to be from France. This latter factor was doubly damaging to Yahoo!, since the Court relied heavily upon it when assessing Yahoo!'s ability to comply with the order by filtering out users coming from France.

Geo-blocking feasibility As to compliance, a three man panel of technical experts was empanelled and asked to consider whether it was technically possible for Yahoo! to comply with the order, and if not to what extent could compliance be achieved. 6–023

The panel reported that Yahoo! could exclude about 70% of users emanating from France.[47]

It could not achieve 100% for three reasons: first, a number of large ISPs (of which AoL was the best-known example) allocated IP addresses to their users from their bank of US addresses, so that a French AoL user would appear to be accessing Yahoo! from Virginia, US; secondly, users of multinational corporate networks similarly would often appear to be accessing from a country other than that in which they were located; thirdly, users could readily make use of anonymising services, which hide the IP address of the user and replace it with another one. Indeed one of the empanelled experts, Mr Ben Laurie, in a personal statement[48] after the judgment, commented that the "rather flakey guess at nationality, using IP address or domain name" could be "trivially circumvented".

The majority of the expert panel (Vinton Cerf dissenting on the feasibility of geographical filtering) suggested that the filtering effectiveness could be increased to about 90% by requiring a statement of nationality (which the court interpreted to mean geographical origin) in cases of ambiguous IP addresses.

The expert panel also examined the question of how Yahoo! should identify the material to which French users were to be denied access, such as filtering on the item descriptions and on users' search keywords.

On compliance, the Court decided that geographical localisation was possible and, in dismissing Yahoo!'s objections that this was a crude tool, relied heavily on Yahoo!'s own use of the technique to serve up banner advertisements to users 6–024

decisions, together with the expert reports, are in French on *https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-du-20-novembre-2000/* [Accessed 21 November 2019].

[47] The panel report occasionally seems to use French nationality and French location interchangeably. In context, the panel must be taken to be referring to French location, at least in the case of IP address filtering.

[48] B. Laurie, "An Expert's Apology" 21 November 2000 at *http://www.apache-ssl.org/apology.html* [Accessed 10 October 2019].

to (7). These mirror the provisions of art.3.4 of the Directive. The derogations are to be strictly construed and as exceptions to the general rule under the Directive they are exhaustive.[101]

Regulation 5(2) sets out the circumstances in which a court (which is not an enforcement authority under the Regulations, and includes any court or tribunal) may take such measures.

Regulation 5(2) provides that in any case where an enforcement authority with responsibility in relation to the requirement in question is not party to the proceedings, a court may, on the application of any person or of its own motion, apply any requirement which would otherwise not apply by virtue of reg.4(3) in respect of a given information society service, if the application of that enactment or requirement is necessary for and proportionate to any of the objectives set out in reg.5(1). As with an enforcement authority, under reg.5(3) a court may take such measures only where the information society service prejudices or presents a serious and grave risk of prejudice to an objective set out in reg.5(1).

6–091 **Notification** Article 3.4(b) of the Directive provides that prior to taking the measures in question, and without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation, the Member State must have asked the Member State with country of origin control to take measures and the latter either did not take measures or they were inadequate; and also notified the Commission and the Member State in which the service provider is established of the intention to take such measures. The Member State may in the case of urgency, take measures without complying with those conditions so long as it notifies them in the shortest possible time afterwards to the Commission and the Member State in which the service provider is established, indicating the reasons for which the Member State considers that there is urgency.

The Commission under art.3.6 shall, without prejudice to the Member State's possibility of proceedings with the measures in question, examine the compatibility of the notified measures with Community law in the shortest possible time. Where the Commission comes to the conclusion that the measure is incompatible with Community law, the Commission shall ask the Member State in question to refrain from taking any proposed measures or urgently to put an end to the measures in question. This formulation of the Commission's powers is significantly weaker than the Commission's original proposal, which required Member States to cease or refrain from measures in the event of a Commission negative decision.

Under the Electronic Commerce Regulations, court proceedings, including preliminary proceedings and acts carried out in the course of a criminal investigation, are under reg.5(5) exempt from the requirement of reg.5(4) first to request the home Member State to take measures and to give advance notice to that Member State and the European Commission.

[101] *eDate Advertising GmbH/Martinez* (C-509/09 and C-161/10) 25 October 2011 CJEU at [59] and *European Commission v Ireland* CJEU I-140, 29 September 2011 at [44]. See *R. (on the application of Ordanduu GmbH) v Phonepayplus Ltd* [2015] EWHC 50 (Admin) at [49].

6–092 **Deterrence** The derogation provisions could potentially provide scope for Member States to seek to justify existing restrictions against a "given" service on one of the grounds set out in art.3.4,[102] or to put in place new restrictions under the urgency procedure and then to fight a political campaign seeking to justify the measures taken. However *R.(on the application of Ordanduu) v Phonepayplus Ltd*,[103] discussed below, illustrates that the derogations do not amount to a carte blanche for disproportionate or ill-considered action.

It is perhaps unclear whether a "given" service can extend to a designated type of service, or must mean a particular service emanating from a particular provider. However, applying measures beyond the specific service that has given rise to the concern may be disproportionate.[104]

(g) Use of the Directive's internal market derogation provisions

6–093 In November 2003, the European Commission published its First Report[105] on the operation of the Electronic Commerce Directive. It said that it had received only five formal notifications under the service-specific measures provisions of the Directive. All five emanated from the same Member State and all concerned the fraudulent use of premium rate numbers. We can probably infer that those notifications all emanated from the UK.

6–094 **Use against premium rate services** In October 2002, ICSTIS, the UK Independent Committee for the Supervision of Standards of Telephone Information Services, took action to suspend web-related premium rate telephone services provided to the UK by two companies established in Spain and Germany. It barred access to the services for two years, fined the companies £75,000 and £50,000, issued a formal reprimand and instructed them to offer redress to all complainants.

In this case, ICSTIS relied on the full urgency exception provided in reg.5(6). On the basis of ICSTIS' account of the facts, the activities of the companies in question presented a serious danger to UK consumers. According to ICSTIS, the companies' websites downloaded dialler software to users' computers without their knowledge. The dialler program would then dial up a premium rate number charged at £1.50 per minute. The promotional material for one website is said to have contained references to paedophilia and sexual acts involving children.

It is open to question, on these facts, whether ICSTIS' action was constrained by the Directive at all. To constitute an information society service within the Directive, a service must be provided "at the individual request of a recipient of the service". The nub of the complaint here was that the dial-up occurred without the user's knowledge, which by definition can hardly have occurred at the user's individual request. However, ICSTIS proceeded on the basis that they had to justify their actions within the terms of the Directive.

[102] The effect of the Directive on existing legislation is not spelt out. It is not clear whether Member States can seek to justify existing legislation under the art.3.4 derogations, or whether any attempt to enforce existing legislation is a "measure" subject to the notification procedures of art.3.4.

[103] *R. (on the application of Ordanduu GmbH) v Phonepayplus Ltd* [2015] EWHC 50 (Admin).

[104] *R. (on the application of Ordanduu GmbH) v Phonepayplus Ltd* [2015] EWHC 50 (Admin).

[105] 21 November 2003, COM(2003) 702 final.

- information about selection of preferential numbers or discount calls.

It goes on to discuss passwords[88]:

> "Some telecommunications operators may choose to retain user passwords as clear text for business purposes. In this context passwords would constitute entity data. Any information, such as a password, giving access to the content of any stored communications or access to the use of a communications service may only be sought under Part 3 of the Act from a telecommunications operator in the following circumstances: where such information is necessary in the interests of national security; or for preventing death, injury or damage to health."

This limitation on the purpose for which access can be obtained to stored passwords[89] is stricter than in the 2016 Act itself and appears only in the Code of Practice. The equivalent RIPA Code of Practice contained a similar provision, but limited to national security only.

8–067 **Examples—events data** As for events data, the Code of Practice explains:

> "Events data covers information about time-bound events taking place across a telecommunication system at a time interval. Communications data is limited to communication events describing the transmission of information between two or more entities over a telecommunications service. This will include information which identifies, or appears to identify, any person, apparatus or location to or from which a communication is transmitted. It does not include non-communication events[90] such as a change in address or telephone number for a customer."

The Code gives examples of events data:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and email headers—to the extent that content of a communication, such as the subject line of an email, is not disclosed);

[88] It also observes that communications data authorisation cannot authorise a public authority to use a password obtained through that or another communications data authorisation. Since that would amount to interception it would require appropriate lawful authority.

[89] As to whether a password can be entity data, although a password would appear to be capable of being data about an association between a telecommunications service and an entity (the user or the user's device) for the purpose of s.261(3)(a)(ii), it is less clear how a password can be said to identify or describe the entity for the purpose of s.261(3)(b).

[90] In this respect, events data appears to be narrower than "identifying data" that identifies an event for the purpose of inclusion in secondary data, since s.263(2)(b) is not limited to communications events.

- itemised telephone call records (numbers called);
- itemised internet connection records;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded; and
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

Bulk Code categorisation The Bulk Communications Data Acquisition Code of Practice takes a different approach to explaining communications data, even though it is founded on the same definition as the ordinary Communications Data Acquisition Code. Rather than split its explanation into entity and events data the Bulk Code focuses on the subdivisions of the composite "entity or events data" set out in s.261(5)(a) of the 2016 Act. 8–068

The Bulk Code explains that: "In the context of telecommunications, communications data includes data held or obtainable by a telecommunications operator[91] or which is available directly from a telecommunication system[92] and comprises four elements": service provision, traffic, service use and system architecture.

Service provision This is data about an entity to which a telecommunications service is provided and which relates to the provision of the service.[93] The Bulk Code states: 8–069

> "2.15 This data includes information about any person to whom a service is provided, whether a subscriber or guest user, and whether or not they have ever used that service. For example, this may include information about the person associated with an email address even if that email address has not been used since its creation.
>
> 2.16 An entity can also include devices, so this data would cover information about the devices owned by a customer as well as the services to which the owner of the devices subscribes. This data may include names and addresses of subscribers.
>
> 2.17 Importantly, this data is limited to data held or obtained by the telecommunications operator in relation to the provision of a telecommunications service—it does not include data which may be held about a customer by a telecommunications operator more generally which are not related to the provision of a telecommunications service.
>
> 2.18 For example, for a social media provider, data such as the status of the account, contact details for the customer and the date a person registered with the service would all be communications data as they relate to the use of the service. However, other data held by the provider about a customer which does not relate to the provision of the telecommunications service, including personal information such as political or religious interests included in profile information, is not within scope of the definition of communications data."

[91] 2016 Act s.261(5)(a). Under the Act this applies only to data within s.261(5)(a)(i) to (iii).

[92] 2016 Act s.261(5)(a). Under the Act this applies only to data within s.261(5)(a)(ii).

[93] 2016 Act s.261(5)(a)(i).

8–076 **Person with a right to control** The Court of Appeal in *R. v Stanford*[97] considered the meaning of the person with the "right to control the operation or the use of the system" for the purposes of RIPA s.1(6). It held that it is a person who can authorise or forbid the use of the system by others. The mere right to use or operate the system, such as a system administrator equipped with broad privileges and the necessary passwords would have, was not sufficient to fall within s.1(6).

There was no challenge to the ruling of the first instance judge that if the express or implied consent of a person with the right to control the system is to be relied upon, it must be consent to the specific interception, not a mere general authorisation to operate and run the system. The Court of Appeal rejected the argument that the civil remedies provided by the Act would suffice to protect privacy rights in the case of unauthorised interceptions by persons who had been granted administrator access: "The scheme of the legislation is that criminal sanctions should provide the primary protection against the interception of private communications". The decision should apply equally to the 2016 Act.

8–077 **Employers** Since an employer will be a person with the right to control the operation or use of its own network, the exclusion from criminal liability (but not from civil liability) provisions has the potential to cover the ability of employers to read emails and other communications in their own systems. The Business Monitoring and Record-Keeping Regulations discussed in Ch.5 provide lawful authority for some activities of that kind.

8–078 **Private telecommunication system** "Private telecommunication system" is defined in s.261(14) as any telecommunication system which:

> "(a) is not a public telecommunication system,
> (b) is attached, directly or indirectly, to a public telecommunication system (whether or not for the purposes of the communication in question), and
> (c) includes apparatus which is both located in the United Kingdom and used (with or without other apparatus) for making the attachment to that public telecommunication system."

This is substantially the same as the definition in RIPA s.2(1).

8–079 "Public telecommunication system" means (s.261(9)): a telecommunication system located in the UK:

(a) by means of which any public telecommunications service is provided; or
(b) which consists of parts of any other telecommunication system by means of which any such service is provided.

Again, this is substantially the same as the definition in RIPA s.2(1).

8–080 "Public telecommunications service" means (s.261(8)):

> "any telecommunications service which is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom."

[97] *R. v Stanford* [2006] EWCA Crim 258.

This has not changed significantly compared with RIPA s.2(1).

8–081 "Telecommunications service" is defined as (s.261(11)):

> "any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service)."

8–082 **Cloud services** Section 261(11) is supplemented by s.261(12):

> "For the purposes of subsection (11), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system."

Section 261(11) is identical to the original RIPA definition. Section 261(12) repeats an amendment to RIPA made by the Data Retention and Investigatory Powers Act 2014 s.5.

8–083 "Telecommunication system" means (s.261(11)):

> "a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy."

This has not changed significantly compared with RIPA s.2(1).

8–084 **Private versus isolated telecommunication system** Since "private telecommunication system" includes only systems attached directly or indirectly to a public telecommunication system, any private network not so attached is excluded from the scope of the Act, since it is neither a private nor a public telecommunication system as defined. However, this is unlikely to exclude more than a very small minority of physically isolated networks.

"Private telecommunication system" is likely to catch any private network on which, for instance, it is possible to send or receive external email or access the internet. This will include almost all office networks.

The Explanatory Notes to RIPA (para.27) stated that:

> "an office network, linked to a public telecommunication system by a private exchange, is to be treated as a private system …An entirely self-standing system, on the other hand, such as a secure office intranet, does not fall within the definition."

The reference to a secure office intranet is puzzling. Most intranets, while located behind secure firewalls to prevent unauthorised access from the outside world, are nevertheless connected to the outside world and permit traffic to flow between the intranet and the public network beyond the firewall. According to the definition in the legislation, it would seem that a secure intranet would only fall outside the definition of "private telecommunication system" if it were completely physically isolated from the public network.

8–188 **No interception** An authorisation may not authorise interception of communications in the course of their transmission by means of a telecommunication system.[238]

8–189 **Telecommunications operator duty to assist** A telecommunications operator is under a duty, subject to reasonable practicability and the effect of a technical capability notice,[239] to comply with a communications data acquisition notice.

8.6.5 Internet connection records

8–190 Special restrictions on acquisition apply to internet connection records (ICRs). ICRs may loosely be thought of as information about the destination of an internet communication, such as the website being visited. They approximate to "weblogs" discussed in s.8.2.

(a) ICRs defined

8–191 The formal definition of an ICR is:

> "communications data which:
> (a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and
> (b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person)."

(b) Restrictions on ICR access and processing

8–192 Restrictions apply to who (e.g. local authorities are excluded) can request access, and for what purposes, to data which is, or can only obtained by processing, an ICR.

The purposes for which access can be obtained are, paraphrased and simplified (some apply only to some situations), to identify:

- Who or what is using an internet service where only the service and time of use are already known.[240]
- Which internet communications service is being used, when and how, by a known person or apparatus.[241]
- Which internet service is being used, when and how, by a known person or apparatus.[242]

[238] 2016 Act s.60A(6). Since s.4 defines interception for the purposes of the Act, s.60A(6) includes the extended meaning of in the course of transmission, under s.4(5).
[239] 2016 Act s.66.
[240] 2016 Act s.62(3).
[241] 2016 Act s.62(4)(b)(i) and 62(5)(c)(i).
[242] 2016 Act s.62(4)(b)(iii) and 62(5)(c)(iii).

- Where or when a known person or apparatus is obtaining access to, or running, a computer file or program which wholly or mainly involves making available, or acquiring, material whose possession is a crime.[243]

Internet service and internet communications service Neither "internet service" nor "internet communications service" is defined in the 2016 Act. These are not industry or technical terms of art. The footnotes to the Communications Data Code of Practice contain some clues, but little illumination. 8–193

Footnote 50 says that an "internet service" is a service provided over the internet. On the face of it, this would seem to exclude a service consisting of providing access *to* the internet. However the telecommunications operator example illustrating s.62(3) in para.9.6 of the Code suggests otherwise.

Footnote 50 goes on to say that "internet service" includes "internet communication services, websites and applications". Paragraph 9.3 of the Code also suggests examples of online travel booking or mapping services. This explanation presents some problems.

First is the suggestion that internet communication services are a subset of internet services. If that is right, then the second purpose above is redundant since the third already covers internet services in identical terms. Paragraphs 9.3 and 9.7 of the Code suggest that the third purpose relates to "other" internet services. However, that language does not appear in the Act. 8–194

Secondly, is the suggestion in fn.50 that websites and applications are different from internet communications services. On the face of it an internet communication service could mean just email or a messaging service. But if so, what should we make of "applications" as something different, since many messaging services are app-based?

Thirdly, fn.49 of the Code of Practice says that an internet communication service is a service which provides for the communication between one or more persons over the internet and "may include" email services, instant messaging services, internet telephony services, social networking and web forums.

This would go wider than just email and messaging services, but how much wider is unclear. Would it, for instance, include online games with the ability to chat to other players? In this context, does "person" refer only to a human being, or does it include machine communications?

Material whose possession is a crime As to "material whose possession is a crime" (fourth purpose, listed in para.8–192), there are relatively few offences that are committed by mere possession of material. Illicit drugs and child abuse imagery are two mentioned in the Code of Practice. Questions that may arise include whether the section applies more widely than mere possession, for instance where possession is an offence only if it is with a view to some other activity. Would it apply to possession offences where, for instance, possession is not an offence if it is for personal use? 8–195

Examples The question of what kinds of real world data may fall within the definition of communications data is discussed above under "Content v metadata" (section 8.3.5). 8–196

[243] 2016 Act s.62(4)(b)(ii) and 62(5)(c)(ii).

9.1 INTRODUCTION

9–001 This chapter discusses how current UK and EU communications and broadcasting regulation applies to the internet and to services provided by means of the internet.

When considering regulation in this context, it is important to ask who is doing what. A communications network provider that owns and operates the communications infrastructure that makes up the internet is performing a different function from an internet service provider (ISP) that provides internet access and web hosting services to its customers over the communications network provider's infrastructure, or an Application Service Provider (ASP) that provides online applications and services over the internet to its customers. We are now seeing (at least in Europe) a trend towards the increased application of the communications regulatory framework to services provided over the internet. This has resulted in some curious paradoxes, some of which are discussed in this chapter.

9.1.1 History

9–002 **The EU framework** The Communications Act 2003 (the Communications Act) introduced significant changes to the regulation of communications and broadcasting in the UK. The most notable changes were the implementation into UK law of the 2002 Regulatory Framework for electronic communications in the EU (the EU Regulatory Framework) and the introduction of a converged[1] regulator, the Office of Communications (Ofcom).

The EU Regulatory Framework was reviewed and amended in 2009 by two further EU Directives, the Better Regulation Directive[2] and the Citizens' Rights Directive.[3] An EU-wide regulator, the Body of European Regulators for Electronic Communications (BEREC), was also created at that time under a separate EU Regulation.[4]

More recently, the EU has comprehensively revised the EU Regulatory Framework. In September 2016, the European Commission published a proposal for a new EU Directive that would repeal and replace the Directives of the EU Regulatory Framework. In June 2018, the EU co-legislators (the European Parliament and Council) agreed on a new EU Directive named the European Electronic Communications Code (EECC).[5] The EECC was published on 11

[1] Ofcom replaced the previous Office of Telecommunications, Independent Television Commission, Radiocommunications Agency, Broadcasting Standards Commission and Radio Authority.

[2] Directive 2009/140 amending Directives 2002/21 on a common regulatory framework for electronic communications networks and services, 2002/19 on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20 on the authorisation of electronic communications networks and services [2009] OJ L337/37.

[3] Directive 2009/136 amending Directive 2002/22 on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11.

[4] Regulation 1211/2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office [2009] OJ L337/1.

[5] Directive 2018/1972 the European Electronic Communications Code [2018] OJ L321/36.

December 2018. Transposition of the EECC into the national laws of the Member States is required by 21 December 2020.[6]

9.1.2 Regulatory challenges and the internet

The rapid speed at which the internet has evolved as a means of facilitating service provision has given rise to certain mismatches with established regulations and procedures. This challenge is compounded by increasingly complex (and indeed creative) service value chains. This has meant that the applicability of national telecoms regulatory rules to an internet based communications service may not always be obvious. This situation can, in turn, lead to regulatory uncertainty. 9–003

Convergence As we explain in this chapter, the internet has also facilitated technical and service convergence. The convergence of the broadcasting, communications and IT industries has allowed text, data, video, audio, and images to be reduced to binary code before transmission to the end-user, often rendering it impossible to know what type of content is being transmitted. This is particularly the case with the internet where, generally, data is reduced to uniform packets transmitted using the TCP/IP protocol. Whether the type of content regulation that has been applied in respect of broadcast media has any place in relation to interactive content, has been, and remains, a hotly debated topic. Much content on the internet has its roots in print media or individual speech (which are relatively unregulated) rather than in television (which is heavily regulated). These issues are discussed further below (section 9.6). 9–004

This trend towards convergence can place pressure on a traditional sector-specific approach towards regulation. This is not a new phenomenon, however, and technical and service convergence has revised approaches such an approach towards sector regulation in the past. For example, increasing convergence led to the replacement of the existing separate communications and broadcast regulatory structures with a single regulatory framework in the UK by the Communications Act, which, as noted above, also introduced a single regulator, Ofcom.

9.1.3 Regulatory background

(a) Communications regulation

Deregulation and privatisation The communications sector is, currently, heavily regulated. This is true at both the network and service level. In common with water, gas, electricity and rail, communications services were, for many years, provided by a government-owned utility company with monopoly rights. The UK state owned incumbent, British Telecommunications Plc (BT), was privatised by the 1984 Telecommunications Act to facilitate transition to a competitive market. The monopoly had previously been broken with the grant of a licence to Mercury Communications in 1982. 9–005

[6] Directive 2018/1972 the European Electronic Communications Code [2018] OJ L321/36 art.124.

guidance on the definition of "ECS" since it is relevant to determining who is subject to the administrative fee payment requirement and how this should be calculated.

The Guidance recognises that a broad range of services fall within the definition of ECS and that in some cases, it may not be easy to decide whether an ECS is being provided. It goes on to sub-classify ECS, depending on the level of additional network resources and associated facilities that they require as well as whether there is any interaction, manipulation or storage of content, as being either:

- basic services—these are services provided over an ECN without the support of databases or servers; Ofcom lists telephone calls and video conferencing as examples of these services;
- advanced services—these are services provided over an ECN but which require the support of an associated facility; Ofcom lists "instant messaging" supported by a "presence database" as examples of these services; or
- enhanced services (value-added services)—these are services provided over an ECN but which either interact with content, manipulate content or store content with the support of an associated facility; Ofcom lists "email supported by email servers" as an example of this type of service.

9–053 These sub-classifications are not used in the EU Regulatory Framework, the Communications Act or General Conditions. They are merely classifications that Ofcom has used to try to explain the scope of a difficult, potentially broad definition. However, Ofcom does comment that the classification of these services as ECS is consistent with the definition of ECS under EU law under the EU Framework Directive.[56]

9–054 **Instant messaging** Ofcom's decision to classify all instant messaging services supported by a presence database as advanced services does not appear to align with the position stated by BEREC on this issue. As discussed in para.9–044 above, the BEREC Report includes OTT instant messaging services in the OTT-1 category, which it does not regard as ECS. Moreover, and although not explicitly stated in the BEREC Report, there seems to be no reason to believe that BEREC would treat instant messaging services with PSTN break-out any differently to similar type OTT voice services (which it classifies as ECS in the OTT-0 category for the purpose of its report).

9–055 **Developments since 2005** The Ofcom Relevant Activity Guidance is (at the time of writing) 14 years old. Much has happened in the meantime in respect of the deployment and regulation of new technology services including instant messaging services. It is therefore possible that, in light of the BEREC Report and the relevant jurisprudence discussed above (para.9–042), Ofcom's approach may have changed since 2005 in respect of how these types of services are regulated. Indeed, the 2007 VoIP Consultation would seem to suggest a change in

[56] Directive 2002/21 on a common regulatory framework for electronic communications networks and services [2002] OJ L108/33.

approach by Ofcom. As noted in para.9–045 above, Ofcom classified (in the 2007 VoIP Consultation) peer-to-peer services to make and receive voice calls on the internet only, usually within the same application community, as a Type 1 VoIP that is not subject to regulation.

Webmail The same observation applies with respect to the position stated in the Ofcom Relevant Activity Guidance on webmail services. 9–056

More recently, the status of webmail services for the purposes of telecoms regulation under EU law has been determined by the CJEU in a reference case from a regional court in Germany.

In July 2012, the Bundesnetzagentur (BNetzA) (Federal Network Agency—Germany), which is responsible for regulating the national telecommunications market, formally determined that Gmail was a regulated ECS under German law. Following this, Gmail requested that the Verwaltungsgericht Köln (Administrative Court, Cologne) annul the Federal Network Agency's determination. By judgment of 11 November 2015, the Administrative Court dismissed Gmail's action. Gmail then appealed this decision to the Higher Administrative Court for the State of North Rhine-Westphalia arguing that the Gmail service does not constitute an ECS under German law because Google's operation of the service does not involve the conveyance of any signals. The Higher Administrative Court referred a question to the CJEU on the scope of the definition of "a telecommunications service". In a judgment handed down in 2019, the CJEU accepted Google's argument and held that the service was not an ECS stating that

> "a web-based email service which does not itself provide internet access, such as the Gmail service provided by Google LLC, does not consist wholly or mainly in the conveyance of signals on electronic communications networks and therefore does not constitute an 'electronic communications service' … ".[57]

EECC As noted in para.9–049 above, EECC Recital (17) explicitly states that ICS cover services like traditional voice calls between two individuals as well as "all types of emails, messaging services or group chats". This indicates a preference on the part of the EU legislator for a broader approach that would include all types of instant messaging and webmail services within the definition of ECS. 9–057

9.3.5 Internet of Things (IoT)

IoT refers to an ecosystem of devices communicating with one another primarily across the internet using fixed and wireless access networks without human involvement. The growth of machine-to-machine communications and the trend towards IoT has the potential to significantly affect many aspects of our lives. In the view of BEREC: 9–058

[57] *Google LLC v Bundesrepublik Deutschland* (C-193/18) 13 June 2019.

between situations where the parties are commercial entities negotiating at arm's length over a non-standard form of contract and those which involve contracts (almost always in standard form) with consumers.

10.3.1 Applicable law and jurisdiction

10–110 The contract should specify a governing law. If it does not do so there will be even more room than usual to argue over which country's law governs the terms of the contract and its operation. Where no governing law is referred to in a contract, contracts made on or after 17 December 2009[79] are subject to the Rome I Regulation,[80] which provides rules[81] for specific categories of contract to be applied in the absence of a specified governing law.

In cases not covered by the specific rules (or where more than one rule applies), Rome I applies the law of the place where the party performing the service that characterises the contract has their habitual residence (art.4(2)).

10–111 **Brexit** In the event of a "no-deal" Brexit the Rome I Regulation would be retained law under the EU Withdrawal Act 2018, so would operate effectively as domestic law post-exit. By statutory instrument, the previous Rome Convention rules would continue to apply to contracts entered into between 1 April 1991 and 16 December 2009.[82]

10–112 **B2C contracts** In relation to B2C contracts, Rome I art.6(1) states that, in the absence of an express choice of law, a contract will be governed by the:

> "law of country where the consumer has his habitual residence, provided that the professional:
> (a) pursues his commercial or professional activities in the country where the consumer has his habitual residence; or
> (b) by any means, directs such activities to that country or to several countries including that country, and the contract falls within the scope of such activities."

Where the B2C contract specifies the choice of law to govern the contract, that choice of law shall be valid save that, under Rome I art.6(2):

[79] Contracts made before that date remain governed by the provisions of the Contracts (Applicable Law) Act 1990.

[80] Regulation 593/2008 on the law applicable to contractual obligations [2008] OJ L177/6.

[81] Rome I art.4 contains the relevant information regarding applicable law in the absence of choice. The special rules relate to specific types of contracts. These are: sale of goods; auction sales; services; franchise agreements; distribution agreements; rights in land and tenancies; holiday lets; and financial markets contracts.

[82] Ministry of Justice, "Cross-border civil and commercial legal cases after Brexit: Guidance for legal professionals" at *https://www.gov.uk/government/publications/cross-border-civil-and-commercial-legal-cases-after-brexit-guidance-for-legal-professionals/cross-border-civil-and-commercial-legal-cases-after-brexit-guidance-for-legal-professionals* [Accessed 14 October 2019].

> "such a choice may not … have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law which, in the absence of choice, would have been applicable on the basis of [art.6(1)]."[83]

Unfair choice of law term A term purporting to impose a different law may be not only unenforceable under Rome I but also contrary to the Consumer Rights Act 2015 (see section 10.2.3 above). In *Verein fur Konsumenteninformation v Amazon EU Sarl*,[84] the CJEU held that a standard term of a B2C contract that designated the law of a particular EU Member State as governing the contract was an unfair term (under the EU Directive on Unfair Terms in Consumer Contracts, now implemented in the UK by the Consumer Rights Act 2015) to the extent that it gives the consumer the impression that only the law of that member state applies to the exclusion of mandatory local law under Rome I. Governing law clauses in B2C contracts should therefore explain to consumers when they are entitled to rely on the mandatory provision of their local law. 10–113

Local choice of law rules If courts in other countries are seized with a dispute under the contract they may apply different rules for deciding what is the governing law, such as the law of the place of contracting or the law of the place of performance.[85] The risk, therefore, to a seller offering its goods for sale online—even where these are offered in the seller's standard "click-wrap" terms, is that the laws of a country other than that specified in the contract may be applied to the contract by operation of law, notwithstanding that the seller has no connection with that legal system and is unaware of the consumer protection laws in that country. 10–114

Stipulating law and jurisdiction When it comes to choosing a governing law the obvious choice will be the law with which the persons preparing the contract are most familiar. However, at the time of specifying a governing law of any contract it is normal to also specify in the courts of which country it is at least preferred that any dispute is dealt with, and it is clearly going to be easier for those courts and the conduct of any dispute if the governing law of the contract is that of the court dealing with the matter. 10–115

Enforceability In choosing the preferred courts (the jurisdiction) some consideration needs to be given to enforceability of the judgment of any such court against the parties. If a person has a place of business in the same country as the court giving the judgment there is no problem. But if this is not the case then one has to look to the availability of reciprocal enforcement treaties between the country in which the court is situated and the country in which the person against whom the judgment is given is based. 10–116

[83] There are exceptions to the application of Rome I art.6, set out in art.6(3), such as contracts of carriage other than a contract relating to package travel.

[84] *Verein fur Konsumenteninformation v Amazon EU Sarl* (C-191/15) 28 July 2016.

[85] But a Rome I Regulation country will, subject to the UK position after Brexit, operate the same rule.

preclude signature by most (but not necessarily all[129]) forms of electronic signature. If, on the other hand, a writing requirement were broadly defined so as to encompass a document in electronic form, that would suggest that an accompanying signature requirement could be satisfied by signing the document electronically.[130]

Most obstacles to the use of electronic signatures in fact flow from surrounding formalities rather than from any signature requirement per se. Surrounding formalities can be divided into three categories: medium, form and process.

Writing is the most common medium formality. The Interpretation Act 1978 contains a definition of writing which covers most varieties of electronic data, but due to its requirement of visibility could exclude wholly automated electronic transactions.[131] Some EU Directives have laid down requirements for a "durable medium".[132]

An example of the second category, form, would be a requirement that a signature be placed in a particular position in a document.[133] Examples of process formalities include presence of witnesses and delivery of a deed.

10–176 **Law Commission** Uncertainty as to whether all these requirements can be satisfied electronically or remotely prompted a joint working party of the Law Society Company Law Committee and the City of London Law Society Company Law and Financial Law Committees to publish in 2016 a Note on the Execution of a Document Using an Electronic Signature.[134]

Subsequently in 2018, the Law Commission initiated a project on Electronic Execution of Documents.[135] As to electronic signatures, the resulting Consultation Paper, published in August 2018, confirmed the Law Commission's previous view in its 2001 Advice on Electronic Commerce: Formal Requirements in Commercial Transactions that an electronic signature is capable of satisfying a statutory requirement for a signature:

> "Our provisional view is that the combination of eIDAS, domestic legislation and case law means that an electronic signature is capable of meeting a statutory requirement for a signature if an authenticating intention can be demonstrated. This view is not limited to a particular type of electronic signature: the law is flexible."[136]

[129] The US E-SIGN legislation specifically contemplates the possibility of a non-electronic document being signed electronically.

[130] See, however, *Cowthorpe Road 1-1A Freehold Ltd v Wahedelly* [2017] L. & T.R. 4, in which HH Judge Dight held that the signature requirement in that case indicated that what had to be signed was an original not a copy. That evinced a contrary intention so as to exclude the definition of "writing" in the Interpretation Act 1978, which in turn precluded service by email. The Court of Appeal considered the decision in *Knight v Goulandris* [2018] EWCA Civ 237, but expressed no view on its correctness.

[131] See Law Commission Advice on "Electronic Commerce: Formal Requirements in Commercial Transactions" (December 2001) at 3.14 to 3.23. The Electronic Transactions (Guernsey) Law 2000 contains definitions of "writing" and "physical writing" that address this problem.

[132] See below, para.10–263.

[133] See *Bassano v Toft* [2014] EWHC 377 (QB) at [45].

[134] 13 July 2016 at *http://www.citysolicitors.org.uk/attachments/article/121/LSEW%20%20CLLS%20Joint%20Working%20Party%20-%20Note%20on%20the%20Execution%20of%20a%20Document%20Using%20an%20Electronic%20Signature.pdf.*

[135] See *http://www.lawcom.gov.uk/project/electronic-execution-of-documents/* [Accessed 14 October 2019].

The Law Commission considered whether there should be legislative reform to include a statement in statute that an electronic signature is as valid as a handwritten signature. It was not persuaded that this was necessary in England and Wales because of its provisional conclusion that the current law already accommodates electronic signatures. However, it thought this was a finely balanced question.

As to surrounding formalities, the Consultation Paper went on to make provisional suggestions that would enable witnessing and attestation to take place electronically and remotely (e.g. by video link) or to introduce a new concept of electronic acknowledgment. The Law Commission published a "Final Report" in September 2019, including a summary statement of the existing law on electronic signatures confirming its provisional conclusion.

Liberal view English law has traditionally taken a liberal view of what satisfies a legislative requirement for a signature. Indeed, there is no English case in which a signature has been held not to satisfy a legislative requirement for a signature merely because it is not in the correct form.[137] 10–177

Signatures have been disqualified for different reasons: because they were applied by an agent when the particular statute on its true construction requires a personal signature (i.e. one applied by the signatory)[138]; or because the name that was alleged to be a signature simply was not a signature[139]; or because the

[136] Summary at para.1.19, citing paras 3.83 to 3.87 of the consultation paper.

[137] HH Judge Purle QC in *Lim v Thompson* [2009] EWHC 3341 (Ch) rejected a photocopy, to which witnesses had added their signatures, of a previous version of a will, on the basis that "In my judgment, a photocopy a previous version of the will with a photocopied signature of the testator is not a document which is signed by the testator at all". He went on, citing the prevention of fraud policy underlying the Wills Act: "... it is very important that what must survive is an original signature, whether of the deceased or someone else signing at his direction in his presence". The formalities and signature requirements of wills are currently under review by the Law Commission of England and Wales.

[138] e.g. *Re Prince Blucher Ex p. Debtor* [1931] 2 Ch. D. 70. See also *Ni v Slocum* (Cal. Ct. Appeal 30 June 2011; (2011) 16(27) E.C.L.R. 1140), in which a signature traced on a ballot paper petition using an iPhone was assumed to be a valid electronic signature, but nevertheless was held not to satisfy the California Election Code requirement that the signature be "personally affixed". *Prince Blucher* itself was held in *General Legal Council ex parte Whitter v Frankson (Jamaica)* [2006] UKPC 42 to have been wrongly decided.

[139] e.g. *Firstpost Homes v Johnson* [1995] 4 All E.R. 355. The Court of Appeal, interpreting the Law of Property (Miscellaneous Provisions) Act 1989 s.2, rejected the previous "generous" interpretations of the Statute of Frauds and the Law of Property Act 1925 s.40 as inapplicable to the 1989 Act. They held that the printing or typing of the name of an addressee of a letter, when the addressee had printed or typed the document, was not the signature of the addressee. However, this was not on the grounds that the "signature" was printed or typed, but on the grounds that inserting the name of an addressee of a letter did not amount to signing the document. Peter Gibson LJ stated: "This decision is of course limited to a case where the party whose signature is said to appear on the contract is only named as the addressee of a letter prepared by him. No doubt other considerations will apply in other circumstances." The decision focused not on the form of the signature, but on the fact that the name was typed as the addressee of the letter, leaving open the possibility that in other circumstances a typed signature would suffice. Although not expressly stated, on the logic of the reasoning the same result would have been reached if the addressee had written out the letter by hand.

of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service (art.43.2).

These correspond to the provision for qualified electronic signatures that they shall have the equivalent legal effect of a handwritten signature (art.25.2).

10–210 The 2000 Act defines "electronic communication" (as amended by the Communications Act 2003) as meaning a communication transmitted (whether from one person to another, from one device to another or from a person to a device or vice versa):

(a) by means of an electronic communications network; or
(b) by other means but while in an electronic form.

"Communication" includes a communication comprising sounds or images or both and a communication effecting a payment.

10–211 **Authenticity** References in the 2000 Act to the authenticity of any communication or data are stated to be references to any one or more of the following:

(i) whether the communication or data comes from a particular person or other source;
(ii) whether it is accurately timed and dated;
(iii) whether it is intended to have legal effect;

and references to the integrity of any communication or data are stated to be references to whether there has been any tampering with or other modification of the communication or data.

There is no definition of "electronic".

The view of the Government was that these provisions met the obligation to implement art.5.2 of the Directive.[171] No changes were made to accommodate the eIDAS Regulation. However, s.7 is not a straight transposition of art.5.2 of the then Directive or of the various provisions of the eIDAS Regulation. It is considerably more detailed and on the face of it differs in certain respects from both, for instance:

- it contains a definition of authenticity which does not appear in the then Directive or the eIDAS Regulation;
- it requires that a signature or seal be "incorporated into", rather than "attached to" other data in electronic form;
- the definition of "electronic time stamp" contains a requirement that the data be "incorporated into or otherwise logically associated with any electronic communication or electronic data" which does not appear in the eIDAS Regulation;
- the definition of "electronic document" contains minor differences from that in the eIDAS Regulation;

[171] DTI Consultation on the Directive, March 2001 para.36.

- an "electronic registered delivery service" is defined (in part) as "a service which provides for the transmission of data …" rather than "a service that makes it possible to transmit data …" as in the eIDAS Regulation;
- it omits any reference to "legal effectiveness", restricting itself to admissibility. (However, that is permissible under the eIDAS Regulation Recital (49), which states that it is for national law to define the legal effect of electronic signatures, except for the requirement that a qualified electronic signature should have the equivalent legal effect of a handwritten signature);
- it places a restriction on the purposes for which the electronic signature or other items are stated to be admissible which does not appear in the then Directive or the eIDAS Regulation.

There are also other provisions (references to integrity in relation to electronic signatures, admissibility of certificates) which are not expressly included in the Directive or the eIDAS Regulation.

10–212 None of this matters if, as already suggested, ss.7 to 7D should be regarded as purely permissive and not intended to restrict the admissibility of signatures, other items and certificates under the general evidential rules regarding documentary evidence.

Certainly nothing in the Act purports to restrict the admissibility of other electronic signatures and certificates and the Act does not include any express amendments to other evidence legislation. Nothing in the eIDAS Regulation suggests that its provisions on admissibility as evidence are intended to be anything but facilitative, enabling admissibility of material in electronic form where it would be admissible if it were in non-electronic documentary form. That is to be inferred from the reference in each case to not being denied admissibility "solely on the grounds that it is in electronic form".

10–213 **Signature as real evidence** In both civil and criminal proceedings a signature (whether on paper or electronic) would, we suggest, be likely to constitute "real" evidence (see discussion of evidential issues below at section 10.7) and therefore admissible with appropriate founding testimony.

As to the other items, to the extent that they would be admissible in paper form eIDAS merely requires them to be admissible if they are in electronic form. If that is correct, then no further legislative provision was probably required to secure the admissibility of electronic signatures of any nature in English proceedings. It would be unfortunate if s.7 were to be regarded as having introduced, by implication, a restriction on such admissibility. As yet, no judgment has suggested that.

(c) Advanced electronic signatures and qualified signatures

10–214 The Directive, by art.5.1, permitted Member States to accord a special status to advanced electronic signatures based on a qualified certificate and created by a secure-signature-creation device. Member States were required to ensure that such signatures

- If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise: (a) advanced electronic signatures; (b) advanced electronic signatures based on a qualified certificate for electronic signatures; and (c) qualified electronic signatures in at least the formats or methods defined in the reference formats and methods specified by the Commission in its implementing acts issued under the Regulation. The implementing acts are published on the eIDAS Observatory website.[184]
- If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise: (a) advanced electronic signatures based on a qualified certificate; and (b) qualified electronic signatures, as specified in those reference formats and methods.
- A Member State shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than a qualified electronic signature.

(i) Exclusions

10–242 Under art.2.2, the Regulation does not apply to the provision of trust services used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.

Under art.2.3, the Regulation does not affect national or EU law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.

10.6 FORMALITIES AND ELECTRONIC TRANSACTIONS

10.6.1 Background

10–243 Many countries have legislated specifically for electronic commerce and electronic transactions. Early adopters included the UK, US, Australia, Bermuda, Guernsey, Hong Kong, Ireland, Jersey, the Isle of Man, and Singapore. More have joined the fray since. Some of this legislation is based, to a greater or lesser degree, on the 1996 UNCITRAL Model Law on Electronic Commerce.[185] Some EU legislation addresses e-commerce in the broadest sense, for instance the parts of the Electronic Commerce Directive that address facilitation of electronic transactions generally.

England and Wales is a relatively liberal jurisdiction, formalities requirements for contracts or other types of transaction being the exception rather than the rule. There has, therefore, been little need to legislate either to remove formalities requirements that might impede electronic transactions or, conversely, to attempt

[184] See *https://ec.europa.eu/futurium/en/content/eidas-implementing-acts* [Accessed 14 October 2019].

[185] The Model Law was amended in 1998 to add art.5*bis* concerning information referred to, but not incorporated in, a data message (*http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html* [Accessed 14 October 2019]).

to replicate physical world formalities in the electronic environment. The result is that dealings are conducted electronically by the millions every day.

Nevertheless a few obstacles remain for some kinds of transaction. General doubts still occasionally surface about the ability to transact electronically. Although such concerns are often expressed in terms of the ability to use electronic signatures (as to which, see section 10.5), the obstacles that do exist tend in the main to result from other formalities, a requirement for witnessing being a good example. The Law Commission has conducted a project on Electronic Execution of Documents. It published a Consultation Paper in August 2018 and issued a final Report in September 2019.

Categories of formality Formalities can be categorised into four kinds: signature, medium, form and process. A requirement for a signature may specify a signature generally, or a specific kind of signature (see para.10–174). Writing is example of a formality of medium, as is durability (see para.10–263). An example of a requirement of form would be that a signature be applied at a specific place in a document or that prescribed text be displayed in a box of a particular colour or size. Witnessing is a process requirement, as is filing at a registry. 10–244

Such requirements have the potential to interact with each other. Thus in *Bassano v Toft*,[186] the question of whether the signature was applied in the place in an electronic document required by regulations was affected by the prior question of what constituted the signature. Pressing an "I accept" button was held to constitute the signature. The button was in the designated space in the document, thus satisfying the statutory requirement:

> "In the Borro Loan Agreement, the signature is made by the electronic communication of the words 'I Accept' which are in the space designated for a signature … The name on page one is of relevance because it is evidence that 'I' is Mrs Bassano's mark, if any were needed in addition to the evidence that it was she who clicked the button; but it is the words 'I Accept' which constitute the signature, not the name on the previous page."

Validity versus evidence The effect of non-compliance with a formality may be to render the transaction invalid (i.e. void, voidable, unenforceable, or unenforceable without permission). Validity has to be distinguished from the issue of evidential admissibility and weight. A document may be admissible in evidence, yet the transaction still invalid through failure to comply with a required formality. A document may be formally admissible in evidence and comply with a required formality, yet carry insufficient evidential weight to prove some critical matter. 10–245

Evidential value has two aspects: most obviously how to prove the contents of the document and its parties, but also how to prove that any required formalities were complied with. That in turn may involve considering how any potentially relevant evidential presumptions might apply to an electronic document.

In this section we will discuss various approaches to legislating for electronic transactions. First, however, a brief summary of some of the formalities that exist in English law.

[186] *Bassano v Toft* [2014] EWHC 377 (QB).

November 2010 to November 2013 at least 4,259 people were charged and at least 2,070 cautioned under the Malicious Communications Act 1988 or under s.127, nearly two thirds of which were under s.127. At least 355 of these cases involved social media.

12–049 **Prosecution Guidelines** The Director of Public Prosecutions published interim social media prosecution guidelines[33] in December 2012 (which became final in June 2013[34] and were later revised in 2016[35]), spurred by public concern over some arrests and prosecutions and in recognition of the breadth of social media content that could be caught by the various offences.[36]

12–050 **Equivalent offences elsewhere** In March 2015, the Indian Supreme Court held that a provision of Indian law closely modelled on s.127 was constitutionally vague, arbitrarily excessively and disproportionately invaded the right of free speech, and also was overbroad in that it encompassed protected and innocent speech and was liable to be used in such a way as to have a chilling effect on free speech.[37]

12–051 **History of s.127** The application of s.127 to the internet and social media is an accident of history. Section 127 goes back to the 1935 Post Office (Amendment) Act and, in some respects, as far back as 1884. The first limb, including "grossly offensive", was framed to deter telephone users from being abusive to telephone operators and others[38]; the second to catch senders of distressing hoax telegrams. Instances of malicious or even fraudulent hoax telegrams were known from at least the early 20th century.

The first limb of s.127 can be traced back as far as the Post Office (Protection) Act 1884. The ancestry of the section, focusing on the origin of "grossly offensive", in shown in Diagram 1.

12–052 **Grossly offensive** "Grossly offensive" originated in 1884 as part of a prohibition on material on the outside of postal packets (including telegrams). At the outset, an MP, Charles Warton, voiced concern in Parliament about what might be caught[39]:

[32] See *https://bigbrotherwatch.org.uk/2015/02/careless-whisper-how-speech-is-policed-by-outdated-communications-legislation/* [Accessed 16 October 2019].

[33] See *https://web.archive.org/web/20130115163041/http://www.cps.gov.uk/news/press_releases/dpp_launches_public_consultation_on_prosecutions_involving_social_media_communications/* [Accessed 16 October 2019].

[34] See *http://data.parliament.uk/DepositedPapers/Files/DEP2013-1025/social_media_guidelines.pdf* [Accessed 16 October 2019].

[35] See *http://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media* [Accessed 16 October 2019].

[36] See *https://inforrm.org/2012/12/23/prosecuting-social-media-the-dpps-interim-guidelines-alex-bailin-qc-and-edward-craven/* [Accessed 16 October 2019].

[37] *Singhal v Union of India* 24 March 2015 cited in *DPP v McConnell* 5 January 2016 at [16]. See also *Monis v The Queen* [2013] H.C.A. 14, an Australian case concerning the constitutionality of a provision bearing some similarities to s.127.

[38] The Law Commission Scoping Study at 4.61 points out that although abuse of telephone operators was an initial concern, the intention was also to protect the broader public.

[39] See *https://api.parliament.uk/historic-hansard/commons/1884/aug/09/committee* [Accessed 16 October 2019].

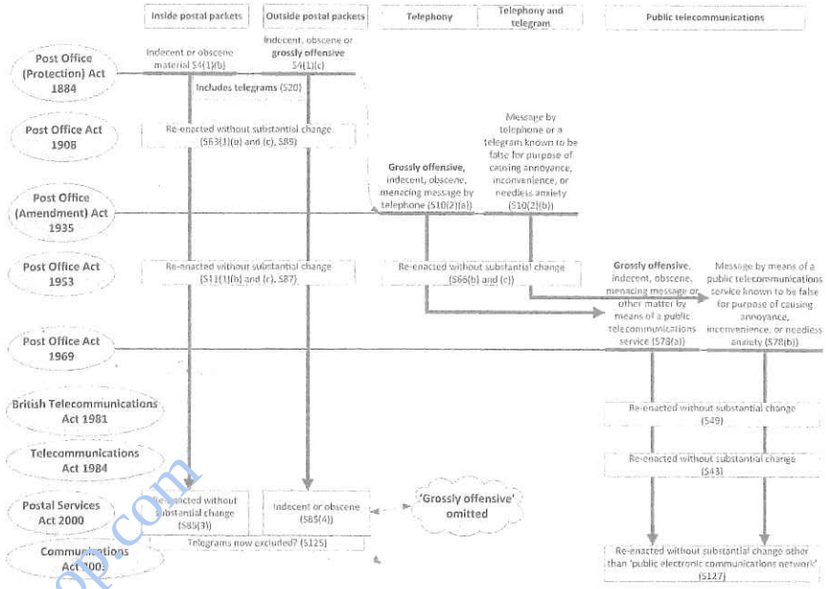

Diagram 1

> "… many people—even many Members of that House—frequently sent letters through the Post with very amusing pieces of scurrility upon them … under this clause, a very heavy liability might attach to it … it might happen that one man would use words—for instance, he might write 'swindler' or 'liar' upon the outside of a letter—which were not really indecent or obscene, only what they would call vulgar, and see what a tremendous penalty the clause imposed for that—imprisonment for 12 months."

In the event, the MP's fears were borne out in 1913 when one John Cole was convicted under the 1884 Act at Leeds magistrates after sending postcards to various local officials, calling a well-known local alderman an "insurance swindler". This was found to be grossly offensive.

The prohibition on "grossly offensive" material on the outside of postal packets remained unchanged until the Postal Services Act 2000. By that time, the legislative line of descent had forked. While "grossly offensive" was removed from the postal packets offence, it remained in the telephony provision. That was widened to cover messages sent by public telecommunications services in 1969, then amended to "public electronic communications network" in 2003.

It is not clear why in 2000 "grossly offensive" was removed from the prohibition applicable to the outside of postal packets, but not removed from what in 2003 became s.127.

Who is caught Section 127 catches the originator of the material rather than the person distributing it. Therefore it is unlikely that the internet service provider will be caught by this provision in the Act (and in any event would most likely 12–053