Questions for National Reporters of LIDC 2015, Stockholm

Question B: The Protection of Trade Secrets and Know-How

Are countries providing enough or too much protection?

United Kingdom

Michael Browne

Redd Solicitors LLP

22 Tudor Street

London

EC4Y 0AY

+44 (0) 207 776 4760

michael.browne@redd.eu

Contents

		Page Number
1.	**Legal Framework**	**3**
1.1	Applicable Legal Systems in the United Kingdom	3
2.	**The protection of rights in confidential information under the English Common Law**	**3**
2.1	Genus of the cause of action	**3**
2.2	The Modern Approach	4
	2.2.1 The First Requirement: The information must have the necessary quality of confidence	4
	2.2.2 The Second Requirement: The information must have been "imparted in circumstances importing an obligation of confidence"	6
	2.2.3 The Third Requirement: There must be unauthorised "use of the information to the detriment of the party communicating it"	7
2.3	"Trade secrets" as a sub-set of confidential information	7
2.4	Personal and private information	8
2.5	Duration	9
3.	**Remedies for breach of confidential information**	**9**
3.1	Overview	9
3.2	Injunctive relief	10
3.3	Financial compensation – damages and account of profit	11
3.4	Delivery up or destruction	12
3.5	Declarations	12
3.6	Publication and dissemination of judgment	12
4.	**The protection of confidential information by contract**	**13**
5.	**The treatment of confidential information in litigation**	**13**
6.	**Attempts to reform the law relating to the protection of rights in confidential information**	**14**
7.	**Personal reflections**	**15**

1. Legal Framework

1.1. Applicable Legal Systems in the United Kingdom

The United Kingdom incorporates three separate and distinct legal jurisdictions, comprising English law (applicable in England and Wales), Scottish law and Northern Irish law, each of which are common law jurisdictions. This report focusses on the protections afforded to know-how and trade secrets under the English common law, as acknowledged and developed by the case law of the courts of England and Wales. In general terms the position under Scottish law is largely the same as that in England and Wales, albeit with variations in terms of practice and procedure that are outside the scope of this paper.[1]

2. The protection of rights in confidential information under the English common law

2.1. Genus of the cause of action

There is no statutory protection of a "trade secret" as such in this jurisdiction. Trade secrets are treated as a sub-set of the broader category of rights in confidential information.

Rights in confidential information are protected under the equitable jurisdiction of the courts in accordance with the English common law, as well as the law of contract in appropriate cases. This section of the report focusses on the protection of confidential information under the English common law, with contractual considerations addressed in Section 4 below.

Whilst previous cases had dealt with issues relating to rights asserted in confidential information in the context of other established legal regimen, such as those governing employment relationships, copyright, patents and contractual relationships, it is generally accepted that the origin of the protection of rights in confidential information *as such* under the English common law was the High Court decision in *Prince Albert v Strange* (1849) 41 ER 1171.

Prince Albert v Strange related to an application for injunctive relief to prevent the publication of a catalogue that amongst other things described a number of etchings created by Prince Albert and Queen Victoria, prints of which were to be shown as part of an exhibition to be held by the defendant. The defendant had acquired copies of the prints from an employee of a printer engaged by the royal family who had made the copies *"without [the printer's] consent or knowledge, and in violation of the confidence reposed in him"*. In confirming the decision to grant a perpetual injunction preventing publication of the catalogues containing descriptions of the prints, as well as the exhibition of the prints themselves, Lord Chancellor Cottenham acknowledged that "*this case by no means depends solely on the question of property; for a breach of trust, confidence, or contract itself would entitle the Plaintiff to the injunction*" [emphasis added]. This was the first time that the English court had acknowledged a free-standing right in "confidence" as a separate and distinct cause of action.

[1] The Reporter gives thanks to Iain McDougall and Andy Harris of MBM Commercial for providing insight regarding the position under Scottish law.

2.2. The Modern Approach

The protection of rights in confidential information under the English common law was subsequently acknowledged in a number of cases following the decision in *Prince Albert v Strange*, most notably in the Court of Appeal decision in *Saltman Engineering Co. Ltd v Campbell Engineering Co. Ltd* (1948) 65 RPC 203 which re-affirmed that rights in confidential information extend beyond those in which the parties were bound to one another by contract.

The modern statement of the law in this area is now generally accepted to have been summarised in the decision in *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41 in which Megarry J set out the following three requirements which must be established in order to succeed in an action for breach of confidence:

> *"First, the information itself…must 'have the necessary quality of confidence about it'. Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be unauthorised use of that information to the detriment of the party communicating it"*

The requirements set out by Megarry J in *Coco v A N Clark* are now routinely applied in breach of confidence cases and have been approved and applied by the Supreme Court (previously the House of Lords), which is the most senior court in this jurisdiction.[2]

2.2.1. The First Requirement: The Information Must Have the "Necessary Quality of Confidence"

In essence, the first requirement is that the relevant information must be confidential in the sense that it is 'secret' and not freely available in the public domain. In describing this requirement in *Coco v A N Clark,* Megarry J repeated the comment of Lord Greene MR in *Saltman* that the relevant information is *"not public…property and public knowledge"*.

The dissemination of information "publically" to a limited number of recipients or for a short period of time by means that would not draw it to the attention of the public at large may not be sufficient to destroy the "quality of confidence" necessary in order to enjoy protection[3]. Whether or not the information is "public knowledge" is therefore a question of fact and degree and depends on the specific circumstances of each case, involving an assessment of whether or not the relevant information was generally available and known within the jurisdiction at the relevant time.

It is knowledge of the public within this jurisdiction which is relevant to this assessment. For example, in *Franchi v Franchi* [1967] RPC 149 the mere fact that a patent specification had been published in Belgium did not in and of itself render the information contained in that specification incapable of being protectable confidential information in this jurisdiction. Rather, it was the fact that the court accepted that British patent attorneys would become aware of and inspect Belgian patent applications that rendered the information "public knowledge" and, therefore, incapable of protection under the law of confidence. Again, whether or not information has been made available to the public within this jurisdiction is a question of fact and degree. However, advances in communications technologies which have resulted in

[2] See *Douglas v Hello! Ltd (No. 10)* [2007] UKHL 21, for example.
[3] See *Franchi v Franchi* [1967] RPC 149

much easier access to information published around the world, particularly via the internet, has undoubtedly broadened the scope of information that may be said to be "public knowledge" within this jurisdiction.

The public release of a product may but does not automatically render any confidential information embodied in that product "public knowledge". It is the form that the particular embodiment of the confidential information takes and, in particular, whether or not that embodiment allows members of the public to access and understand the confidential information that is of key importance.

An interesting question arises in the context of products which do not disclose the relevant confidential information by their very release to the public, but from which it is possible to ascertain the relevant confidential information through reverse engineering of them. Jacob J considered this question in *Mars UK Ltd. v Teknowledge* [1999] EWHC 728 (Ch), a case in which the defendant had reverse engineered claimant's encrypted "coin discriminator" technology in order to re-programme coin operated machines to accept new denominations and currencies. Jacob J's view in that case was that despite being encrypted, in the defendant's hands the claimant's coin discriminator technology "clearly" did not possess the quality of confidence necessary to qualify for protection as confidential information because the defendant's right of ownership of the relevant machine in which the technology was incorporated included the right to find out how that machine worked.[4] However, at the same time Jacob J also acknowledged that if a third party was to steal the relevant information from the claimant directly, without going to the effort and expense of reverse engineering a machine to obtain it, that would amount to an unlawful breach of confidence.[5] One attempt by commentators to reconcile these apparently contradictory statements of the law has been to suggest that reverse engineering in these circumstances removes the confidential information *vis-à-vis* the party that has undertaken the reverse engineering exercise, but not the rest of the world. However, this approach is somewhat contrary to the statement of Morritt J in *Alfa Laval v Wincanton* [1990] FSR 583 that ownership of a machine gives rise to an entitlement *"to dismantle the machine to find out how it works and tell anyone he pleases"* [emphasis added], which Jacob J relied on in support of his observations in *Mars UK Ltd v Teknowledge*. An important point to note is that Jacob J's comments in *Mars UK Ltd v Teknowledge* were *obiter* and therefore not part of the binding decision of the case. As far as the Reporter is aware, this point has not been considered in any subsequent decisions and so this is an area of the law of confidence in this jurisdiction which remains open to further discussion and development in due course.

It is possible that a body of information that is comprised of constituent elements that are independently available in the public domain may nevertheless possess the "necessary quality of confidence" such as to be protected as confidential information. In such cases, the court will consider the extent to which independent time, skill (in the sense of intellectual effort) and labour has been expended in order to create the thing which is said to constitute confidential information. If that thing could only be created by undertaking the same processes that the party asserting a right in confidential information undertook to create it, then it may be protectable. A classic example of this is the approach to customer lists which although comprised of individual items of information that are individually publically available, such as

[4] Jacob J at [31]
[5] *Ibid* [32]

names, addresses and contact details, may nevertheless amount to confidential information by virtue of the time, skill and labour expended in order to create them.

2.2.2. The Second Requirement: The Information Must Have Been "Imparted in Circumstances Importing an Obligation of Confidence"

In *Coco v A N Clark,* Megarry J described this second requirement as an objective test as follows:

> *"…if the circumstances are such that any reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given to him in confidence, then this should suffice to impose upon him the equitable obligation of confidence"*

In circumstances where information is imparted under express terms which identify the relevant information as confidential, such as a disclosure made in accordance with the express terms of a contractual non-disclosure agreement or in a form which bears the word "confidential", ordinarily there should be little difficulty in establishing that this requirement has been satisfied. This will often be the case in relation to trade secrets, as noted by Lord Goff in *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 (HL). Again, whether or not the circumstances of disclosure of the relevant information alone and in the absence of an express statement gives rise to an obligation of confidence is a matter of fact and degree which is to be considered on a case by case basis.

The manner in which the information is treated by the parties, particularly the disclosing party, will be highly relevant. For example, in *Ocular Sciences v Aspect Vision Care* [1997] R.P.C. 289, Laddie J commented that *"If technology was treated by the parties as if it was common knowledge, it is likely to be reasonable for them to assume that it is being treated in the same way when it is passed on between them"*.

The conduct of the 'receiving' party is also relevant to this assessment. The reference to information being "imparted" should not be misconstrued as a restriction of the protection afforded to confidential information to only those cases in which the disclosing party willingly communicates information to another. The use of surreptitious means in order to gain access to confidential information has also been found to amount to good evidence that a 'receiving' party knew or objectively should have known from all of the relevant circumstances that the information obtained was confidential.[6] Of course, the use of surreptitious means to gain access to confidential information may also give rise to additional causes of action (under the tort of trespass, for example) or even criminal offences (such as those arising under the Computer Misuse Act 1990).

Other factors that have been found to be relevant to this enquiry include the nature of the information itself, whether the information was disclosed in a formal/business setting or a more informal setting and whether or not the parties understood subjectively that the information being disclosed was confidential. In *Attorney General v Observer Ltd.* [1990] 1 AC 109 (HL), Lord Goff sitting in the House of Lords went as

[6] See *Creation Records Ltd and Others v News Group Newspapers Ltd* [1997] E.M.L.R. 444, for example.

far as to suggest that the recipient of information acquired by accident may nevertheless be bound by a duty of confidence if that information is contained in an *"obviously confidential document*".[7]

A form of secondary liability may also apply in the case of a party which itself receives confidential information indirectly from a party which itself is bound by a duty of confidence to another. In *Vestergaard Frandsen A/S v Bestnet* [2013] UKSC 31, a case specifically concerning trade secrets, the Supreme Court confirmed that a third party that obtains information which it does not appreciate is confidential at the time of receipt may nevertheless become liable for a breach of confidence if it later becomes aware that the information is in fact confidential, even though the relevant information was not imparted to it by the party to which that duty is ultimately owed.[8]

2.2.3. The Third Requirement: There Must be Unauthorised "Use of the Information to the Detriment of the Party Communicating It"

This third and final requirement was described by Megarry J in *Coco v A N Clark* as the need to demonstrate "*an unauthorised use of the information to the detriment of the person communicating it*".

In many cases, once it has been found that a duty of confidence exists (i.e. that the first and second requirements have been satisfied) a subsequent finding that there has been an unauthorised use of the relevant information will usually be sufficient to establish that detriment has also been caused to the disclosing party. In many cases, the direct result of the misuse of confidential information is the unfair 'boost' achieved by the party which uses the information for purposes other than those for which it was disclosed to it. Of course an unfair 'boost' enjoyed by a competitor causes an indirect form of detriment to the party whose confidential information has been misused and which is therefore placed at a competitive disadvantage in the marketplace. This form of detriment has been readily acknowledged by the English courts as discussed in more detail in Section 3 below, in particular in relation to the concept of "springboard" injunctions.

2.3. "Trade secrets" as a sub-set of confidential information

As noted above, "trade secrets" fall within the general class of rights in confidential information under the English common law. There is no fixed definition of confidential information which amounts to a "trade secret".[9] However, the concept of a "trade secret" generally arises in the case law in one of two forms.

---

[7] Lord Goff at [281]-[282]
[8] Lord Neuberger at [25]
[9] Whilst Section 43(1) of the Freedom of Information Act 2000 ("FOA 2000") includes an exemption to the obligation upon public bodies to disclose information upon submission of a request under the FOA 2000 where the information requested constitutes a "trade secret", Ministry of Justice guidance has acknowledged that the FOA 2000 does not provide a definition of that term and nor is there a precise definition of it in English law generally – see here: https://www.justice.gov.uk/downloads/information-access-rights/foi/foi-s43-exemptions.pdf. Note also that the exclusion for information that amounts to a trade secret under Section 43(1) FOA 2000 is not absolute and therefore the relevant information will only be exempt from disclosure if, in all of

The first is as a general way of describing confidential information of a commercial, rather than a private or personal nature. Under this definition, a "trade secret" may take one of any number of forms. As noted above a list of customer details may qualify for protection as confidential information and may also therefore be considered a "trade secret" due to the commercial nature of the information. A business may choose to keep technical know-how relating to an inventive product, process or technique confidential, rather than apply for patent protection which necessitates disclosure of the relevant information in exchange for a limited period of monopolistic protection. Again, such information might also be considered a "trade secret" given the commercial context in which it arises. Even confidential technical know-how which might not be patentable may amount to a "trade secret" under this definition. Indeed, the "secret" recipes of well-known foodstuffs such as Coca Cola, Kentucky Fried Chicken seasoning and McDonald's "Special Sauce" are all very well-known examples of confidential information that would also be regarded as a "trade secret".

A second, narrower form of "trade secrets" has also been applied in cases considering the post-employment obligation of confidence owed by an employee to its former employer. A distinction between "trade secrets" and other forms of confidential information in a post-employment context was drawn by the Court of Appeal in *Faccenda Chicken Ltd v Fowler [1987] 1 Ch. 177*. That case involved an alleged breach of confidence by ex-employees of the claimant who had used sales information acquired whilst working for a former employer, including customer names, addresses, delivery routes and prices, when establishing a rival business. In its judgment in that case, the Court of Appeal noted that an employee owes a duty of good faith to its employer during the course of its employment which includes *inter alia* a duty not to disclose its employer's confidential information to third parties. However, once the employment contract has come to an end an ex-employee's implied duty of confidence to its previous employer was said to extend only to "*information which is of a sufficiently high degree of confidentiality as to amount to a trade secret"*.[10] By implication, therefore, in *Faccenda Chicken* the Court of Appeal suggested that certain categories of confidential information (trade secrets) are "more confidential" than other categories.

This report focusses on the wider form of "trade secrets" set out above. As noted above, the narrower definition set out by the Court of Appeal in *Faccenda Chicken* relates specifically to circumstances arising in the post-employment context only. In that regard, the court had to weigh up the interests of an employer in protecting its commercially sensitive information against the interests of former employees not being the subject of unduly restrictive obligations which might give rise to restraint of trade issues. As such, the definition of "trade secrets" set out in the *Faccenda Chicken* case is largely accepted to apply in a specific employment-related context only.

2.4. Personal and private information

Whilst rights in "personal" or "private" information had also historically been recognised as another sub-set of information that may fall within the general class of rights in confidential information, the enactment of the Human Rights Act 1998 ("HRA 1998") which came into force on 2 October 2000 (enacted in order

---

the circumstances of the case, the public interest in maintaining the exclusion outweighs the public interest in disclosing whether the public authority holds the information (FOA 2000 ss. 2 (1) - (3)).

[10] See Neill LJ at [135G]

to give effect to the European Convention for the Protection of Human Rights) resulted in the further extension of protection of this category of information within the law of confidence in this jurisdiction. A detailed review of the law of privacy post-HRA 1998 is outside the scope of this paper, which focusses on the protection of confidential information of a commercial nature i.e. trade secrets and know-how (see further discussion of which at 2.3 above). However, it should be noted that many of the leading cases arising from the rights in personal and private information extended by the HRA 1998 relate to actions brought by celebrities seeking to restrict the commercial exploitation of private information by the media[11] and the fact that many celebrities now routinely exploit their own private and personal information for commercial means (by allowing "exclusive" access to private functions such as weddings, for example) demonstrates that the enforcement of rights in private information may also have commercial implications.

2.5. Duration

In principle, a duty of confidence continues until the relevant information is no longer confidential unless the duty is otherwise released by the party to which it is owed, irrespective of how the information comes into the public domain.

As noted in Section 3 below, in certain circumstances the court will impose injunctions to prevent a party enjoying the benefit of its misuse of confidential information in circumstances where the information itself has become public. However, such injunctions will be time-limited and so a party will not be prevented indefinitely from using information which has become public.

3. Remedies for breach of confidential information

3.1. Overview

The court has a variety of different remedies that it may award depending on the particular factual circumstances giving rise to a finding of a breach of confidence. Forms of relief that are frequently awarded in breach of confidence cases in this jurisdiction include:

- Injunctions, both interim and final;
- Financial compensation by way of damages or an account of profit;
- Delivery up or destruction of materials and articles containing the relevant information or which embody a misuse of it;
- Declarations that the relevant information is (or is not) confidential in nature; and
- Publication and dissemination of the relevant judgment.

[11] See *Campbell v Mirror Group Newspapers Ltd [2004] UKHL*, which is now the leading case in this area

3.2. Injunctive relief

In many cases, including those involving commercial know-how and/or trade secrets, it is imperative that a claimant is able to prevent the misuse of confidential information quickly and before the conclusion of a full trial on the merits of the claim. The ability to obtain an interim (preliminary) injunction is therefore a very important form of relief available in breach of confidence cases.

In addition, for obvious reasons an injunction preventing the threatened but not yet actual disclosure or use of confidential information is often also extremely important and such injunctions, known as *quia timet* injunctions, are also available in appropriate cases.

The general principles applied by the court when considering applications for interim injunctions in this jurisdiction generally are set out in the House of Lords decision in *American Cyanamid Co. v Ethicon Ltd* (1976) AC 396. First, it must be established that there is a serious issued to be tried. If so, the court must then ask whether damages would be an adequate remedy for a party injured by the grant or refusal to grant the requested injunction. If not, the court must then consider where the balance of convenience lies, taking into account all of the circumstances of the case. If the matter is finely balanced, the court will usually seek to preserve the status quo, which in breach of confidence cases where a *quia timet* injunction is sought will often mean granting an interim injunction preventing use or disclosure of the relevant information pending determination of the claim at trial. A party which seeks an interim injunction will be required to give a cross-undertaking in damages which seeks to protect the subject of the injunction in the event that the claim subsequently fails at full trial. An interim injunction will be discharged once a final determination of the relevant claim has been made at which point a final injunction will be put in place if the claim is successful.

Ordinarily, injunctions in this jurisdiction are granted against specific individuals and/or legal persons. As such, an interim injunction will usually only bind those parties specifically named in the relevant court order. However, this position is slightly altered in breach of confidence cases by a principle arising from the House of Lords decision in *Attorney General v Times Newspapers Ltd* (1992) 1 AC 191 which established that a third party may also be liable for contempt of court if it discloses information that the court has ordered a party not to disclose and which would impede or interfere with a claim before the court if that third party also has knowledge of the terms of the relevant interim injunction. This principle, known as the "*Spycatcher"* principle due to the name of the publication to which the House of Lords case related, has particular implications in the context of publishing and broadcasting, where it may be desirable to put various publishers and broadcasters on notice of an injunction granted against specific parties. However, there is no reason why it might not also apply in other contexts, including those in which an interim injunction preventing the disclosure of confidential information that would be classified as commercial know-how and/or trade secrets has been granted.

Final injunctions are also available at the conclusion of a trial on the merits of a claim if a claim is successful and, again, such injunctions are also available on a *quia timet* basis.

The duration of any final injunction granted will depend on all of the factual circumstances of each individual case. Where a *quia timet* injunction has been granted, the court might be expected to grant an injunction restraining disclosure of the relevant information generally. Should such information subsequently enter the public domain by a route other than breach of the injunction, the party that is the subject of the injunction would then be free to apply to the court to have the relevant injunction discharged, much in the same way a defendant in patent infringement proceedings might apply to have an injunction against further 'infringing' activity discharged in the event that the relevant patent is subsequently invalidated.

The position is different in cases where the claim arises from a misuse of confidential information which has already taken place and that misuse has itself destroyed the confidential nature of the relevant information. Whilst the court will not ordinarily grant an injunction against the use of information which is no longer confidential, irrespective of the circumstances in which the information lost its confidential nature, the principle of the "*springboard*" injunction has developed over time in order to limit the commercial advantage that might otherwise be enjoyed in certain cases by a party that misuses the confidential information of one of its competitors.

The basis of the "springboard" doctrine was reviewed in detail by Arnold J in *Vestergaard Frandsen A/S v. Bestnet Europe Limited* (2009) EWHC 1456 (Ch). In that case, the judge noted springboard injunctions are only available in cases where the relevant information could have been compiled or obtained from other sources. Whilst the parameters of the doctrine remain somewhat unclear, Arnold J explained that in a situation where the defendant is still misusing the confidential information which has subsequently become publically available, the duration of any "springboard" injunction preventing the continued use of that information should be limited to the time it would take someone starting from public domain sources to reverse engineer or compile the relevant information, since this reflects the limited degree of confidentiality that is being enforced. The injunction granted in such circumstances is therefore designed to address the 'head start' advantage gained by the defendant's failure to undertake the exercise of obtaining the information from public sources.

3.3. Financial compensation – damages and account of profit

Financial compensation awarded in the form of damages that are awarded upon a finding of breach of a contractual duty of confidence (discussed in more detail in Section 4 below) will be calculated in such a way as to try to put the claimant in the position that it would have been in had it not been for the breach of contract. In that sense, damages for a contractual breach of confidence are compensatory rather than punitive and the calculation of an appropriate award will depend on all of the relevant circumstances, such as whether or not the claimant uses or used the relevant information for its own benefit or if it derives income via a licensing model, for example. Damages are also available upon a finding of the breach of equitable common law rights in confidential information[12] and will be calculated on a similar basis, i.e. to put the claimant in the same position as it would have been in had it not been for the breach of confidence.

[12] Senior Courts Act 1981 s. 50

An alternative form of financial compensation may be ordered by way of an account of the profit generated by the defendant as a result of its misuse of the relevant confidential information. Only those profits directly attributable to the defendant's misuse of the relevant confidential information may be recovered on this basis, so an apportionment of actual profits generated must be made. In practice, this can be a difficult calculation to undertake with any degree of certainty and the court will often be prepared to make an award on estimated percentages supported by evidence.

Many breach of confidence cases will be dealt with on a 'split trial' basis, with a trial to determine liability followed at a later stage by enquiry as to quantum (in the event liability is established). Ordinarily, a successful claimant will be given the opportunity to elect between financial compensation in the form of damages or an account of profit. However, the court will often order further disclosure of relevant information to be made in accordance with the jurisdiction established in *Island Records Ltd v Tring International pls* (1996) 1 WLR 1256 prior to such election being made in order to enable a claimant to choose the basis that is most advantageous to it.

3.4. Delivery up or destruction

Positive injunctions requiring the delivery up or destruction of copies or articles containing or embodying confidential information are usually available as alternatives to one another, the former often preferred in cases where the claimant has concerns as to whether the defendant can be trusted to destroy the relevant materials. In circumstances where destruction is ordered against a corporate defendant, it is common to seek an order that a named representative of the defendant company provides a witness statement endorsed by a statement of truth that destruction has taken place so that the relevant individual may be personally liable for contempt of court in the event that destruction does not take place in accordance with the relevant order.

In appropriate cases, the court may order the modification of an article or erasure of confidential information from a document rather than complete destruction of it, which again reflects the restitutionary rather than punitive nature of relief in breach of confidence cases in this jurisdiction.

3.5. Declarations

Rule 40.20 of the Civil Procedure Rules ("CPR") provides that the court may make binding declarations whether or not any other remedy is claimed, which would include the power to declare that certain information is or is not confidential. Naturally, any such declaration would need to be sought in such terms as not to destroy the confidential nature of the relevant information.

3.6. Publication and dissemination of judgment

The publication of judgments in intellectual property cases required in accordance with Article 15 of Directive 2004/48/EC on the enforcement of intellectual property rights has also been extended by the English court to breach of confidence cases.[13]

4. The protection of confidential information by contract

In addition to the equitable protection of rights in confidential information under the English common law, in this jurisdiction it has also long been possible to protect rights in confidential information by contract.

In many sectors, the entry into a confidentiality agreement (commonly known as non-disclosure agreements or NDAs) at the outset of a prospective trading relationship is accepted as a matter of routine and many other forms of commercial agreement will include specific contractual terms governing the disclosure, use, retention and return of any confidential information that may flow between the respective parties during the course of the relationship.

There are a number of perceived benefits of seeking to protect confidential information, including commercial know-how and trade secrets, by contract. For example, as noted above a key "ingredient" necessary to establish a common law right in confidential information is to show that the relevant information has been imparted in circumstances importing an obligation of confidence. This is an objective question which involves a factual enquiry and, therefore, gives rise to potential uncertainty. The entry into an explicit agreement governing the use of information which is designated 'confidential' by the relevant parties avoids such issues. Another benefit is that the parties to a contractual agreement are largely free to agree between themselves the relevant safeguards that are to be put in place in order to preserve the confidential nature of the relevant information, which may extend far beyond the scope of relief that might be available via the court when relying on a common law right.

Of course, contractual obligations generally only bind the parties to the relevant contract. As such, there are many situations in which a party may need to rely on the protection offered by the common law duty of confidence, rather than rights in contract, in order to protect valuable know-how or trade secrets.

5. The treatment of confidential information in litigation

In proceedings before the courts of England and Wales, a party that is under a duty to disclose a certain category of document must do so irrespective of whether or not that category includes documents containing confidential information, unless such documents are also fall into narrow categories of documents that are privileged from disclosure (such as documents containing communications that are subject to client-attorney privilege). As a general rule, a party to whom a document has been disclosed also

[13] See the order of Arnold J at 114 in *Vestergaard Frandsen A/S v. Bestnet Europe Limited* (2009) EWHC 14556 (Ch), for example.

has a right to inspect that document.[14] The potential for disclosure of commercially sensitive know-how and trade secrets during the course of proceedings is obvious.

Whilst it is generally the position that documents disclosed in the course of proceedings may only be used for the purpose for which they are disclosed[15], it is well recognised that this basic safeguard may not in and of itself sufficiently protect legitimate rights in confidential information from misuse by a receiving party. Therefore, in order to balance the interests of parties to litigation seeking to maintain the confidential nature of commercially sensitive information, a number of practices have developed to restrict the scope of the unnecessarily broad circulation of confidential information during litigation.

The use of 'confidentiality clubs' is one way in which the circulation of commercially sensitive information can be restricted to an acceptable level. In basic terms, the court may order that copies of certain discloseable documents are only made available to certain named individuals (in cases involving highly sensitive information, this may be to legal advisors only). Members of the 'club' will frequently be required to give personal undertakings not to misuse or disseminate any confidential information that is made available to them in the course of proceedings, giving rise to personal liability, including the possibility of contempt of court, if such information is subsequently misused.

The redaction of commercially sensitive information which is irrelevant to the relevant proceedings from otherwise discloseable documents is another frequently-used way of limiting the risk of disclosure of commercially sensitive information in litigation.

As a general rule court hearings in this jurisdiction are heard in public, which gives rise to a further risk of disclosure of confidential information to the public at large. Again, the court procedures have developed to mitigate this risk somewhat. In extreme cases requests can be made to have proceedings heard *in-camera* (i.e. not in public), albeit it is unlikely that the court would grant such a request on the basis of the risk of disclosure of commercial confidential information only. It is more likely that the court might be prepared to hear evidence or submissions relating to confidential information only *in-camera*, or to agree not to read the contents of documents containing such information out in open court.

6. Attempts to reform the law relating to the protection of rights in confidential information

There have been relatively few attempts to reform the modern law relating to the protection of rights in confidential information.

In 1997, the Law Commission of England and Wales published a consultation paper entitled "Legislating the Criminal Code: Misuse of Trade Secrets" which concluded that there was a *"strong case*" in favour of the criminalisation of the misuse of trade secrets.[16] However, this recommendation was not acted upon and

[14] CPR 31.3
[15] CPR 31.22(1)
[16] See here: http://lawcommission.justice.gov.uk/docs/cp150_Legislating_the_Criminal_Code__Misuse_of_Trade_Secrets_Consultation.pdf

no further steps towards the enactment of legislation to introduce an offence relating to the misuse of trade secrets have been taken since that time.

By way of an example of the general consensus amongst practitioners that the law in this area is generally sufficiently developed, a review conducted by AIPPI UK Group in 2010 in response to questions relating to "Protection of trade secrets through IPR and unfair competition law" concluded that "*trade secrets can in practice in the UK be effectively protected through actions brought in the civil courts for breach of confidence*".[17]

More recent consideration and discussion of the law in this area has, of course, been stimulated by the draft Directive on the Protection of Undisclosed Know-how and Business Information originally published on 28 November 2013. In September 2014 the Law Societies of England and Wales, Scotland and Northern Ireland issued a joint position paper in response to the EU Council's opinion on the draft Directive.[18] The response to the draft Directive has been reasonably positive, with general agreement that there are benefits to be enjoyed as a result of a common approach to the protection of trade secrets across Europe. However, as noted by the Law Societies' paper "*the devil is always in the detail*" and concerns have been raised about certain aspects of the proposed Directive. For example, the need to establish a link between the commercial value of information as a result of its confidentiality in order to qualify as a trade secret under Article 2(1) b of the draft Directive has been questioned. Such a requirement would represent a reasonably significant departure from the general approach to rights in confidential information and, by extension, trade secrets, in this jurisdiction.

7. Personal reflections

The Reporter shares the view expressed by Lord Neuberger in the Supreme Court in *Vestergaard Frandsen A/S v Bestnet* [2013] UKSC 31 that "*…in a modern economy, the law has to maintain a realistic and fair balance between (i) effectively protecting trade secrets (and other intellectual property rights) and (ii) not unreasonably inhibiting competition in the market place"*.[19]

The way in which the protection of rights in confidential information under the equitable jurisdiction of the courts in accordance with the English common law has developed over time has, in the Reporter's view, broadly resulted in a position which at present does achieve the balance referred to by Lord Neuberger.

Admittedly, there are certain aspects of the law in this area that remain unclear (such as the position regarding the status of confidential information that has been obtained by reverse engineering, for example) and commercial uncertainties arising from that, ideally, are to be avoided. However, there is much to be said for the flexibility that arises from the court's ability to deal with these cases in accordance

[17] A full copy of the AIPPI UK Group response to Question 215 is available here: https://www.aippi.org/download/commitees/215/GR215united_kingdom.pdf
[18] A copy of the full response paper is available here: file:///C:/Users/R3ddo9/Downloads/LSBO-Briefing-Trade-Secrets.pdf
[19] at [44]

with its equitable jurisdiction, as opposed to the potentially more rigid approach that might result from attempts to codify the law in statute.

The AIPPI UK Group 2010 response referred to above (to which the Reporter also contributed) reflects the Reporter's general perception that practitioners in this jurisdiction consider that the law as it stands does provide effective protection for know-how and trade secrets in this jurisdiction as things stand. As such, there seems little need or appetite for significant reform in this area at this time. That being said, the prospect of greater harmonisation of the protection of valuable trade secrets across EU Member States is also to be welcomed, as long as the proposed Directive can achieve the right balance between the fair protection of the legitimate interests of rights holders on the one hand and commercial competition on the other.