

Can you keep a secret? The trail of confidential information and the need for reasonable enquiries

Alexandros Antoniou
a.antoniou@essex.ac.uk

Citations of relevant cases

Travel Counsellors Ltd v Trailfinders Ltd [2021] EWCA Civ 38 (19 January 2021)
Trailfinders Ltd v Travel Counsellors Ltd and Ors [2020] EWHC 591 (12 March 2020)

Single sentence summary

In dismissing an appeal against the decision of the IPEC in *Trailfinders Ltd v Travel Counsellors Ltd and Ors* [2020] EWHC 591, the Court of Appeal held that an equitable duty of confidentiality arises when the recipient of information is reasonably expected to have made enquiries in relation to the confidential nature of that information but fails to do so.

Legal context

Trade secrets are valuable commercial assets in that they allow businesses to gain a competitive edge over their rivals without competitors knowing how that advantage is achieved. In the UK, trade secrets can be protected under two different regimes: the common law of confidentiality and the statutory regime under the Trade Secrets (Enforcement, etc) Regulations 2018.

The common law tort of breach of confidence has evolved over the years and has been tested on several occasions before the courts. Three elements are typically required if a case of breach of confidence is to succeed: first, the information itself must have the necessary quality of confidence about it; second, that the information must have been imparted in circumstances importing an obligation of confidence; and third, there must be an unauthorised use of that information to the detriment of the party communicating it, usually the right holder (*Coco v AN Clark (Engineers) Ltd* [1969] RPC 41, 47). An alleged breach of confidence may be defensible if it is in the public interest, e.g. to expose wrongdoing, negligence or hypocrisy (*Lion Laboratories v Evans* [1985] QB 526).

The tort of breach of confidence initially offered limited protection as it was only available where there was a pre-existing relationship of confidence between the parties, e.g. an employer–employee relationship or a marriage (*Argyll (Margaret Duchess of) v Argyll (Duke of)* [1965] 1 All ER 611). Over the years, this requirement lessened. Lord Goff stated in *Att-Gen v Guardian Newspapers (No 2)* [1990] 1 AC 109, 281 that such a relationship was no longer required, thereby expanding the law: where confidential information is given by one person to another and the recipient is either expressly told by the discloser or ought to understand from the circumstances surrounding the communication that the information is fairly and reasonably to be regarded as confidential, then equity acts on the recipient's conscience to prevent them from making an unauthorised use of the information at issue. The test regarding the recipient's appreciation of whether the information was confidential is objective, in that it requires the discloser to show that the recipient ought to have appreciated the information was confidential, regardless of their actual state of mind (*Coco v AN Clark* at 48).

Trade secrets are also protected in the UK by the statutory regime established by the Trade Secrets Regulations, which came into effect in June 2018 and implemented the Trade Secrets Directive (EU) 2016/943. Before the implementation of the Directive, EU member states afforded a markedly uneven protection and enforcement options to trade secrets. This patchwork of separate national laws risked creating barriers to cross-border investment and know-how transfers. The Directive provides a minimum level of uniform protection across member states to enable businesses which monetise their trade secrets to undertake commercial activities across national borders with reasonable certainty. Under the Directive, information qualifies as a trade secret if it meets all of the following three criteria (Article 2(1)): first, it must be a secret, meaning that the information must not be generally known among (or readily accessible to) relevant persons within the circles that normally deal with the kind of information in question. Second, the information derives its commercial value from the fact that it is secret; and third, reasonable steps have been taken by the owner to keep the information secret.

Under the Directive, the acquisition, use and disclosure of a trade secret is unlawful in a range of contexts, including where a trade secret has been acquired in breach of a confidentiality or other contractual obligation (Article 4(3)), or by any other conduct which may be considered under the circumstances 'contrary to honest commercial practices' (Article 4(2)(b)). The latter remains undefined and therefore open to broad interpretations and potentially divergent implementation practices by member states. In addition, the Directive protects against the subsequent use or disclosure of trade secrets that have previously been unlawfully acquired (Article 4(4)). Importantly, it also makes it illegal to deal in goods 'the design, characteristics, functioning, production process or marketing' of which has benefited significantly from trade secrets that have been unlawfully acquired, used or disclosed (Articles 2(4) and 4(5)). The Directive introduces a minimum set of measures, procedures and civil remedies (including interim injunctions and precautionary seizure of suspected infringing goods) (Articles 6 and 7) that are available for the misappropriation of trade secrets. The Directive also covers the preservation of confidentiality during litigation generally (Article 9).

As the UK's common law framework for protecting trade secrets as a specific form of confidential information is well-established and robust, the Trade Secrets Regulations do not purport to transpose the whole Directive into UK law. They introduce a new statutory regime (which enacted the Directive's definition of a trade secret), thereby creating a parallel legal framework which neither replaces nor conflicts with but rather supplements the protection afforded to confidential information under the UK common law. The explanatory memorandum to the Regulations states that several provisions of the Directive have already been implemented in the UK by the principles of common law and equity, statute and court rules and thus 'the instrument addresses only those areas where gaps occur or where the implementation of the provisions of the Directive [in the UK] will ensure legal certainty, making the law more transparent and coherent' (Explanatory Notes to the Trade Secrets (Enforcement, etc.) Regulations 2018, para 2). Regulation 3 also clarifies that the question of whether the acquisition, use or disclosure of a trade secret is unlawful is to be determined by reference to the law of confidence and that the remedies available at common law will also be available to a trade secret holder who has brought proceedings under the Regulations. The Trade Secrets Regulations do not dispel the need for contractual confidentiality provisions and non-disclosure agreements (NDAs), which are commonly used in business settings to govern, clearly, business relationships. NDAs can still be used to impose more rigorous or extensive obligations in the exchange of valuable information. Such agreements can also be helpful from an enforcement perspective and be relied upon to bring a parallel claim for breach of contract.

The Intellectual Property Enterprise Court (IPEC) explored the interplay between the tort of breach of confidence and the Trade Secrets Directive in the case of *Trailfinders Ltd v Travel Counsellors Ltd and Ors* [2020] EWHC 591. This decision is the first judicial reference to the Directive and provides an example of its impact on the protection of trade secrets in an employment context, as several cases of misuse of trade secrets, in practice, tend to involve employees' activities (see European Commission, *The scale and impact of industrial espionage and theft of trade secrets through cyber* (April 2019) 42 <<https://ec.europa.eu/docsroom/documents/34841>> accessed 12 August 2020). Although the IPEC referred in its judgment to the Directive, the Court of Appeal in *Travel Counsellors Ltd v Trailfinders Ltd* [2021] EWCA Civ 38 did not consider its applicability any further, as the events in question occurred prior to its implementation.

Facts

The facts of the dispute are not uncommon in trade secrets cases. Trailfinders, an independent travel agent, claimed that the defendants (its former sales consultants) took client information from its customer databases whilst they were employed and subsequently accessed such information from Trailfinders' client-facing platform after they left to join the competitor Travel Counsellors Ltd (TCL), which operates under a franchise model with self-employed travel consultants. The information at issue concerned client names and contact details, nationalities, dates of birth, passport numbers, details of past and provisional bookings with relevant reference numbers, clients' preferences and typical budgets as well as significant dates, like anniversaries, which were stored on the company's databases. In January 2020, Trailfinders brought an action against TCL.

Analysis

Trailfinders alleged that the ex-employees breached the implied terms of their employment contracts and/ or their equitable duties of confidence owed to their former employer (Trailfinders). TCL was also alleged to have breached its obligation of confidence by receiving the confidential information at issue and allowing it to be exploited for the pursuit of future business.

Trailfinders v TCL (2020): The IPEC judgment

In assessing the liability of Trailfinders' former employees, HHJ Hacon stated that, although the substantive principles governing the protection of confidential information under English law remain intact, the Directive 'shines an occasional light on those principles' (at [18]). Earlier authorities show that the nature of the information involved has a bearing on the extent of the contractual duty of confidence. In particular, the leading judgments in *Faccenda Chicken Ltd v Fowler* [1985] FSR 105 and *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] UKSC 31, have established that there are different types of information to which employees could be exposed during their employment that enjoy varying degrees of protection: the first category includes information which is not confidential, i.e. information which is not commercially or competitively sensitive, information which is trivial or part of the public domain (Faccenda Category One); the second category comprises information obtained during the course of an employee's career and forms part of their skills and experience (Faccenda Category Two); and the third, most sensitive, category involves trade secrets (Faccenda Category Three). Trailfinders' client information was 'highly characteristic' (*Trailfinders* at [69]) of information long regarded by the English courts as liable to be subject both to an implied term of confidence in an employment contract and an equitable obligation of confidence. The defendants had accessed and compiled the information on the company's database while still employed and subsequently retrieved further information after leaving Trailfinders.

The general duty of fidelity and good faith, which is an implied term of the contract of employment, prevents an employee *during* the period of their employment from disclosing to an employer's competitor confidential information which was honestly acquired in the normal course of employment and remains in their head as part of their own experience and skills (*Marathon Asset Management LLP v Seddon* [2017] EWHC 300, [111] (Leggatt J)). This duty terminates post-employment (*Trailfinders* at [43]), but it does not follow that such information (second category) can always be freely used or disclosed when the relevant employment ends. There may still be a finding of liability if, for example, while still employed an employee copied down customer information or deliberately memorised it for disclosure or use (e.g. sale or exploitation) *afterwards*. The act of copying, e.g. extracting Outlook contacts list of names on a portable flash drive, suggests that this information was not part of the employee's general knowledge as they could not remember it without copying. If that information is used, or so threatened, in an unauthorised way to the detriment of the owner, this copying or memorising can be actionable, without disturbing the balance between, on the one hand, effectively protecting trade secrets and, on the other, not unreasonably restricting employees in their honest attempts to seek new opportunities in the marketplace (*Trailfinders* at [43]; *Vestergaard* at [44]). By copying client information for use by TCL after leaving Trailfinders, the defendants were found to have breached their implied contractual terms of confidence.

The disclosure of the information by the defendants to their new employer (TCL) and its subsequent use also amounted to a breach of their equitable obligation of confidence. HHJ Hacon ruled that Trailfinders' former employees appreciated, or ought to have appreciated, that the client information was confidential. Consistently with the law on implied contractual terms of confidence, the equitable obligation of confidence owed to Trailfinders could not be enforced by the claimant in relation to information acquired as part of the defendants' experience and skills while employed but extended to cover any information that was 'deliberately memorised' (*Trailfinders* at [43] and [77]) for use after the conclusion of the employment. Information acquired in this manner would not count as an employee's own skill and experience (and thus would fall outside Faccenda Category Two information). The defendants' argument that none of the information taken was confidential because it was accessible from publicly available sources (or by speaking to the clients) was rejected by the judge. It was not a defence to an allegation of breach of confidence that the individual in breach could have obtained the information elsewhere (*Force India Formula One Team Ltd v Aerolab Srl* [2013] EWCA Civ 780, [72] (Lewison LJ)). This is because the defendants dispensed with the necessity of going through the process of compiling the information themselves and thereby saved a great deal of trouble, labour

and time after the end of their employment with Trailfinders, instead of piece-by-piece sourcing the information from public sources. As such, they benefited from a head-start over others by using the information they had received in confidence from their previous workplace (*Trailfinders* at [35] - [38]).

Information qualifying as a trade secret (Faccenda Category Three) is treated differently: HHJ Hacon explained that an implied term in an employee's contract of employment restrains the use or disclosure of trade secrets without the employer's consent both during and after the period of employment (*Trailfinders* at [21]). Whether a piece of information can be conferred the status of a trade secret depends on factors such as the nature of employment and information itself, the employer's attitude towards it and whether the relevant information is readily separable from an employee's general knowledge that is free to use or disclose (*Faccenda Chicken Ltd v Fowler* [1987] Ch 117, 137-138 (Neill LJ)). In examining whether the information taken by Trailfinders' ex-employees were of a sufficiently high degree of confidentiality to be elevated to the level of trade secrets, the judge referred to the test under the Trade Secrets Directive and held that the client information met the required criteria (although the claimants had classified the information at issue as falling into Faccenda Category Two). HHJ Hacon observed that the definition adopted by the Directive provides the 'best guide' (*Trailfinders* at [29]) on the distinction between information which is confidential and information which is not.

More specifically, HHJ Hacon found that the definition of trade secrets in the Directive is wider than the common law categorisation, in that it encompasses information falling both within Faccenda Category Two and Category Three (*Trailfinders* at [14]). This might seem puzzling at first sight. The rationale behind Category Two is that if information capable of becoming part of an employee's skill and experience was to be classed as trade secrets protected by confidentiality after the end of employment, trade and competition would be inhibited by unreasonably restraining employee mobility. This is recognised in Article 1(3)(b) of the Directive which states: 'Nothing in this Directive shall be understood to offer any ground for restricting the mobility of employees. In particular, in relation to the exercise of such mobility, this Directive shall not offer any ground for [...] limiting employees' use of experience and skills honestly acquired in the normal course of their employment.' So, for the purposes of the Directive, 'honestly acquired' Faccenda Category Two information is not deemed a trade secret, leaving thus unaffected the principle that post-employment such information is not confidential and can be legitimately deployed (*Trailfinders* at [9]). But, if honestly acquired information is excluded from the scope of the Directive, it seems reasonable to maintain that *unlawfully* acquired Faccenda Category Two information is covered. This must have been the basis of the judge's finding.

The Court missed, however, the opportunity to provide clarity on the question of what constitutes 'reasonable steps' in ensuring that trade secrets are protected under the 2018 Regulations. *Trailfinders* suggests that the threshold for satisfying this requirement was not overly demanding in this case. The protection of client information through systems security and other specific internal agency protocols (e.g. use of passwords and online portals that limit data access to clients by requiring their name and booking reference) may not have been 'as rigorous as it should have been' (*Trailfinders* at [73]), but was deemed sufficiently robust under the circumstances. The evidence before the court demonstrated that an attempt to withhold access had been made and reasonable procedures had been put in place to safeguard the information from public disclosure. HHJ Hacon concluded that the franchisee travel consultants who used their previous client lists in their new jobs breached not only implied terms of their employment contracts and equitable duties of confidence owed to Trailfinders but also committed unlawful acts in breach of Articles 4(2) and 4(3) of the Directive.

As far as the scope of liability was concerned, TCL's business model with franchisee travel consultants meant that it did not employ the defendants and was not vicariously liable for their acts. The defendants were not TCL's agents either and thus TCL could not be made liable for their individual acts as their principal (*Trailfinders* at [133] – [136]). However, and on the facts, HHJ Hacon found that the franchisees were 'encouraged to bring with them details of existing clients and were not warned about any risk of breach of confidence' (*Trailfinders* at [123]). It was also evident from the franchisee agreement signed by the defendants that TCL regarded its own equivalent information as confidential and part of its intellectual property. Therefore, the prospect of TCL believing that Trailfinders did not consider its client information as being confidential was 'highly improbable' (*Trailfinders* at [121]). TCL had received a large quantity of client information from the defendants in circumstances which put it on notice that some of the information was likely to be confidential to

Trailfinders. Any reasonable person of sufficient significance in TCL's operations such as their CEO would have been aware that at least part of the contact information brought to TCL by the defendants was likely to have been copied from customer data belonging to Trailfinders. 'There was too much of it to have been carried in their heads' (*Trailfinders* at [131]), HHJ Hacon observed. TCL therefore knew, or ought to have known, under the circumstances that they received information which the claimants reasonably regarded as confidential. Consequently, TCL was held to have breached both an equitable obligation of confidence owed to Trailfinders and Article 4(4) of the Directive (i.e., the use or disclosure of a trade secret shall be considered unlawful when the recipient knew or ought to have known under the circumstances that the trade secret had been obtained unlawfully, or in breach of any contractual duty, or any other duty to limit the use of the trade secret).

TCL v Trailfinders (2021): The Court of Appeal decision

In January 2021, TCL appealed on the grounds that the IPEC applied the wrong legal test in finding that TCL owed an obligation of confidence to Trailfinders with respect to the information received by it from the sales consultants. The Court of Appeal unanimously dismissed the appeal, holding that HHJ Hacon had articulated and applied the correct test to the facts. In particular, the recipient or acquirer of confidential information must either have been told the information was confidential or had notice that this was the case. Whether or not the recipient or acquirer ought to have appreciated it was confidential is to be objectively determined from the perspective of 'a reasonable person standing in the position of the recipient' (*TCL* at [14] citing *Primary Group (UK) Ltd v Royal Bank of Scotland Plc* [2014] EWHC 1082, [223]).

The Court of Appeal held that 'if the circumstances are such as to bring it to the notice of a reasonable person in the position of the recipient that the information, or some of it, may be confidential to another, then the reasonable person's response may be to make enquiries' (*TCL* at [28] (Arnold LJ)). If the reasonable person would, on the facts, make enquiries as to whether the information was confidential, but the recipient abstained from doing so, then an equitable duty of confidentiality arises. It is not essential for the recipient to have turned a blind eye as to whether the information was confidential (*TCL* at [29]). The lack of reasonable enquiries can be enough to breach the equitable duty of confidence.

The decision also clarified that an obligation of confidence would not arise only when the recipient was on notice that the entirety of the information received was likely to be confidential. If the reasonable person in TCL's shoes had been aware that at least some of the information was likely to be confidential, then they would have made enquiries (*TCL* at [30] – [31]). TCL did not do so. The quantity of the information disclosed by one of the Trailfinders' ex-employees supported the finding that TCL was on notice that at least part of the information was likely to be confidential to their competitor. The Court of Appeal agreed with HHJ Hacon that 'TCL must have appreciated that [one of the franchisee consultants] could not have carried all that information in his head, which made it probable that he had copied at least some of it from Trailfinders' client database (as was in fact the case)' (*TCL* at [33]).

Practical significance

The Court of Appeal's conclusion provides additional guidance on the equitable duty of confidence in circumstances where confidential information belonging to a business was misused by a competitor who had received it by virtue of that business' ex-employees. The decision is of interest because, prior to the TCL appeal, there had been 'surprisingly little authority' (*TCL* at [25]) specifically addressing the question of whether the absence of reasonable enquiries on the part of the recipient of the information is sufficient to breach the equitable duty of confidence.

The Court of Appeal ruling serves as a warning of the duty placed on a recipient of potentially confidential information to make enquiries as to whether the information received (or some of it) was confidential to another, where a reasonable person would do so. However, the issue of whether a reasonable person *would* make such enquiries, and if so, what nature they should assume and what processes might be engaged, will inevitably be fact-specific and context-dependent. The decision in *TCL v Trailfinders* emphasises that businesses receiving from a third party (e.g., a new employee) information that relates to a competitor may need to make reasonable enquiries about its source and

This is an Accepted Manuscript of an article published by Oxford Academic in the ***Journal of Intellectual Property Law and Practice*** and is available online at the following permanent link: <https://doi.org/10.1093/jiplp/jpab086>

carefully consider its status in order to mitigate the risk of being found liable for breach of equitable obligations of confidence.

Finally, in ruling that the implementation of the Directive has not affected the substantive English law principles on the protection of confidential information (including the protection afforded by equitable obligations of confidence and implied terms of employment contracts), the IPEC judgment in *Trailfinders* is a welcome clarification in showing how the two regimes can work together in practice.

Accepted