35/10; [2010] VSC 293

SUPREME COURT OF VICTORIA

AUTOMOTIVE DEALER ADMINISTRATION SERVICES PTY LTD v KULIK

Mukhtar AsJ

4, 25 June 2010

CIVIL PROCEEDINGS – DISCOVERY — INSPECTION OF DOCUMENTS — COMPUTER DATABASE AS DOCUMENT — EXPERT INSPECTION OF COMPUTER SERVER AND NETWORKED DOCUMENTS — ALLEGED BREACH OF CONFIDENCE — SEARCH FOR CONFIDENTIAL INFORMATION ON DATABASE — DISCRETIONARY CONSIDERATIONS – WHETHER APPROPRIATE TO GRANT APPLICATION FOR DISCOVERY.

ADAS is in the business of handling warranty claims made by car owners against motor car dealers. K. was the director and sales manager of ADAS but ceased his employment and set up his own company with a similar business in name and structure as ADAS. It was alleged by ADAS that K. diverted their business to his company by inducing the customers of ADAS to deal with K.'s company in the mistaken belief that they were dealing with ADAS principally as a result of its deceptively similar name. In response to the application for discovery, K. stated that the information obtained by his company came not from the database of ADAS but from various emails and from enquiries made directly with the customers namely, the motorcar dealers.

HELD: Application for discovery of documents granted.

1. Discovery and inspection are essential tools of justice to enable litigants, both plaintiff and defendant, to investigate facts ultimately to enable a Court to get to the truth of the matter. Agreements are frequently made in the course of litigation in order to avoid interlocutory skirmishes and added expense. In the context of civil procedure, such agreements usually as here involve an existing duty or obligation to comply with procedural steps anyway, and therefore lack consideration. Such agreements cannot be regarded as binding in a sense of precluding any additional steps being taken. The "agreement" was the product of an isolated summons and in any event, the previous arrangements did not extend to inspection of the computer server and the networked computers.

2. A Court might intervene and prevent further discovery and inspection if the Court regards the additional pursuit over and above that which was "agreed" as being indicative of a misuse of court processes. But this is not the case here. To the contrary, it appears that the nature of the investigative exercise is such that it now does require the involvement of a computer expert to look into or "interrogate" the database and the server and the network computers to truly make the most of the discovery process. One cannot tell, but it may well result in the ascertainment of facts which corroborate the defendants' case.

3. Orders of the type sought by ADAS are naturally resisted in trade or commerce because they are, by their nature, invasive. No business is comfortable having a litigation adversary having access to its database, its server and its networked computers. There is the probability that the ADAS's expert scrutineer will come across irrelevant or privileged or confidential information, and the inspection exercise will be disruptive to the second defendant's business. But there is no avoiding this. The discretion to be exercised in this case is beneficial in character. The most a Court can do practically speaking is to put in place undertakings as to strict non-disclosure and confidentiality by the computer expert and directions requiring that the expert's work be done under the supervision of K's company and that any information extracted be also given to the defendants or their legal representatives. Another measure is to ensure the second defendant has an opportunity to seek legal advice and consult with its lawyers to see if there are claims of privilege or confidentiality for any documents or information as extracted by the expert or proposed to be extracted.

4. The application is not fishing. With protective measures in place, ADAS' request is legitimate. The investigative task has become unavoidably computer technical, and it requires expert investigation. It would be unjust to deny ADAS to inspect the database again, and the server and the networked computers. Accordingly, the application is granted.

MUKHTAR AsJ:

1. When the milkman in *Wessex Dairies v Smith* [1] did his last round on a Saturday afternoon,

he told his employer's customers that he was going to set up business for himself, and would be in a position to supply them with milk. That was held to be a breach of an employee's duty to serve his employer with fidelity until the last hour of his service.

2. The evidence here is not so clear because the plaintiff alleges the methods were surreptitious and were a matter of timing, and require the "interrogation" of the second defendant's computer system as part of the discovery and inspection pre-trial process.

3. The plaintiff is in the business of handling warranty claims made by car owners against motor car dealers. The plaintiff's "customers" are the car dealers or traders who give the warranty to the car owner on sale. The confidential information is the customer database, and the warranty administration database which identifies the renewable contracts handled by the plaintiff.

4. The first defendant, Kulik, was the plaintiff's director and sales manager. The third defendant was the plaintiff's claims manager. The fourth defendant was an employee of the plaintiff, and Kulik's de facto wife. It is alleged that Kulik incorporated the second defendant Automotive Dealer Services Pty Ltd ("ADS") on 27 May 2008. That is a strikingly similar name to the plaintiff's name of Automotive Dealer Administration Services Pty Ltd. The plaintiff alleges that between then and 30 June 2008 (when Kulik and the others ceased their employment with the plaintiff) Kulik took or accessed the plaintiff's customer database and the warranty administration database to set up the same business to be conducted by his new company, ADS. There are other allegations of theft and misappropriation of cheques. The plaintiff alleges that ADS has diverted the plaintiff's business to itself by inducing the plaintiff's customers to send their business to ADS in the mistaken belief that they were dealing with the plaintiff, principally as a result of its deceptively similar name. The plaintiff alleges that since 1 July 2008 it has had virtually no business calls and has received but a very small fraction of expected new business.

5. In its defence ADS and Kulik say amongst other things that they obtained the alleged confidential information from the motorcar dealers in various emails around July 2008 and not by taking the plaintiff's database. That is, Kulik made enquiries directly of the customers, in this case the motorcar dealers.

6. ADS has filed a supplementary affidavit of documents in which document number 3 is identified as "ADS Customer & Warranty Database in electronic format." A database is a "document" for present purposes. Inspection of the database may be ordered by the Court under r29.11, more especially under r29.12. That is clear from the definition of "document" in s38(d), (e) and (f) of the *Interpretation of Legislation Act* 1984 (Vic). Reference may also be made to Part 1 of the Dictionary provisions of the *Evidence Act* 2008 (Vic). And I think a computer database would also be describable as "property" within the meaning of the Court's power to order inspection under rule 37. Having discovered the database, the plaintiff is entitled to inspection of it, there being no objection taken to inspection on the ground of any type of privilege or oppression or some other basis.

7. The plaintiff's solicitor has sworn a number of affidavits which, in substance, states the following facts. On 3 March 2010, the plaintiff filed a summons seeking particular discovery of, amongst other things, the second defendant's warranty administration and customer database in its "native electronic format." ADS eventually agreed, subject to confidentiality agreements, to allow for an inspection to take place of the second defendant's database but not of other files or information contained on the computer. It is apparent from that correspondence that the plaintiff was looking to inspect the native electronic format for the forensic purpose of establishing the dates and the circumstances in which the defendants caused information contained in the plaintiff's database to be used by them.

8. Timing is crucial because the plaintiff alleges that Kulik took the database in May or June 2008 whilst he and the other defendants were still working for the plaintiff and whilst, in the case of Kulik, being subject to fiduciary duties as a director. Particulars of that allegation have not been given. But as often is the case in these situations, the plaintiff is dependent upon the investigative processes of discovery to obtain facts that are covert or uniquely in the possession of its adversary. In general, such an unparticularised allegation will survive strike-out and legitimately attract the beneficial operation of discovery as long as there is some factual or evidentiary foundation to the

allegation. In this case, without going into details, the evidentiary foundation is largely inferential or circumstantial.

9. The arrangement made between the parties for an inspection of the database led to a consensual Court order being made on 18 March 2010 for the plaintiff's summons seeking further discovery to be dismissed with no order as to costs.

10. On 29 March 2010, the plaintiff's solicitor attended ADS' premises and inspected the ADS database. The evidence is that there is an extensive volume of information contained in the database. It is said there were 55,817 individual contracts processed from 23 April 2002 to 30 April 2008.

11. The defendants have given discovery of e-mails from certain car traders to ADS, and the plaintiff has made discovery of e-mails by which certain traders requested the plaintiff to provide them with lists of active contracts held by the plaintiffs. The plaintiff's solicitor swore a comprehensive affidavit on 3 June 2010 the details of which I shall not recite. In substance, it is apparent to me that she has undertaken a diligent examination of documents as discovered in hard form by the defendants, and has extracted other information from her inspection of the ADS database. The upshot is that there are grounds to believe that the ADS database contains information which was not included in the dealer e–mails and the database contains data in various categories which was not included in the data provided by dealers.

12. This may all be explicable or shown to be incorrect, but for discovery purposes, it is sufficient in my view to show there are grounds to further investigate the question whether the ADS database truly is attributable to information obtained from dealers after 30 June 2008 or from sources which the law would not regard as confidential, or, whether there is now an intensified basis for inferring that information was pre-existing and taken from the plaintiff.

13. The plaintiff now seeks another inspection of the ADS database by a forensic computer expert. For that purpose, the plaintiff has engaged a Mr Andrew David McLeish as an expert in forensic information technology. He has sworn an affidavit stating his experience and his credentials. He says that an inspection of the database would allow him to extract electronic reports of information contained on the database. He says he could then employ specialist software in order to compare information contained in those reports with information extracted from the plaintiff's database. Critically, he says for most comparisons, he would be able to give an expert opinion as to whether the data in the ADS database came directly from the plaintiff's database as opposed to other sources.

14. But the expert says he also requires access to the computer server on which the ADS database is located, and access to computers used by ADS (including desktop and laptop computers) networked to the ADS server. I shall abstain from the technical explanation he gives, but in essence, he swears that an inspection of the server as well as the networked computers would allow him to locate "link" files stored on the server. All of this, he says, will allow him to potentially identify when information was entered into the ADS database.

15. None of this evidence was challenged by ADS. But it refuses to grant another inspection of the database, or an inspection of the server and the networked computers. Hence by summons filed 21 May 2010, the plaintiff has sought the Court's orders for inspection of all those facilities.

16. ADS' resistance was two-fold.

17. First, Mr Ehrlich submits that the exchange of correspondence between solicitors for the inspection of the database which occurred on 29 March 2010 (to which I have already referred) constituted an agreement under which the plaintiff agreed to limit its inspection rights in this case to the database and no other files or information. He says the plaintiff is now seeking to "rewrite" the inspection agreement to permit forensic examinations that were expressly agreed to be outside its ambit. The submission is "there is no basis on which the plaintiff should be permitted to unilaterally vary the contractual inspection regime agreed between the parties pursuant to the inspection agreement." As I understood this argument, it was said there was a once and for all agreement about inspection.

18. I cannot accept that submission. I need say no more than the letters which gave rise to the earlier right of inspection cannot in any sense be regarded as "once and for all". Discovery and inspection are essential tools of justice to enable litigants, both plaintiff and defendant, to investigate facts ultimately to enable a Court to get to the truth of the matter. Agreements are frequently made in the course of litigation in order to avoid interlocutory skirmishes and added expense. In the context of civil procedure, such agreements usually as here involve an existing duty or obligation to comply with procedural steps anyway, and therefore lack consideration. Such agreements cannot be regarded as binding in a sense of precluding any additional steps being taken. The "agreement" was the product of an isolated summons and in any event, the previous arrangements did not extend to inspection of the computer server and the networked computers.

19. A court might intervene and prevent further discovery and inspection if the Court regards the additional pursuit over and above that which was "agreed" as being indicative of a misuse of court processes. But this is not the case here. To the contrary, it appears to me that the nature of the investigative exercise is such that it now does require the involvement of a computer expert to look into or "interrogate" the database and the server and the network computers to truly make the most of the discovery process. One cannot tell, but it may well result in the ascertainment of facts which corroborate the defendants' case.

20. I would rule that absent a form of procedural estoppel of a type for example that was argued in *Verwayen*[2], the plaintiff is not precluded from persevering with further applications for discovery or inspection.

21. The second argument in opposition was that the plaintiff was engaging in a fishing exercise. That term is so frequently used that it tends to be forgotten that it means making enquiries of something not pleaded in the hope that it can then be alleged. True it is, the plaintiff is under the handicap of a limited pleading in which it must, on instructions and on some evidentiary foundation, plead the wrongdoing. Beyond that, as I have said, it must rely upon the process of discovery to enlarge or investigate the facts of the wrongdoing as pleaded.

22. A good part of Mr Ehrlich's submission seemed to be dedicated to attacking the overall merits of the plaintiff's case. In many cases alleging a breach of confidence or use of trade secrets, there tends to be issues such as the availability of the alleged confidential information and the defendant's store of knowledge or memorised information in a particular trade. They all go to the merits of the case. They will not inform discovery obligations unless they can show that the plaintiff's case is so manifestly weak that discovery is being used for an improper purposes. I see no basis to reach that conclusion.

23. I accept that orders of the type sought by the plaintiff are naturally resisted in trade or commerce because they are, by their nature, invasive. No business is comfortable having a litigation adversary having access to its database, its server and its networked computers. There is the probability that the plaintiff's expert scrutineer will come across irrelevant or privileged or confidential information, and the inspection exercise will be disruptive to the second defendant's business. But there is no avoiding this. The discretion to be exercised in this case is beneficial in character. These sorts of difficulties were faced more acutely in *Sony Music Entertainment (Australia) Limited v University of Tasmania (No. 1)*[3] The most a court can do practically speaking is to put in place undertakings as to strict non-disclosure and confidentiality by the computer expert and directions requiring that the expert's work be done under the supervision of ADS and that any information extracted be also given to the defendants or their legal representatives. Another measure is to ensure the second defendant has an opportunity to seek legal advice and consult with its lawyers to see if there are claims of privilege or confidentiality for any documents or information as extracted by the expert or proposed to be extracted.

24. In my opinion, the application is not fishing. With protective measures in place, I think the plaintiff's request is legitimate. The investigative task has become unavoidably computer technical, and it requires expert investigation. I think it would be unjust to deny the plaintiff to inspect the data base again, and the server and the networked computers. Accordingly, I will grant the application.

25. At the suggestion of counsel, I will leave the parties to prepare some minutes of order and

a protective regime under which inspection should take place.

---

[1] [1935] 2 KB 80; [1935] All ER 75.
[2] *Commonwealth v Verwayen* [1990] HCA 39; (1990) 170 CLR 394.
[3] [2003] FCA 532; (2003) 129 FCR 472; 198 ALR 367; 57 IPR 77; [2003] AIPC 91-900.

APPEARANCES: For the plaintiff Automotive Dealer Administration Services Pty Ltd: Mr SR Senathirajah, counsel. Malleson Stephen Jaques, solicitors. For the second defendant: Mr PL Ehrlich, counsel. Katz Silver, solicitors.
