SECTION TWO

Read the following decision from the General Division of the Singapore High Court and answer the questions below.

ABC Pte. Ltd. v. Dan Dang

[2020] SGHC 1

The facts

1. The appellant operates a SaaS business for an application called Great Images. Great Images contains a product feature that uses the appellant's proprietary ML model called "PixMe" to select stock images that are appropriate for use in marketing materials. Over 200 customers in 10 countries across Asia subscribe to the Great Images application. A number of other materials surround and underlie the operation of Great Images.
2. The respondent joined the appellant in 2015. He found the appellant's PixMe ML model to be flawed and inaccurate. He decided to start a personal venture called "Project BetterMe" to improve on PixMe.
3. In 2017, Dan resigned from the appellant to work full time on Project BetterMe. He completed Project BetterMe in January 2018.
4. The appellant came across the BetterMe website around October 2018, which advertised a SaaS service similar to Great Images and substantially overlapped in scope with the geographical scope of the appellant's service. The appellant instructed Forensics Technology Pte Ltd ("Forensics") to conduct some investigations into BetterMe's activities.
5. Based on the forensics investigators, the appellant applied and obtained a court order to search and seize evidence at the respondent's residence. Following the seizure of equipment, Forensics discovered in a Dell server seized from the respondent, a folder titled "Testing" which contained, among other things, appellant's source codes. Forensics also discovered an email sent by the respondent to an IT consultant attaching the Greater Image source code.
6. The BetterMe application differs than the Great Images application in both architecture and design. The Distrct Court (the "Judge") examined the evidence and concluded that the BetterMe application could not have been copied from the Great Images application.
7. Several claims were asserted before the Judge that are not now in appeal. The only issue before the High Court concerns the claim for breach of confidence.

The decision below

8. The Judge noted that there are three well-established elements of a successful claim for breach of confidence, these being: (a) the information must possess the quality of confidentiality; (b) the information must have been imparted in circumstances importing an obligation of confidence; and (c) there must have been some unauthorised use of that information to the detriment of the party from whom the information originated. *Clearlab SG Pte Ltd v Ting Chong Chai and others* [2015] 1 SLR 163 ("*Clearlab*") at [64] citing *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 ("*Coco*") at 47.

9. The Judge considered that while the respondents owed the appellant obligations of confidence, the third limb could not be established because there had been no unauthorised use of its confidential information. Specifically, the Judge concluded that there was no evidence to show that any of the source codes or databases used by the BetterMe application constituted material reproduction of any portion of the Great Images application.

10. There is no dispute that the Dell server contained a copy of the source codes for Great Images or that the respondent viewed the source codes several times (based on the log retrieved from the Dell server).

11. The Judge held that whilst there might have been an intention to make use of its materials, the appellant still had to show that any reference to and review of these materials resulted in the creation of the respondents' own materials. Since there was no evidence that the respondent's own materials were developed using the information from the appellant (other than the undisputed fact that the respondent stored a copy of the Greater Images source code in its Dell server), there could not have been a breach of confidence.

Our decision

12. In recent years, the requirement that plaintiffs must show unauthorised use of their materials and resulting detriment has resulted in cases being dismissed often in circumstances where evidence to suggest the defendants wrongfully accessed or acquired confidential information exist, but it was much harder to demonstrate evidence of use or disclosure of information to others. It is time to consider whether the appellant's proposition, that the respondent's mere possession of and their act of referring to the confidential materials should be sufficient to complete the cause of action for breach of confidence.

13. The appellant's argument for a modern approach prompts the question of whether the current law of confidence is sufficiently broad to encompass the myriad of ways in which confidentiality might be undermined. There are three considerations this court should have in mind in answering this:

    1. What interests are sought to be protected by the cause of action?
    2. What is the nature of the threat to these interests?
    3. What are the remedies that ought to be made available where the relevant interests have been infringed?

The protected interests

14. The answer to the first question can be gleaned from the history of the law of confidence. In particular, *Prince Albert v Strange* (1849) 41 ER 1171 ("Prince Albert") involved Prince Albert seeking injunctive relief to prevent the exhibition and publication of a catalogue that described etchings by himself and Queen Victoria which the defendant had come about through a breach of trust. The request for injunction was granted on the reasoning that the unpublished etchings, being the "produce of labour", were a kind of property and the common law "provided for their security, at least before general publication by the writer's consent". There was some question over how the defendant got its hands on the etching and the court, in dicta, mentioned that if the defendant had obtained the etchings through a breach of trust,

there should be a legal avenue to stop the illegitimate use of the etchings on the theory of a breach of trust. The dicta was cited with approval and it is now held that an implied duty of confidentiality ought to exist that "b[inds] the conscience" of the defendant. *Saltman Engineering Co Ltd and others v Campbell Engineering Co Ltd* [1948] 65 RPC 203. So long as a defendant uses "confidential information directly or indirectly obtained from a plaintiff, without [their express or implied consent], he will be guilty of an infringement of the plaintiff's rights".

15. The use of the word "conscience", imports a broader, more fundamental, equity-based rationalisation for the protection of confidentiality. It places defendants under a duty; they are "bound" not to deal with confidential information in a manner that adversely affects their conscience. Depending on the circumstances under which the obligation arises, this duty may extend beyond refraining from acts of unauthorised use or disclosure.

Threat to the interest

16. A question that follows is whether there is a threat to this wrongful loss interest that warrants a more robust response by the law. The elements of breach of confidence set out in Coco explicitly protect the wrongful gain interest. Although there is often a degree of overlap, it may not always be the case that a defendant's conduct will affect both the wrongful gain and wrongful loss interests. This is exemplified by the facts of the present appeal. It was not proven that the respondents directly profited from their use of the appellant's confidential materials. However, this does not detract from the fact that the respondents knowingly acquired and circulated these materials without consent. Such conduct would have affected the respondents' conscience, invoking the wrongful loss interest, because it was known that the relevant materials had been subject to an obligation of confidence.

17. This illustrates a significant and unchecked threat to the wrongful loss interest. The vulnerability of this interest is magnified when considered against the backdrop of advances in modern technology. It is now significantly easier to access, copy and disseminate vast amounts of confidential information. This can be done almost instantaneously, often without the knowledge of plaintiffs. As in the present case, employees will often have access to large volumes of confidential business material for the purposes of their employment. If at some point they were to proceed to surreptitiously download this information for their personal use or to start a competing business, employers are likely to be none the wiser for a considerable time. It is nearly impossible in these situations to safeguard information from all potential wrongdoing. The fragility of such confidential information suggests the need for stronger measures to protect owners from loss. An undue focus on the wrongful gain interest to the exclusion or diminution of the wrongful loss interest, under the current law of confidence, would mean that those measures are lacking.

Availability of remedies

18. A final consideration relates to the adequacy of remedies in situations where the wrongful loss interest has been infringed.

19. Unfortunately, the wrongful loss arising from dissipation of the confidential character of the information does not always immediately translate into monetary terms or quantifiable detriment. The owner of the compromised information may know he has

suffered loss but may only be able to speculate as to how, for example, this will negatively affect his business or future operations. This means that even a simple claim for damages will not necessarily succeed. It is clear that there can be significant obstacles in the way of plaintiffs seeking to vindicate their wrongful loss interest, independently of their wrongful gain interest.

Modified approach

20. With these considerations in mind, we set out a modified approach that should be taken in relation to breach of confidence claims. Preserving the first two requirements in Coco, a court should consider whether the information in question "has the necessary quality of confidence about it" and if it has been "imparted in circumstances importing an obligation of confidence". An obligation of confidence will also be found where confidential information has been accessed or acquired without a plaintiff's knowledge or consent. Upon the satisfaction of these prerequisites, an action for breach of confidence is presumed. This might be displaced where, for instance, the defendant came across the information by accident or was unaware of its confidential nature or believed there to be a strong public interest in disclosing it. Whatever the explanation, the burden will be on the defendant to prove that its conscience was unaffected. In our view, this modified approach places greater focus on the wrongful loss interest without undermining the protection of the wrongful profit interest.
21. A shift in the burden of proof also addresses the practical difficulties faced by owners of confidential information in bringing a claim in confidence. As noted at [17], plaintiffs may often be unaware of the fact that someone has done an act inconsistent with their right of confidentiality. A potential breach could be discovered years after, placing them on an evidential back-foot. Defendants are comparatively better positioned to account for their suspected wrongdoing.

6. Before *ABC v. Dan Dang*, what would have been the elements of a claim for breach of confidence? (Please cite the case standing for your proposition.)

The three elements are:

(a) the information must possess the quality of confidentiality;

(b) the information must have been imparted in circumstances importing an obligation of confidence; and

(c) there must have been some unauthorised use of that information to the detriment of the party from whom the information originated.

Case is *Clearlab SG Pte Ltd v Ting Chong Chai and others* [2015] 1 SLR 163 ("*Clearlab*") at [64] citing *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 ("*Coco*") at 47.

7. Under the standard pre-ABC v. Dan Dang standard, why did the Judge rule that Dan Dang did not engage in a breach of confidence?

It was found by the Judge that the third element of requring an unauthorised use of the information to the detriment of the party from whom the information originated, was not met. There was no

evidence to show that any of the source codes or databases used by the BetterMe application constituted material reproduction of any portion of the Great Images application.

8. What interests does the law of confidence seek to protect?

Wrongful loss interest and wrongful gain interest.

Wrongful gain interest - where a defendant who is in possession of a plaintiff's confidential information gains an advantage and profited from the use of the plaintiff's confidential information.

Wrongful loss interest - when the defendant's conscience is affected by breach of obligation of confidence

9. For each of the interests you identified in Question 8, what threats will arise in the absence of a modification to the pre-*ABC v. Dan Dang* standard?

Wrongful loss interest - the advances in modern technology makes it easier for people to access, copy, and disseminate vast amounts of confgidential information. This increases the vulnerability of businesses to larger losses as it would be nearly impossible to safeguard information from all potential wrongdoing.

Wrongful gain interest - cases like the present might not affect both wrongful gain and wrongful lost. Thus if the court only focussed on wrongful gain interest, there would be cases that would be dismissed because this element is not proved.

10. How did the High Court's analysis in regard to the availability or lack availability of remedies weigh in favour of establishing a modified approach to determine whether a breach of confidence has occurred?

Wrongful loss arising from dissipation of the confidential character of the information does not always immediately translate into monetary terms or quantifiable detriment. The owner of the compromised information may know he has suffered loss but may only be able to speculate as to how, for example, this will negatively affect his business or future operations. Due to this uncertainty, simple claims for damages will not necessary succeed. Thus the modified approach would aim to overcome this challenge.

BETTER ANSWER: The court believed that the existing *Coco* framework over-emphasized the need to establish a wrongful gain, which, in turn, meant that complainants who were mostly affected because they suffered a wrongful loss could not receive adequate remedies for the wrong that they have suffered. This circumstance has arisen because frequently, the damages that a complainant suffers from the dissipation of the confidential character of the information will not immediately translate into quantifiable damage. Yet, at the same time, the complainant frequently must file suit as soon as possible to preserve the complainant's interest and prevent further harm due to the continued dissipation or breach of confidence, even though it cannot quantify its potential or even actual losses or the adverse effects on its future business.

Therefore, the *Coco* framework should be modified so that the interest in protecting complainants from suffering wrongful losses in a breach of confidence claim can be adequately protected.

11. Identify the *rationes decidendi* of *ABC v. Dan Dang*.

An action of breach of confidence would be presumed when the first two requirements in Coco are met where the information in question “has the necessary quality of confidence about it” and if it has been “imparted in circumstances importing an obligation of confidence", and that the confiodential information had been accessed or acquired without the plaintiff's knowledge or consent. The burden of proof will be on the defendant to prove that its conscience was unaffected by the circumstance.

12. Based on *ABC v. Dan Dang*, explain whether ABC should succeed in its claim for breach of confidence and why. If you believe that there is a need to conduct further fact-finding to determine whether or not ABC should succeed, describe the issues that merit further fact-finding and explain how these issues will affect the ultimate conclusion.

ABC should succeed in its claim. Firstly, it is clear that materials found in the possession of the respondent were confidential in nature and formed a key part the appellant's business. The court also found that the materials were subject to an obligation of confidence. The acquiring and referencing to the materials thus constitute a breach of duty of confidence on the part of the respondent. These thus fulfil the first two prerequisites of Coco. The issue stands whereby Coco's approach would not be enough to protect the appellants wrongful loss interest and as such, the modified approach is required. This approach requires the respondent to prove that his conscience was not affected by unaffected. If the respondent fails to prove that his conscience was unaffected by the circumstances (e.g.l he found the materials by accident), the respondent can then be found to have acted in breach of confidence.

13. In 2021, a similar case involving a different company and a different employee was considered by the Court of Appeals. The case was XYZ v. Pretty Pun. The Court of Appeals deciding for XYZ v. Pretty Pun is bound by the ABC v. Dan Dang decision. True or false?

False

SECTION THREE

Rahim is 75-years-old, is single and has no kids. Because of Covid, Rahim set up internet banking to settle his living expenses from his home so that he could avoid going to the bank and risking infection. However, Rahim has not gotten the bank of digital banking and relies heavily on his younger relatives to help him gain access to his bank account. His grand-nieces and nephews help him from time to time by using TeamViewer (remote access and remote control software) to gain control of his laptop and walk him through the internet banking process.

Aaron is Rahim’s grand-nephew. Aaron owes his bookies some money and he’s desperate to settle his debt before things turn worse. He decided to borrow some money from Rahim. He calls Rahim up and Rahim said that he could lend Aaron $200 but he didn’t know how to transfer the money to Aaron. Following the usual protocol established between Rahim and Aaron, they fire up their respective laptops and Rahim gave Aaron permission to use TeamViewer to gain access to Rahim’s device. Using TeamViewer, Aaron clicks on the browser installed on Rahim’s laptop and accesses the bank’s internet website. Following Aaron’s instructions, Rahim entered his username and password to log into his bank account. Through TeamViewer, Aaron then takes control and clicks on the relevant links on Rahim’s browser to authorize a bank transfer for $200 to Aaron’s own account. Thinking that the transaction had ended, Rahim walked away from his laptop to make himself a cup of coffee.

Unknown to Rahim, Aaron's TeamViewer access was not terminated nor did Aaron help Rahim log out of his bank account after the transaction was over. On the contrary, Aaron lurked within Rahim's bank account and decided to transfer another $1,000 to himself. He was convinced that he would win the lottery draw that night and he would be able to pay back Rahim the principal with interest. Over the last year, Aaron has done this many times and transferred over $20,000 to his own account. However, he has also won the lottery many times and have been able to pay Rahim back any money he took with a very generous interest. In fact, Aaron has deposited into Rahim's account over $25,000 without Rahim realizing what was going on.

Analyze whether Aaron has committed any crime under Sections 3 or 4 of the Computer Misuse Act. Make use of the definitions given to you.

You must identify the elements of the crimes and explain whether each element is met or not met using the facts given to you. Avoid making assumptions - the facts given to you are complete. Do you assume facts to simplify your analysis. However, if there are critical investigations that must be conducted to establish whether a crime has been committed, outline the investigations you need to conduct and explain why the answers to these investigations are critical to your analysis.

Facts of case: Aaron and Rahim use Teamviewer to grant Aaron remote access. Rahim logs in to bank account and Aaron uses that authentication to carry out money transfers. He did secret money transfers repeatedly . He deposited money back with $5000 interest without Rahim realising what was going on.

s 3(1) - Unauthorised access to computer material - To prove that Aaron has commited an offence under s 3(1), we need to prove that Aaron had knowingly caused a computer to perform a function to secure access without authority to a program or data held in a computer. Here, the two key elements to prove are the firstly, that Aaron had caused a computer to perform a function to secure access to a program or data, and secondly, he knowingly did so without authority.

In this case, the access in question refers to Aaron's access of Rahim's bank account via the bank's internet website. From s 2(3)(b), a person is said to have secured access to a program if he uses it by causing the computer to run a function which is itself a function of the program. In this case, Aaron has caused Rahim's computer (via Teamviewer) to run a function of the money transfers on the bank's website ("the program"),

With reference to s 2(5), access by a person is unauthorised if he is not himself entitled to control access of the kind in question and does not have consent to access from any person who is so entitled. From *Lim Siong Khee v Public Prosecutor [2001] SGHC 69*, it was found that there was a general understanding in a relationship of consumer and industry, the account holder is entitled to access the data and is responsible for control of access. Applying this to the present case, Rahim is thus the person who provides the consent to access to his bank account. Despite Rahim allowing Aaron to use his bank account, it must be noted that that consent was given for the purpose of Aaron transferring the money as discussed and any extra transfers beyond the discussed were not authorised by Rahim. We also then need to prove that he was aware that his actions were unauthorised. This can be contributed by his conduct of repeating the act several times, while keeping Rahim oblivious of what has been occuring. This conscious steps taken to hide his unauthorised acts largely resemble the case of *Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin [1993]* in which the respondent made active steps to conceal his acts by erasing his traces. The judge found that the courts would have to apply principles of strict liability in such cases. In the present case, the repeated same offences that required Aaron to make transfers conciously without the knowledge of Rahim fulfills the mens rea element required in s 3(1).

s 4(1) - Access with intent to commit or facilitate commission of offence - To prove that Aaron has committed an offence under s 4(1), we need to prove Aaron had caused a computer to perform a function for the purpose of securing access to any program/data in any computer with intent to commit an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years. It should be noted that according to s 4(4)(a), it is immaterial whether the access is authorised or not unauthorised. The two elements to prove here are firstly, that Aaron caused a computer to perform a function for the purpose of securing access, and secondly, did so with the intent to commit a crime within the stated scope. The first element has been proved in the proof above for s 3(1) where Aaron, had caused Rahim's computer to secure access to Rahim's bank account. The second element can be fulfilled by the Aaron's act of allegedly committing theft by the transfer of money without Rahim's knowledge. However, this charge of theft has to be investigated further according to the Penal Code. This would include proving that the temporary removal of Rahim's money from his account, which was eventually returned, would sufficiently constitute theft. Should the charge of theft be held, the elements of s 4(1) would then be met and Aaron would thus be guilty.