Nicholas Andreatidis QC (NA)

Welcome, everybody to our panel discussion on the High Court decision of *Glencore v Commissioner of Taxation*. What we're going to discuss in our panel are the risks that are faced by clients in protecting privileged material in a technological age, what they can do to minimise those risks, and what steps or actions they should take - according to the panel - post a breach, should that occur. And given what we're seeing on Twitter regularly it is something very frequent.

I'd like to introduce you all to our panellists. I will start with Brendan Read who joins us from KordaMentha. Brendan is a person who has had more than 15 years' experience as a computer technology forensic expert, both in the private and commercial areas. He is frequently retained by both public and private entities to assist them in technologically related forensic matters.

If I could then introduce James Green. James is one of the juniors here at Level Twenty Seven. James is regularly involved in large, complex commercial matters. Prior to joining us at Level Twenty Seven, James worked for an international law firm and a national law firm both here in Australia and in the UK.

And finally, Sophie Gibson who is also one of the barristers here at Level Twenty Seven. Sophie, similarly to James, is frequently, briefed in large complex commercial disputes. Prior to joining us at Level Twenty Seven Sophie was Justice Keane's Associate in the High Court. And, prior to joining us, was at an international law firm.

I should mention that James was also Chief Justice Keane's Associate, as His Honour then was in the Federal Court.

So, as I said, we're going to be talking about *Glencore*. And I'll invite Sophia to just give a very brief overview of the case.

GLENCORE INTERNATIONAL AG V COMMISSIONER OF TAXATION – CASE BACKGROUND

Sophie Gibson (SG)

Thanks, Nic.

I'm sure by now everybody is well aware of the facts of the *Glencore* decision but in summary, Glencore sought legal advice from a law firm about the restructure of a number of its Australian entities. The law firm's databases were subsequently hacked, and the Glencore advices were amongst a large number of papers which were sent by the hackers to a group of journalists. These documents came to be known as the Paradise Papers. The existence and content of the Paradise Papers received global media coverage. The ATO obtained copies of the papers, and the Glencore advices were relevant to the calculation of Glencore's Australian tax liabilities.

Glencore sought injunctive relief from the High Court restraining the ATO from using the Glencore advices and requiring their return.

The relief was claimed solely on the basis that legal professional privilege was attached to the documents. The ATO demurred to the statement of claim principally on the ground that no cause of action was disclosed.

Glencore accepted that to succeed in obtaining an injunction it was necessary to establish that they had an actionable legal right. Glencore's core argument was that LPP has been described in previous decisions of the High Court as a fundamental common law right, and that no decision of the High Court had expressly held that privilege operates on this immunity. Glencore contended that it is unsound for legal professional privilege to be recognised as a fundamental right, but for confidentiality to provide the only basis for its enforcement. It was argued that there's a gap in the law if an injunction will be granted on the basis that documents are confidential, but not on the basis that they are privileged.

The ATO ran two arguments. The first was that LPP was not an actionable right and that Glencore had disclosed no cause of action sufficient to found an injunction. And the second was at section [166] of the *Income Tax Assessment Act* it entitled the ATO to retain and use any document in its possession for the purposes of discharging its statutory obligations.

In the event, the Court refused to grant the injunction. In a joint judgment, the Court held that Glencore had not established a cause of action. Their Honours held that while the documents were clearly privileged, LPP is not a right. It's an immunity from the exercise of legal power or control compelling the disclosure of certain communication. They held that privilege is a shield rather than a sword. It does not give rise to an action on the case of damages and is not enough to grant an injunction.

The Court confirmed that equity will restrain and apprehend a breach of confidential information and will do so with respect to documents which are the subject of LPP and which are confidential. However, Glencore did not run an action for breach of confidence. The Court made observations that it may have had difficulties in doing so primarily because the Glencore documents were in the public domain, and there was no allegation made about the Commission's conduct or knowledge. On this premises, the court found that it was not necessary to consider the ATO section [166] argument and Glencore's case was dismissed.

CYBER SECURITY THREATS TO ORGANISATIONS

NA

Brendan, could you just give us a rundown on the types of risks that are being faced by businesses these days?

Brendan Read (BR)

Sure Nic. So obviously, I'll start by just saying with this COVID-19 pandemic and the move to this remote working model, everyone who's listening to this recording now would be very well aware of how much businesses are reliant on technology for just day to day operational means. That in itself just poses new risks as well to business. But in terms of when we're talking about internal threats, what I've got listed there, the first two are employees and there's no sort of mistake as to why employees are listed first, because they are the biggest risk to the business. Disgruntled employees can be a major concern for a business. There was a recent matter that involved Landmark White, where an IT consultant had come into the business, and decided that he would take a whole lot of sensitive, confidential information, and then put that on the internet for other people to view. As to the reasons why that particular person did that is totally unknown.

The other risk is just IT administrators. You have to remember that these particular individuals have the keys to the kingdom in terms of the data for these organisations. You need to be really mindful of how these particular individuals are monitored and managed, because they have the ability to impact the business overnight.

Then you've got the careless employees. Employees that are receiving emails, and there might be a phishing email that would look legitimate and just purely from a lack of education and training, might click on a link that opens a backdoor for a hacker to come in and steal a whole lot of corporate information.

The other side of it that I see in terms of those inside threats is just the way that businesses and organisations manage their confidential and sensitive information. There is just no thought or procedures in place to how they actually lock and secure confidential, privileged information for the business. And that may mean something as simple as how they make copies of that information. They may keep that information in a secure area on a file server, but they're not aware of the other copies of that information that are floating around on external hard drives or USB thumb drives.

NA

And of course, that risk is increased by the fact that people are liberal when it comes to cell phones, tablets, all sorts of cloud services. Things that we don't necessarily turn our minds to which can escalate these things.

BR

Correct. With cloud based technologies, it's so simple to upload a document to a particular application and that's instantly replicated across the world to other servers. So yeah, it is a real risk.

And in terms of those external threats, obviously hackers are seeing these organisations as a massive target, and a revenue stream for them. No one is immune, it could be a corporate entity, it could be a law firm. There was a recent law firm in New York that was hit with a massive ransomware attack. Servers were locked down and they were hit with a request for a ransom for a payment in the millions of dollars, otherwise that information would be uploaded and shared with the world.

NA

I think the three of you will recall in one of the sessions we did talking about this case that one of the audience members recounted the story to us where he was at a seminar or a conference where someone like Brendan presented and there were a lot of non-believers in the audience. The presenter pulled out his mobile phone and tapped a few things and said "Is there a Margaret here?" Someone called Margaret put their hand up. "You're on Facebook watching this right now aren't you?" Everyone was freaking out that within a matter of seconds this guy was hacking everybody's phones. So hackers are armed with very powerful tools.

BR

That's right. And even just for any individual that wants to do this sort of behaviour can get access to these tools and use them in a malicious way.

Obviously, just on that last point there, hackers are providing that information to journalists and other investigators causing another risk to business.

GLENCORE - TAKEAWAYS

NA

Now James, what is the takeaway for clients from Glencore with this type of risk?

James Green (JG)

Well, the key takeaway, in my view, is that the decision in Glencore doesn't make any radical change to the law of legal professional privilege, but simply confirms that legal professional privilege is a common law right, which first does not of itself ground a cause of action. Second, it gives rise to no rights which can be breached. The High Court confirmed that privilege is simply an immunity from compulsory production, under court order disclosure processes, and nothing more. In this respect, the case is entirely consistent with the pre-existing legal framework in which legal professional privilege was considered. Very similar principles were expressed by the Victorian Court of Appeal in 2007 in *Cowell v British American Tobacco Australia Services Limited* at paragraphs [32] to [33].

Glencore's argument rested, as Sophie has mentioned, on the basis that these principles leave a gap in the protection afforded to parties over privileged material. The gap, however, is quite narrow, and only arises when the following two circumstances exist. First, the proceedings

between the relevant parties are not on foot, and second, where the material over which privilege is sought to be asserted has entered the public domain. In relation to the first, as Sophie has mentioned, the Commissioner in Glencore had not started any proceedings against Glencore to recover an amount of tax or to enforce any rights or remedies at all. There was accordingly no ability to resist production because production was not sought pursuant to a court order. There was also no basis to object to admissibility of documents because the documents were not being tendered.

The fact that proceedings were not on foot also meant that there was no possibility to have recourse to the remedies which the High Court set out in *Expense Reduction v Armstrong*. The High Court in Glencore confirmed that expense reduction does not stand for any broader proposition which would allow the privilege to be asserted in order for relief in the nature of an injunction to be granted.

In relation to the second circumstance that material had entered the public domain, Glencore argued this meant there was no ability for it to seek to recover these documents or restrain their use in an action for breach of confidence. And we'll come back to this point later. But essentially, the High Court did not think that this limitation, if it was a limitation, justified expanding the traditional basis upon which a party could be restrained from using privileged documents.

So the main takeaways are that the High Court has not expanded the remedies available to a party to restrain the use of documents which are subject to legal professional privilege. Secondly, to the extent that there is a remedy, that remedy is based in an equitable action for breach of confidence.

DOCUMENT PRODUCTION & REGULATOR POWERS

NA

Sophie, will you please take us through the powers of regulators to compel production.

SG

Regulators have broad investigative and information gathering powers. However, the High Court has held that absent clear legislative intent to the contrary there is no obligation to provide regulators with privileged communication. That is because LPP is a fundamental common law immunity. Nevertheless, in some circumstances, it's advantageous for a party to disclose privileged documents to a regulator. For example, waiving privileges is sometimes a condition of cooperative arrangements or deferred prosecution agreements. Limited use disclosure to regulators has become increasingly common practice. When making the decision to voluntarily disclose privileged documents to a regulator, it should be kept in mind that disclosure can amount to waiver. This should be kept in mind even if there are no proceedings currently on foot. Parties should consider whether proceedings are likely to arise in the future, even outside the jurisdiction. *Cantor v Audi Australia* was a class action concerning illegal

devices which had been installed in Volkswagen and Audi vehicles that were designed to cheat emissions testing. Australian class action plaintiffs sought access to documents, including legal advice, which had been exchanged between the Volkswagen and a German regulator. The Federal Court ultimately held that the disclosure of the privileged documents to the regulator did not amount to a waiver but noted that whether limited disclosure of LPP documents to a regulator will amount to a waiver, but that will turn on the facts and circumstances of the case.

NA
Thank you Sophie.

Brendan, would you mind sharing some insights into the type of regulatory activity you see where regulators exert statutory control.

BR
Sure Nic. On a number of occasions, with the regulator, in terms of execution of search warrants. One of the things that businesses need to be mindful of is that when we are entering a premises, we're using specialist forensic tools. Those tools are designed to be able to identify and locate information that the standard user wouldn't normally see. The things that we would be looking for is might be deleted data, data that may be sitting on an old hard drive that they weren't even aware still contained information on mobile devices. There may have previously been specific messages that were existing on those devices that the user believed were deleted, and they may actually be recovered, and then use in or fit in terms of what the warrant is seeking. I suppose the focus is just to be mindful that even if they can't see the data, even if they're IT people are saying that data on those drives is fine it really comes down to someone who's skilled with forensics, and using those forensic tools, to be able to give me an idea of whether there is actually information there.

CYBER SECURITY TIPS TO AVOID DATA HACKING

NA
Still with you Brendan, any tips about what people in the business community should do pre-data breach to try and minimise the risks we've talked about?

BR
Coming back to those risks that we identified, those internal risks. The internal threats in particular, the Australian Cybersecurity Centre, the ASD, they released an essential eight tips that people should do. If organisations turn their mind to those essential eight and are implementing those within their organisation, they're going to be in a very good position to pretty much protect themselves from a majority of those sorts of risks that are coming in, whether they're from a disgruntled employee to a careless employee. Those things such as patching or updating your operating system, as well as the applications themselves, if there are new versions that are

coming out, thinking about two factor authentication, and making sure that you're using that where possible, ensuring that there are backups happening on a daily basis. And just looking at what sort of other applications you can put controls around to ensure that it's just not a free for all in terms of any application running on a corporate network.

The next step I'd be looking at is in terms of we're talking about is password versus encryption. Encryption is something that I would definitely be thinking that most businesses need to be utilising where possible. That could be encryption incorporated into an actual desktop or laptop machine. So if I use Microsoft Windows as an example, BitLocker is now included and enabled by default on those types of devices in that operating system. And that should be something that that is used as a standard. And with encryption, it is a much stronger method for protecting the data that is on those devices, as opposed to a password, which can be potentially broken quite easily. Access to the information gained by an individual encryption is a lot stronger and very difficult to break. It's highly recommended that they use those. Then also just some strict protocols regarding around that confidential and privileged information. There is some sort of lockdown or steps in place to manage those highly sensitive documents.

NA
In terms of digital storage, is that the type of thing you're talking about? That is, the location of the storage?

BR
Correct. Yeah. So where it's located, who has access to it, ensuring that only the people that need to have access to that information do.

NA
That goes back to what we discussed earlier. If it's on someone's telephone, it doesn't matter what the protocol says, if it's on someone's phone, you can access it that way.

BR
Correct, because there's multiple copies, potentially, yes.

MATTER MANAGEMENT TIPS & DOCUMENT SHARING

NA
Any practical tips?

SG
Sure. In terms of practice management for our viewers, we would suggest that you watermark your documents as confidential and privileged so that if they are hacked the party receiving them is on notice.

Limit the reproduction of sensitive documents. If you can, consider circulating hard copies of documents that might be sensitive.

Then if any privileged material is provided to a regulator, ensure that it's made clear *in writing*, that the limited disclosure of that material is made solely for the purpose of the regulator performing its functions and that no broader waiver of privilege is intended. It may be worth suggesting to your clients to have a limited disclosure agreement prepared and on file.

Then prior to the provision of any privileged documents to a regulator attempt to reach agreement that your communications are to remain confidential and that the privileged material will not be provided or disclosed in whole or in part to third parties.

WHAT TO DO POST DATA BREACH – IT TIPS

NA

Now, this is the bit that sends shivers up and down my spine whenever we get Brendan to speak about this. Post breach, what can be done?

BR

Obviously you want to try and get the right specialists in to actually help the organisation recovering from a breach. The thing to remember is that even though some information may already have been removed or exfiltrated from the organisation that risk may still be present. You need to take steps to ensure that that risk is locked down and however the individuals were able to gain entry that that is removed.

NA

I've heard you recounting a story where a client, or client had a hacker, call someone in internally, and they thought they'd captured them, but for months or a considerable period of time, the hackers were working in the background.

BR

Yeah, correct. This particular organisation was initially hacked into and then there was a ransomware infected on one of the servers and they sent a ransomware notice saying that you need to pay us some money. So what the actual IT administrator did then was he just went to the backup system, and then revert it from a backup and then restored it to a previous date in time. But what they didn't do was take those steps to ensure that that risk was removed. So all they did was put it back to a previous state of the network. The hackers still had access and were able to come straight back in. But in this second instance, they took their time, so ensured they actually identified where the offsite backups were. Went into those first, deleted all those backups, then came back into the main corporate network and then encrypted everything again, and then sent the same demand across.

WHAT TO DO POST DATA BREACH – LEGAL RECOURSE

NA

Now, James, you get a phone call from one of your solicitors panicking, saying that one of their biggest corporate clients has just been hacked by an unsavoury protest group. What do you do?

JG

Well, as discussed earlier, the only practical remedy which was available to Glencore was an action for breach of confidence combined with injunctions seeking to restrain the use of documents and potentially to compel their return. As we've mentioned, Glencore's case rested upon the proposition that because the Paradise Papers had been made public, there was no possibility of sustaining an action for breach of confidence or sustaining an action for an injunction because the documents over which Glencore was claiming privilege had been disclosed to the whole world. Accordingly, the protections for legal professional privilege needed to be expanded. Although this was a necessary element of Glencore's argument, it was ultimately not accepted by the High Court. The High Court observed in paragraph [37] of its judgment, that the plaintiff's submission that common law courts elsewhere have granted injunctions on a basis other than breach of confidential information is incorrect. The plaintiff referred in this regard to *Lachaux v Independent Print Ltd*, and *Wee Shuo Woon v HT SRL*. Each of these cases concerned whether there was a loss of the necessary quality of confidentiality to found an injunction. Those two cases are worth looking at in some detail, both because of have relevance to the issues with which we are concerned but also of course because the High Court specifically referred to them.

The first is *Wee Shuo Woon v HT SRL*, a 2017 decision of the Singaporean Court of Appeal. Mr. Lee was the defendant in an action brought by HT, which ironically enough stands for Hacking Team. HT was an Italian company specialising in security technology, which is supplied to law enforcement and intelligence agencies. Mr. Wee was HT's security specialist and quit to work for a competitor. HT sued Mr. Wee for breach of duties owed to his former employer and Mr. Wee counterclaimed for unpaid wages. After this dispute had arisen HT's computer systems were hacked, and approximately 500 gigabytes of data was extracted and uploaded to WikiLeaks. In those documents were emails between HT and its lawyers, which included legal advice, information and materials relevant to the action which HT had against former employee Mr. Wee. Mr. Wee accessed Wikileaks and found those emails and applied to strike out the proceedings against him on the basis that the email showed the cause of action was an abuse of process. HT filed a proceeding against Mr. Wee, which requested an injunction to restrain Mr Wee from further use of the emails and all correspondence between HT and its solicitors. The parties agreed that the emails were covered by a legal professional privilege and they also agreed that the emails were originally confidential in nature.

The matter was heard at first instance by an assistant registrar, who determined that the fact that the documents were publicly accessible, even on the internet, would not necessarily stifle an action in confidence. The assistant registrar went on to say that in each case the court was concerned with whether the degree of accessibility to the information was such that in all the circumstances, it would not be just to require the party against whom a duty of confidentiality is asserted to treat that information as confidential.

The Singapore Court of Appeal effectively endorsed this reasoning. The Court stated that where a document, in respect of which a party asserts privilege, is already in the possession of its opponent the issue is no longer one of withholding disclosure. The question is one of admissibility rather than privilege, and that nevertheless, equity may grant injunctions to prevent the unauthorised use in court proceedings of information contained in privileged material on the basis that the documents remain confidential.

The question was therefore whether the fact that the emails had been published on the internet meant that they were in the public domain. In this regard, the Court held that although the fact that documents had entered the public domain would limit the availability of equitable relief, it was not a principle to be applied mechanistically, it was a general and not an absolute rule. The question for the Court in each case is whether the degree of accessibility of information is such that in all the circumstances it would not be just to require the party to treat the documents as confidential. It was important to focus not only on the extent to which the information question had become accessible but also on the extent to which it had in fact been accessed by the general public. The Court noted that potential abstract accessibility is vastly different from access in fact.

Applying these principles of facts at hand, the Court found that the emails which had been uploaded to WikiLeaks constituted a minute fraction of the approximately 500 gigabytes of data that had been stolen. The Court found that it was highly probable that few, if any, knew of the existence of the emails or the presence of the hacked material, and fewer still would have had the interest or inclination to undertake the task of scouring through that data for the relevant emails. At paragraph [43] the Court made its key finding that the Court was of the view that the emails and the contents were not public knowledge or in the public domain, although they were theoretically accessible to anyone during an intense search on WikiLeaks. The emails thus retained their confidential status and could still claim the protection of the law of confidence.

The other case, which the High Court referred to was *Lachaux v Independent Print Ltd*, a 2017 decision in the English Court of Appeal. This case arose out of an acrimonious divorce between a French citizen living in Dubai and a British citizen. The husband applied for divorce in Dubai and shortly afterward various articles appeared in the UK media which had been based on information supplied by the wife. The husband commenced libel proceedings against the wife

and against the defendant who had printed these articles, Independent Print Limited, alleging that the articles were defamatory.

In the course of what were a multitude of interlocutory and related proceedings, the husband became aware that the wife had provided Independent Print with copies of legal advice obtained by him in relation to the divorce. The wife had obtained access to these documents from a computer to which both she and her husband had access. Although the wife had access to the documents they had not been published.

Similarly to the case in *Wee*, the wife claimed that legal professional privilege couldn't apply because the documents showed that the husband had been dishonest and engaged the court in an abuse of process. This was rejected at first instance, and the court of first instance restrained the use of the documents. On appeal, the court agreed. Unlike the decision in *Wee*, there was relatively little discussion of the extent of the obligation of confidence and there was no suggestion *Lachaux* that the documents have become public or were publicly put on the internet. Nevertheless, the court did recognise the documents remained confidential and said that even if the wife had access to the documents as between her and her husband that did not entitle her to unilaterally pass such documents on to third parties such as the defendant Independent Print Ltd.

Although it seems counterintuitive, there are actually quite a few cases in which courts have restrained publication of material on the basis that that material remains confidential, even after that material has been disclosed to some extent. There is a useful summary of the principles by Justice Ward in *Brand v Monks*, a 2009 decision of the New South Wales Supreme Court, paragraphs [182-184]. The key message is that the most likely remedies and action for breach of confidence and to consider that as a remedy, even if there may have been some potential or theoretical disclosure of the information.

NA

If you watch the actual appeal argument, we all agree that it's something worth watching, because it gives a bit of a measure of the potential appetite that the court might have for arguments that rely on confidentiality in this context. The interaction between the Justices and Senior Counsel for Glencore was very enlightening and very interesting. The reasons obviously reflect the outcome, but that interaction, I think is actually quite an informative discussion. It's something we recommend to you viewers. You need watch only forty-five, fifty minutes or so. It's very, very interesting for a couple of reasons. One, the interaction, and secondly, Senior Counsel for Glencore is Hugh Jackman's brother. He must be one of the coolest people at the Bar. It's something that we recommend to you to watch.

Now Sophie, are there any other protective mechanisms that can be put in place to assist in protecting a client?

SG

Yes, there are. The traditional common law position is that the manner in which a party has obtained evidence is not a ground to reject its admission into evidence. And this approach dates all the way back to the 1800s. There's a decision in *R v Leatham* in which His Honour Compton observed, it matters not how you get it - even if you steal it it would be admissible in evidence. The traditional view is also that LPP is an immunity and not a rule of admissibility.

However, the law has thankfully developed and in modern day Australia there are both statutory and common law protections regarding the admissibility of improperly obtained or privileged documents. The *Commonwealth Evidence Act* contains a number of protections. section 118 provides that evidence is not to be adduced if on objection the court finds that adducing the evidence would result in a disclosure of a confidential communication made between a client and the lawyer for the dominant purpose of legal advice, and section 119 applies the same protection to litigation privilege.

There are also protections in section 138 of the *Evidence Act* regarding improperly obtained or illegally obtained evidence. Section 138 states that evidence obtained in consequence of an impropriety is not to be admitted unless the desirability of admitting that evidence outweighs the undesirability of admitting the evidence in lieu of the way in which it has been obtained. Presumably hacked documents sought to be adduced would be caught by this section.

The *Queensland Evidence Act* does not contain the same protections. However, in the decision of *Bunning v Cross* the High Court held that a court has the discretion to exclude evidence improperly obtained where unfairness to the defendant outweighs the public interest in enforcement of the law and obtaining evidence to aid that enforcement.

In Glencore, while there were no proceedings on foot, the Court did not need to answer the question of whether the Paradise Papers would be admissible in proceedings against Glencore. However, they did make reference to the decision in *Bunning v Cross*. So in the event that you or your clients have had documents hacked and you're involved in litigation in which the other side foreshadows that they intend to tender those documents you should object and then request that the judge hold a *voir dire* for a ruling on whether the documents are admissible prior to the hearing.

CONCLUSION – PURSUING THE CONFIDENTIALITY ARGUMENT

NA

Finally, a question for both Sophie and James. In terms of the scenario I put to James earlier, would you give it a go on the confidentiality argument? Or would you just wait and see what happens in the course of the arguments?

JG

I think it depends on the facts of each case. Generally, I think it's important to be proactive and if there is a case to be made that the documents still maintain confidentiality then I think it's important to attempt at least to bring an action to restrain the use of those documents on equitable principles.

SG

I agree. If you sit on your hands and don't take any steps to enforce your rights in respect to that you might have a harder job down the road trying to object to their admissibility and proceeding.

NA

Yeah, we don't think this is the final chapter.

Well viewers, thank you very much for joining us. Brendan, Sophie, James, thank you very much for your time.

Keep safe.