IN THE HIGH COURT OF NEW ZEALAND
WELLINGTON REGISTRY

I TE KŌTI MATUA O AOTEAROA
TE WHANGANUI-A-TARA ROHE

CIV-2021-485-379
[2021] NZHC 2002

BETWEEN	WAIKATO DISTRICT HEALTH BOARD Plaintiff
AND	RADIO NEW ZEALAND LIMITED First Defendant
	UNKNOWN DEFENDANTS Second Defendants

Hearing by way of teleconference: 3 August 2021

Counsel: J Baigent for Plaintiff
R Stewart for First Defendant
No appearance for Second Defendants

Judgment: 4 August 2021

JUDGMENT OF CHURCHMAN J

Background

[1] On 18 May 2021, the plaintiff, Waikato District Health Board (WDHB), was subject to a cyber-attack by unknown criminals. The attack resulted in data belonging to WDHB being illegally obtained by persons unknown (the Stolen Dataset).

[2] The Stolen Dataset contains personal patient health information, employee information and commercially sensitive operational information. Much of the information is private and confidential and, particularly the personal health information, is of a sensitive nature.

[3] As a result of the cyber-attack almost all of WDHB's systems became encrypted with ransomware, a type of malicious software that prevented WDHB from accessing its systems and digital network.

[4] The perpetrators of the cyber-attack attempted to extort money from WDHB by way of a ransom demand.

[5] WDHB did not comply with the extortionists' demands.

[6] On or around 26 May 2021, WDHB became aware that a media organisation had received and opened a link from an unknown third party which provided access to screen shots of multiple documents that appeared to be part of the Stolen Dataset.

[7] Around mid-June 2021, WDHB learnt that the Stolen Dataset had been leaked and a link to WDHB's data had been made available for download in an online forum on the dark web.

[8] Through appropriate agencies, WDHB attempted to delete the Stolen Dataset from the dark web and to prevent its dissemination through other media channels.

[9] WDHB discovered that the entire Stolen Dataset was on the dark web.

[10] In late June 2021, WDHB discovered that the ransomware link site address on the dark web had been shared on Twitter on 28 June 2021. That Twitter account was subsequently "locked".

[11] On 28 July 2021, WDHB was advised by the New Zealand Police that the dark website containing the link to the Stolen Dataset was no longer available on the dark web.

[12] The knowledge that criminal extortionists have possession of their sensitive personal information and are attempting to obtain financial gain from it by attempting to get media organisations to publish it has caused extreme distress to WDHB staff and patients.

Radio New Zealand's actions

[13] By email dated 3.58pm on Tuesday 27 July 2021, an RNZ journalist contacted WDHB and advised:

(a) it intended publishing a story based on a child patient of WDHB;

(b) the story was sourced from documents posted online by the cyber-attackers who had hacked the WDHB;

(c) the email asked for responses to a number of questions including a question seeking further personal information about the child; and

(d) it required a response by 4pm the following day.

[14] On 28 July 2021 at 9.54am, well before the 24-hour deadline given, WDHB received a call from the RNZ reporter wanting a response to the questions. WDHB indicated that it was still investigating the matter.

[15] At 3.20pm on 28 July 2021, WDHB contacted RNZ to advise that a response would be provided in writing but was unlikely to be available by the 4pm deadline insisted upon by RNZ.

[16] WDHB requested an extension to that deadline.

[17] At 3.27pm on 28 July 2021, RNZ refused WDHB's request for additional time and said that it reserved the right to run the story.

[18] At 5.12pm on 28 July 2021, WDHB through its solicitors wrote to the Editor-in-Chief of RNZ objecting to any use of information from the Stolen Dataset and required RNZ to refrain from publishing such information and, at a minimum, sought an undertaking that RNZ would provide at least 48 hours' notice of any intention to publish any private and confidential health information so that WDHB could take steps to protect its position and that of its patients, as well as to enable individuals to be alerted about the possible publication and to receive the appropriate support.

[19] By email at 6.53pm on 28 July 2021, RNZ refused to provide the undertaking sought.

[20] At 8.35pm on 28 July 2021, WDHB requested RNZ hold off from any publication of its intended story to allow WDHB to take any necessary steps by way of protection of its patients.

[21] Without further notice, at 7am on 29 July 2021, RNZ broadcast the threatened story based on the Stolen Dataset and published a related story on its website.

[22] RNZ subsequently continued to broadcast and publish news items based on the same information from the Stolen Dataset.

[23] The RNZ publications contained confidential patient information from the Stolen Dataset.

[24] As a result of the refusal by RNZ to delay publication for a day so that protective steps could be taken, WDHB did not have an opportunity to contact the child who is the subject of the RNZ publications, nor their whānau or caregivers, prior to publication.

[25] Although the child was not expressly named in the RNZ publications, it is easily identifiable in the RNZ stories by those who know of the child or their circumstances.

WDHB applications

[26] Late on the afternoon of Monday 2 August 2021, WDHB filed an application seeking orders:

(a) restraining the first and second defendants from accessing or performing any set of operations on the Stolen Dataset or its contents without WDHB's consent;

(b) requiring the first defendant to immediately take down and be restrained from further publishing or causing to be published certain specified RNZ publications.

[27] Orders for injunctive relief were sought under r 7.53 of the High Court Rules 2016 (HCR) and the Court's inherent jurisdiction.

[28] The applications were filed without notice but on a *Pickwick* basis with RNZ being provided with a copy.

[29] An urgent teleconference was convened at 11am on Wednesday 3 August 2021. Ms Baigent, solicitor for the plaintiff, and Mr Stewart, counsel instructed on behalf of the first defendant, participated in that teleconference.

The joint memorandum

[30] Immediately prior to the teleconference, a joint memorandum signed by the plaintiff's solicitor and first defendant's counsel was filed. That memorandum recorded that the plaintiff and first defendant agreed by consent that orders might be made in the form attached to the memorandum. A copy of those orders is set out as Schedule 1 to this decision.

[31] The proposed orders differed from the relief sought in the application in that:

(a) there are limited carve-outs from the restraining orders for the use of certain information contained in the Stolen Dataset by the first defendant that has already been published as part of the RNZ publications, and to clarify that the restraining order will not cover information that is lawfully obtained; and

(b) the first and second defendants are to destroy any copies of the Stolen Dataset in their possession.

[32] Subject to the restraining orders being made against both the first and second defendants in the proposed form, the plaintiff no longer sought take-down orders in relation to the RNZ publications.

[33] The description of the "unknown defendants" in the proposed orders is slightly different from that recorded in the statement of claim.

The unknown defendants

[34] As the making of the orders sought against the unknown defendants is a critical component of the consent memorandum, it is necessary for the Court to consider whether grounds exist for making the orders sought against the second defendants.

[35] A preliminary point is whether this application should be considered on a without notice basis. HCR 7.53 sets out the requirements in relation to interlocutory injunctions seeking interim relief.

[36] HCR 7.53(2) permits the Court to grant an interlocutory injunction on a without notice basis in urgent cases.

[37] The Court of Appeal has provided an indication as to how applications for interim relief under HCR 7.53 should be approached. In *Commerce Commission v Viagogo AG*, it said:[1]

> [29] It is commonplace for interim relief to be granted against a defendant present in New Zealand, under the High Court Rules and the court's inherent jurisdiction, before the proceedings have been served on the defendant. This is appropriate where the purpose of the order would be undermined by serving the proceedings before the orders are made, or in cases where the interim relief is so urgent that it is not possible to formally serve the defendant before seeking that relief.
>
> …
>
> [94] An application for interim relief should be made without notice to the defendant only where that is essential, either because giving advance notice will defeat the purpose of the order sought, or because the application is so urgent that it is not feasible to give notice. Applications in the second category should be rare, and every attempt should be made to provide such notice as possible – even if it is only a telephone call or text or email – to alert the

[1] *Commerce Commission v Viagogo AG* [2019] NZCA 472 at [29] and [94].

defendant to what is happening and enable them to participate on a *Pickwick* basis.

[38] Applicants for interim injunctions must file an undertaking as to damages. WDHB has done that.[2]

[39] The Court must determine:[3]

(a) whether there is a serious question to be tried;

(b) where the balance of convenience lies; and

(c) where the overall justice of the case lies.

[40] The New Zealand Courts have recognised the appropriateness of granting injunctions against "unknown defendants" in a variety of circumstances, and in particular where confidential information has been stolen. In *Commerce Commission v Unknown Defendants*,[4] the Court granted an injunction against the persons who had gained unauthorised access to the Commerce Commission's confidential electronic material and persons to whom that information was disclosed or otherwise was made available without the consent of the Commerce Commission. The Court made an order restraining the unknown defendants from, among other actions, copying, distributing, broadcasting or otherwise publishing the stolen data.

[41] Similar orders were made against unknown defendants in *Slater v APN New Zealand Limited* where the plaintiff was the subject of computer hacking.[5]

[42] In the United Kingdom, where there has been a cyber-attack and use of ransomware of the type involved in this case, the Courts have ordered broad

---

2 High Court Rules 2016, r 7.54.

3 *Klissers Farmhouse Bakeries Ltd v Harvest Bakeries Ltd* [1985] 2 NZLR 129 (CA) at 142; and *Intellihub v Genesis Energy Ltd* [2020] NZCA 344 at [23].

4 *Commerce Commission v Unknown Defendants* [2019] NZHC 2609, [2019] NZAR 1945.

5 *Slater v APN New Zealand Limited* [2014] NZHC 2157.

injunctions against "unknown defendants" in relation to the use of illegally obtained data.[6]

Analysis

[43] Having read the affidavits filed in support of the application by Kevin Joseph McMahon and Katherine Elizabeth Coley, I am satisfied that there is a serious question to be tried. There is no doubt that the information in the Stolen Dataset was unlawfully obtained by criminal activity by hackers for the purpose of attempting to extort a ransom from the plaintiff. I am satisfied that, in making the Stolen Dataset available on the dark web and encouraging media outlets to access it and publicise it, the perpetrators of the cyber-attack have done so in an attempt to cause maximum embarrassment and distress to the plaintiff, its staff and patients for the purpose facilitating their attempted extortion.

[44] I am also satisfied that the balance of convenience favours the granting of the injunction sought. There is no doubt that the unknown defendants may well, as RNZ has done, seek to justify publication of information gained from the Stolen Dataset by claiming that the public interest outweighs the interests of privacy and confidentiality that are breached by the publication of such data. They may also argue that the public interest outweighs the consequences of their actions in assisting the cyber-attackers in their attempt at extortion.

[45] Such arguments are not going to be easy to establish as the "public interest" defence to breach of confidence in New Zealand is relatively limited. The Court of Appeal in *Blum v ANZ Bank Limited* described the position as being:[7]

> When the defence is available and is pleaded, what the Court needs to decide is whether the public interest and the protection of confidential information is outweighed by the public interest in disclosure of the confidential information. The onus is on the party seeking to disclose confidential information to identify and establish the public interest. The onus is not readily able to be discharged: the Courts draw a distinction between matters that are in the public interest and those that are merely of interest to the public. Moreover, the test is not only whether the information is a matter of public interest, but whether

---

6 *Health Service Executive v Persons Unknown* [2021] IEHC 75 2021 75 IA; *Clarkson Plc v Person(s) Unknown* [2018] EWHC 417 (QB); and *PML v Person(s) Unknown* [2018] EWHC 838.

7 *Blum v ANZ Bank Limited* [2015] NZCA 335 at [55].

> in all the circumstances it is in the public interest that the duty of confidence should be breached.
>
> (footnotes omitted)

[46] I am satisfied that the prospects of other unknown defendants accessing the Stolen Dataset and publicising the highly confidential and sensitive information that it contains would be a source of immense distress to all individuals whose confidential information is at risk of being so misused.

[47] While those who would wish to publicise the stolen information for their own commercial gain will be inconvenienced in that objective by the issue of an interlocutory injunction, such inconvenience is significantly outweighed by the distress caused to those whose privacy rights in their personal and sensitive information is breached if the Court does not grant the interim relief sought.

[48] In terms of where the overall justice of the matter lies, there are strong arguments to the effect that it is not in the public interest that the confidentiality of the private, personal and sensitive information in the Stolen Dataset be breached.

[49] Equally, there are public policy arguments against permitting unknown defendants to attempt to profit in a way which assists extortionists to inflict maximum pressure on their victim to comply with their ransom demands and/or to intimidate other potential victims by demonstrating to them the willingness of media organisations in particular to utilise stolen confidential data for their own ends.

Conclusion

[50] For these reasons, I am satisfied that this is an appropriate case to make the orders sought against the second defendants, and I make the orders set out in Schedule 1 to this judgment.

[51] I grant leave for any party affected by these orders to move, on four days' notice, to have them varied or set aside.

[52] The plaintiff and first defendant have jointly requested that these proceedings be transferred from the Wellington Registry of the High Court to the Auckland Registry of the High Court.

[53] These proceedings were commenced in the Wellington Registry in accordance with HCR 5.1(1)(a), on the basis that the first named defendant has its registered office in Wellington. The Court has a discretion pursuant to HCR 5.1(5) to transfer a proceeding to a different registry if that would be more convenient to the parties.

[54] The plaintiff and first defendant submit that the Auckland Registry is more convenient because:

(a) the first defendant's relevant editorial staff are based in Auckland, as is the first defendant's legal counsel;

(b) the plaintiff is based in the Waikato and the Auckland Registry is closer and more convenient for it than Wellington, and the plaintiff's legal counsel is also based in Auckland; and

(c) it will be more convenient for the filing of documents including original affidavit evidence if the proceeding is held in the Auckland Registry.

[55] I am satisfied that Auckland is the more convenient registry and transfer these proceedings there.

Churchman J

Solicitors:
Simpson Grierson, Auckland for Plaintiff

R Stewart QC, Barrister, Auckland for Defendant

Schedule 1

Orders

1. Restraining the first and second defendants, their servants, related bodies corporate, subcontractors, directors, officers, employees, personnel, agents or other persons authorised to act on their behalf, from accessing, facilitating access, or performing any set of operations on the Stolen Dataset (or its contents), without WDHB's consent, including creating any derivation of, or using, accessing, linking, collecting, searching, reviewing, copying, structuring, organising, adapting, retrieving, inputting, storing, broadcasting, publishing, sharing, making available to any members of the public, transferring, or disclosing any information, data or documentation, whether by manual or automated means, from the Stolen Dataset.

2. Requiring the first and second defendants, unless the WDHB consents otherwise, to permanently delete any and all copies of the Stolen Dataset in their possession or control or information obtained from it, and provide an undertaking to WDHB that they have done so.

3. For the avoidance of doubt, these orders 1 and 2 do not extend to:

   (a) the content reported in the RNZ publications (being the items already published/broadcast by RNZ, as defined in the schedule annexed to the application for injunction without notice) and the continued publication of issues raised by the RNZ publications, provided that such continued publications do not involve accessing, using or disclosing or otherwise dealing with any content of the Stolen Dataset not already disclosed in the RNZ publications, and continue not to name or otherwise identify the child who is the subject of the publications.

   (b) the lawful use by the defendants of information, data or documentation that is in, or shall have come into, the public domain lawfully and other than as a result of any dealings by any person with the Stolen Dataset or its contents.

4. The second defendants are persons currently unknown who were responsible for the illegally obtained data from the plaintiff as a result of the cyber attack suffered by the plaintiff in May 2021, and those who have obtained, or may obtain, access to or otherwise may be or have been provided with information from the Stolen Dataset.