IN THE EMPLOYMENT RELATIONS AUTHORITY
AUCKLAND

I TE RATONGA AHUMANA TAIMAHI
TĀMAKI MAKAURAU ROHE

[2020] NZERA 284
3093872

	BETWEEN	TALENT PROPELLER LIMITED Applicant
	AND	YJL Respondent

Member of Authority:	Marija Urlich
Representatives:	Richard Upton, counsel for the Applicant Respondent, in person
Investigation Meeting:	30 April and 5 May 2020 by telephone
Submissions received:	11 May, 29 May and 15 July 2020 from Applicant 25 May and 15 July from the Respondent
Further information received:	14 July 2020
Determination:	22 July 2020

DETERMINATION No 1 OF THE AUTHORITY

Non-publication order

[1] The respondent sought an order prohibiting publication of some evidence and her identity because the evidence was subject to a non-publication order imposed in another jurisdiction and publication of her identity would have a detrimental effect on her health. An interim non-publication order was granted on 10 March 2020. Submissions and information have been received from the parties on whether the interim order should be made permanent.

[2] Talent Propeller Limited (Propeller) opposes the interim order being made permanent.

[3] Given non-publication is in place for the subject evidence any risk of its publication is unacceptable. Propeller's suggestion that the determination be written to avoid any reference to the evidence is reasonable but not sufficient to eliminate the risk of publication given the nature of that evidence.

[4] The Authority is satisfied the medical information provided prior to and after the investigation meeting establishes the respondent's health issues are serious and likely to be exacerbated by publication of her identity.

[5] On balance, the requisite high standard has been met and the interests of justice require a final non-publication order on the basis sought by the respondent.[1] The order is made permanent. The evidence described in the Authority minute dated 10 March 2020 and any reference to it or its contents in the evidence is permanently suppressed. The identity of the respondent and any reference to the respondent's identity is permanently suppressed. The order is made under clause 10(1) schedule 2 of the Act.

[6] For the remainder of the determination the respondent is referred to as YJL.

Employment Relationship Problem

[7] Propeller says YJL has, without authorisation, gained access to its computer, banking and social media systems after her employment ended in February 2020. Propeller says it has suffered consequent to this access and seeks orders requiring YJL to comply with the terms of her employment agreement, including her obligation not to retain and/or misuse company property (being company passwords and computer systems) and her obligation of confidentiality. Propeller says an award of a penalty is warranted.

[8] YJL denies she has gained access to Propeller's systems after her employment ended.

The Authority's investigation

[1] *H v A Ltd* [2014] NZEmpC 92, [2014] ERNZ 38 at [78] and *XYZ v ABC* [2017] NZEmpC 40, EMPC 69/2017

[9] On 26 February 2020 Propeller lodged an application in the Authority alleging breaches of duty by YJL prior to and after her employment ended on 19 February 2020. Propeller requested the application be granted urgency.

[10] The parties filed memoranda on the issue of urgency. It was apparent the application would benefit from quick resolution. On 5 March timetabling directions were made which included filing dates for YJL's statement in reply and the parties' evidence and a direction to mediation. An investigation meeting was scheduled for 30 March.

[11] YJL duly filed a statement in reply and has filed a personal grievance against Propeller.

[12] The parties attended mediation as directed.

[13] On 23 March a case management call was held with the parties during which the scheduled investigation meeting was adjourned due to the COVID-19 pandemic lockdown. After hearing from the parties, priority was granted to one aspect of Propeller's claim – YJL's alleged breaches of duty after dismissal.

[14] A priority hearing is appropriate because Propeller says the alleged post-employment breaches are ongoing and harmful and the issue is discrete from the other aspects of Propeller's claim. The balance of the application and YJL's personal grievance are yet to be investigated and determined.

[15] The parties filed witness statements and documents in accordance with a further timetable.

[16] On 30 April and 5 May an investigation meeting was held by telephone. The witnesses identified themselves, affirmed the contents of their witness statements and answered questions put to them by the Authority and the parties. Evidence was given by Sharon Davies, Natasha Smith, Rob Davis, YJL and YJL's partner. Submissions and further information have been subsequently filed.

[17] YJL's submissions, in part, contained unsworn and untested evidence which the Authority has set aside.

[18] As permitted by s 174E of the Employment Relations Act 2000 (the Act) this determination has stated findings of fact and law, expressed conclusions on issues necessary to dispose of the matter and specified orders made. It has not recorded all evidence and submissions received.

The issues

[19] The issues requiring investigation and determination are:

(i) Did YJL gain access to Propeller's computer, banking and social medial systems without authorisation after her employment ended?
(ii) If so, did this breach any duty YJL owed Propeller?
(iii) If so, is a compliance order and penalty warranted?
(iv) Should either party contribute to the costs of representation of the other party?

The employment agreement

[20] The parties' employment agreement includes:

> 19. Confidential Information
>
> 19.1 The parties agree that information, processes, materials, customer lists, data and costs, business, marketing and advertising plans, secrets, intellectual property and the like relating to any aspect of this agreement or any of the business or other affairs of the Company ("Confidential Information") are valuable and essential assets of the Company.
>
> 19.2 The Employee will not at any time during their employment with the Company or after its termination:
>
> (a) make use of the Confidential Information; or
> (b) discuss Confidential Information with, or disclose it to, any person,
>
> except to carry out their Duties or with the Company's written consent. The Employee must not use any Confidential Information in any way which is

detrimental to or in competition with the Company, and will sign any confidential agreement reasonably required by the Company.

25. Termination of Employment

…

Return of Company property

25.11 Upon termination of employment, the employee must immediately deliver to the Company all issued tools, clothing, samples, product or other equipment remaining the property of the Company, and all records, documents, plans, letters, papers, and other material of every description (including copies and extracts of such documents) in the employee's possession or control relating to the affairs of the Company. The value of any property or equipment not returned or damaged shall be deducted from any final payment owed to the Employee.

[21] The obligations in clause 19 survive the employment relationship. The obligation to return property at termination, as set out in clause 25, remains and is enforceable after the employment relationship ends.

Relevant law

Compliance orders

[22] Section 137 of the Act provides where any person has not observed or complied with any provision of any employment agreement the Authority may order compliance. The person seeking compliance must show detriment or prejudice subsequent to the alleged non-compliance.

Evidential standard

[23] The burden is on Propeller to establish the material facts on which the application is based to a standard of probability, that is, is it more likely than not that YJL undertook the alleged actions.[2]

[2] *New Zealand (with exceptions) Shipwrights etc Union v Te Moana* [1989] 1 ERNZ (LC), *United Food & Chemical Workers Union of NZ v Talley* [1992] 1 ERNZ 756 (LC).

Did YJL, without authorisation, gain access to Propeller's systems after her employment ended?

[24] Propeller says this occurred in the following specific instances:

(i) On 19 February 2020 YJL accessed Propeller's computer systems and attempted to alter the password of the Managing Director, Sharon Davies;
(ii) On 20 February 2020 she accessed Ms Davies' inbox through that of her Executive Assistant, Tash Smith and deleted a number of emails;
(iii) On 13 March 2020 YJL accessed Ms Davies' bank card details and attempted to make purchases using that card;
(iv) YJL changed Ms Davis' Linkn password;
(v) In April 2020 YJL made further attempts to access Propeller email addresses.

[25] There is no question YJL did not have authorisation to access Propeller's systems after her employment ended.

[26] There is no question YJL did not have the means to access Propeller's computer systems as she would have during her employment. Prior to her dismissal she returned her work issue laptop. On dismissal she returned her work cell phone and Propeller disabled her email login and password.

[27] There is no question that the unauthorised access as listed in [20] above occurred.

[28] The question is whether YJL was responsible for that unauthorised access.

Context for the application

[29] Propeller says it is more likely than not that YJL is responsible for the unauthorised access because of actions associated with YJL's work computer use prior to the end of her employment (email manipulation and mass deletes of emails), analysis of Propeller's systems logs recording remote access to Propeller's business systems by ISP and VPN accounts it says YJL has used in the past.

[30] The timeline immediately prior to YJL's dismissal provides context for YJL's application:

- In early January issues related to YJL's employment came to Propeller's attention.
- On 28 January YJL's work issued laptop was wiped of its history. The laptop was referred to IT support and reset.
- On 30 January YJL's laptop was wiped again. YJL handed in her laptop and was issued a desk top computer.
- On 3 February Propeller spoke to YJL about employment issues.
- On 4 February after 10.46am, while YJL was on sick leave and away from the Propeller's offices, mass deletions of YJL's emails occurred.
- On 10 February Propeller commenced a disciplinary process against YJL alleging YJL had falsified the parties' employment agreement.
- On 10 February between 12.06pm and 12.15pm there was a further mass deletion of emails from YJL's computer.
- On 19 February Propeller summarily dismissed YJL having satisfied itself she had falsified the employment agreement and produced a falsified document during the disciplinary investigation by way of explanation.

[31] Propeller says the dates of some of the unauthorised access, particularly 19 and 20 February and 13 March, provides further relevant context for the application because they fall on significant dates of interaction between YJL and Propeller – the date of YJL's dismissal, the day after and the day the parties attended mediation.

[32] Propeller says given this context the unauthorised access of its systems cannot be a mere coincidence.

[33] Propeller says further, again given the context, YJL has "form" to have undertaken the unauthorised access described above.

Propeller's evidence in support of alleged breaches

[34] The IT contractor, who dealt with the unauthorised access to Propeller's systems and analysed Propeller's computer logs, provided evidence to the Authority of the conclusions reached and how those conclusions were reached. The contractor has

considerable experience in systems engineering in New Zealand and overseas. The contractor's business provides Cloud and managed IT services to Talent Propeller and has done so for a number of years.

[35] The Authority observes the contractor's evidence did not only involve technical analysis and that he attributed motives to YJL which appear to be informed by information about her employment circumstances received from Propeller which in turn have informed conclusions on the technical matters. For example, in his written evidence the consultant:

- states he was aware Propeller was making inquiries into some employment matters with YJL in late January 2020 and the subsequent disciplinary investigation;
- states YJL "To the best of my knowledge never denied undertaking the full system recovery of this laptop" implying he had some knowledge of inquiries made of YJL about her laptop use;
- concludes YJL reset her laptop for the purpose of deleting her work history from the device;
- became suspicious of "…what [YJL] was doing." because the two resets of the laptop was a situation outside his experience;
- attributes knowledge to all Propeller's employees of Ms Smith's access to Ms Davies' inbox;
- expressed a belief, that following his investigation into the email systems, during the disciplinary investigation, that YJL falsified the email which she produced by way of explanation;
- asserts the investigation established YJL (rather than YJL's work allocated login) uses the VPN client called Web2Objects.

[36] In answer to questions from the Authority the contractor accepted:

- there was no direct evidence YJL is responsible for the unauthorised access to Propeller's systems;
- the analysis of Propeller's systems and logs did not establish directly that YJL was responsible for the password reset request;

- the analysis of the systems logs did not establish YJL knew Ms Smith's password (it was through access to Ms Smith's mailbox that the reset request was made and the emails deleted from Ms Davies' inbox);
- the analysis of the systems logs did not establish YJL had accessed the platform where logins and passwords are stored.

[37] The contractor says in his view the 19 and 20 February access and April attempted access are very likely to have been made by YJL because:

- she had remotely deleted items from her mailbox during her employment, wiping her computer on two occasions;
- the same IP address used on 19 February to access Ms Smith's mailbox was the same IP address used to access YJL's and Ms Smith's mailboxes previously;
- a VPN client Web2Objects account attempted to access Propeller accounts on 1 and 8 April and a Web2Object account had previously accessed YJL's Propeller account;
- Ms Davies did not request the password change on 19 February;
- Ms Smith did not delete the emails from the inbox on 20 February because she was on site at the time of the event and login access was external to Propeller offices.

[38] In reaching this view he has relied, at least in part, on his analysis of Propeller's system logs. These logs record instances where Propeller login accounts (email addresses and logins) have accessed Propeller's systems from devices within and physically external to the Propeller office.

[39] The systems logs record against each access attempt an IP address (internet protocol address) or a VPN address (virtual private network). Such addresses are made up of a series of numbers – an octet. Part of an octet identifies the ISP (internet service provider) or VPN and part of an octet identifies the location of the ISP. IP addresses are assigned by an ISP to the internet connection being used and can be recycled. The number is dynamic and can change. For example if a router is turned off, when it is turned on again a new IP address may be assigned to the internet connection.

[40] A VPN masks the true IP address from the website, email or device to which it is connected.

[41] The system log analysis undertaken by the consultant shows between 24 January and 10 February 2020 YJL's and Ms Smith's email accounts were accessed seventy-five times by the same IP address from the same location. Two examples follow:

- 3 February 2020 45.56.158.163 VPN Consumer Network
- 10 February 2020 104.238.51.117 Web2ObjectsLLC

[42] The systems logs show on 20 February the Web2ObjectsLLC account accessed Ms Smith's email account. Propeller says the deletions from Ms Davies' inbox followed.

[43] Propeller has not asked Web2ObjectsLLC, an off shore IP address, if YJL has an account. Such an inquiry would likely have to be undertaken by the police using that agency's powers to require such information. Propeller has laid a complaint with the police about the unauthorised access. There is no evidence the police are actively investigating this complaint.

[44] There is no direct evidence of YJL's involvement in the unauthorised access at [24](iii) and (iv) above. The claims are not supported by documentary evidence or technical analysis. Propeller says it is reasonable for the Authority to infer it is more likely than not YJL is liable for these instances of unauthorised access given the conduct attributed to YJL before her dismissal and on 19 and 20 February and the improbability of coincidence.

Determination

[45] Propeller's view that YJL is responsible for the unauthorised access attempts to its systems is dependent on two key findings – first, that YJL knew or it was more likely than not that YJL knew Ms Smith's password and second, that YJL controlled or was more likely than not to have controlled the accessing ISP or VPN accounts.

[46] There is insufficient evidence before the Authority to support such a finding:

(i) there is no direct evidence YJL knew Ms Smith's password;

(ii) there is no direct evidence YJL accessed the platform where the passwords are stored to retrieve that information;

(iii) the IP address similarity between the systems access before YJL's employment ended and after relates to the off shore location of the ISP or VPN;

(iv) there is no direct evidence YJL owned or controlled an account with Web2Objects or the VPN which accessed her and Ms Smith's Propeller accounts and attempted to access Propeller accounts in April. YJL denies owning or controlling such accounts.

[47] Further, the Authority is not drawn to infer YJL is responsible for post-employment breaches of her employment obligations based on alleged conduct prior to her dismissal. It is difficult to avoid the conclusion the technical analysis has been tainted by Propeller's concerns about YJL's employment issues. In addition, the key bridge between the alleged pre and post dismissal conduct involves YJL controlling off-shore ISP and VPN accounts, the evidence for which, as set out above, does not meet the necessary threshold.

[48] Propeller seeks findings of fact by the Authority which set a path from disruption caused to its computer systems after YJL was dismissed to the cause of that disruption being YJL. It follows that the evidence to support every step of such a path must be clear and convincing. The evidence does not support the findings sought.

[49] The remaining claims against YJL at [24] ((iii) – (iv)) above are unsupported by sufficient evidence.

Outcome

[50] The application for compliance order is declined. Propeller has not established to the necessary evidential standard YJL has accessed without authorisation its computer, banking and social media systems after her employment ended in February 2020.

[51] The parties will be contacted in due course with dates to investigate the balance of the application and YJL's personal grievance.

Costs

[52] YJL is self-represented. There is no issue as to costs.

Marija Urlich
Member of the Employment Relations Authority