

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

DOMAIN NAME COMMISSION
LIMITED,

Plaintiff,

v.

DOMAINTOOLS, LLC,

Defendant.

NO. C18-0874RSL

ORDER GRANTING MOTION FOR
PRELIMINARY INJUNCTION

This matter comes before the Court on plaintiff’s “Motion for Preliminary Injunction” (Dkt. # 2) and defendant’s “Motion for Expedited Discovery” (Dkt. # 9). Plaintiff is a New Zealand non-profit corporation that regulates the use of the .nz top level domain, including registering new domain names and responding to inquiries regarding registrants. Defendant collects domain and registrant information from around the world, stores the information, and uses its current and historic databases to sell monitoring and investigative services and products to the public. Plaintiff alleges that the way defendant accessed,¹ stores, and/or uses .nz domain

¹ Unbeknownst to plaintiff, defendant stopped accessing the .nz register on June 14, 2018, the day before this lawsuit and the motion for preliminary injunction were filed. Defendant’s voluntary cessation of the challenged conduct does not make plaintiff’s request for an order precluding access moot, however. Otherwise, “the courts would be compelled to leave the defendant free to return to his old ways. . . . [The standard the Supreme Court has] announced for determining whether a case has been mooted by the defendant’s voluntary conduct is stringent: A case might become moot if subsequent

1 and registrant information constitutes a breach of contract and violates the Computer Fraud and
2 Abuse Act and the Washington Consumer Protection Act. It seeks a preliminary injunction
3 precluding defendant from accessing the .nz register, downloading .nz data into its own
4 database,² and publishing certain .nz data (including all historical information). Defendant
5 opposes the motion and seeks discovery it deems critical to its ability to respond to the request
6 for preliminary relief.
7

8 Having reviewed the memoranda, declarations, and exhibits submitted by the parties³ and
9 having heard the arguments of counsel, the Court finds as follows:

10 **A. Preliminary Injunction Standard**

11 Preliminary relief - ordered at the outset of the case and before any discovery has
12 occurred - is an “extraordinary remedy never awarded as of right.” Winter v. Nat. Res. Def.
13 Council, 555 U.S. 7, 24 (2008). In order to obtain preliminary injunctive relief, plaintiffs must
14 establish that “(1) they are likely to succeed on the merits; (2) they are likely to suffer irreparable
15 harm in the absence of preliminary relief; (3) the balance of equities tips in their favor, and
16 (4) an injunction is in the public interest.” Short v. Brown, 893 F.3d 671, 675 (9th Cir. 2018)
17 (2008). In the Ninth Circuit, “if a plaintiff can only show that there are serious questions going
18 to the merits – a lesser showing than likelihood of success on the merits – then a preliminary
19
20
21

22 _____
23 events made it absolutely clear that the allegedly wrongful behavior could not reasonably be expected to
24 recur.” Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 189 (2000)
(internal quotation marks, citations, and alterations omitted). That is not the case here.

25 ² The Court accepts plaintiff’s representation that it is not, at this point, asking that defendant
26 delete the .nz information that already resides in its databases.

27 ³ Defendant’s evidentiary objections (Dkt. # 35) are overruled.

1 injunction may still issue if the balance of hardships tips *sharply* in the plaintiff’s favor, and the
2 other two Winter factors are satisfied.” Feldman v. Ariz. Sec. of State’s Office, 843 F.3d 366,
3 375 (9th Cir. 2016) (quoting Shell Offshore, Inc. v. Greenpeace, Inc., 709 F.3d 1281, 1291 (9th
4 Cir. 2013)) (internal quotation marks omitted, emphasis in original).

5
6 In this case, plaintiff is seeking an order that would require defendant to take affirmative
7 action, namely to alter its products and services so that they do not include or reveal certain .nz
8 registrant information as they have in the past. Such injunctions are considered “mandatory,” go
9 “well beyond simply maintaining the status quo *pendente lite*[, and are] particularly disfavored.
10 Stanley v. Univ. of S. Cal., 13 F.3d 1313, 1320 (9th Cir. 1994). A mandatory injunction will not
11 issue in doubtful cases: the moving party bears the demanding burden of showing “that the law
12 and facts clearly favor [its] position, not simply that [it] is likely to succeed.” Garcia v. Google,
13 Inc., 786 F.3d 733, 740 (9th Cir. 2015).

14 **B. Breach of Contract⁴**

15
16 Prior to June 26, 2016, when a person made a query regarding an .nz domain name or
17 registrant, plaintiff appended to the response a notice that using multiple queries or the responses
18 thereto “to enable or effect a download of part or all of the .nz Register” is “strictly forbidden.”
19

20
21 ⁴ The contracts at issue do not contain a choice of law provision, and defendant argues that
22 plaintiff cannot show a likelihood of success on the merits because it has not established, as a
23 preliminary matter, what law applies. Dkt. # 23 at 20 n. 15. This argument puts the cart before the horse.
24 The Court, sitting in diversity, applies the law of the forum state unless (a) the parties dispute the choice
25 of law, (b) there is an actual conflict between the laws or interests of Washington and the laws or
26 interest of another state, and (c) the Court determines that another state has the most significant
27 relationship to the occurrence and the parties. Defendant has not affirmatively asserted that New
28 Zealand - or some other state’s - law applies, nor has it identified a conflict between the relevant laws.
“Absent an actual conflict, Washington law applies.” Carideo v. Dell, Inc., 706 F. Supp.2d 1122, 1126
(W.D. Wash. 2010).

1 Dkt. # 4 at 75.⁵ After June 26, 2016, the terms of use (“TOU”) were altered to expressly prohibit,
2 among other things:

- 3 ● sending “high volume” queries “with the effect of downloading part of or all of
4 the .nz Register or collecting register data or records;”
- 5 ● accessing the .nz Register “in bulk” (defined as accessing the data in some way
6 other than by sending individual queries to the database);
- 7 ● storing or compiling register data “to build up a secondary register of
8 information;”
- 9 ● publishing historical or non-current versions of the register data; and
- 10 ● publishing register data in bulk.

11 Dkt. # 4 at 71. Plaintiff alleges that defendant submitted enough queries through Port 43 to
12 create a secondary or shadow register, in effect downloading and storing the .nz register data for
13 its commercial purposes, in violation of both versions of the TOU.

14 **1. Likelihood of Success on the Merits**

15 Defendant argues that plaintiff is not likely to succeed on its breach of contract claim
16 because there was no mutual assent to support an enforceable agreement.⁶ “While new

18
19 ⁵ Although it is not entirely clear from the record, it appears that if a query is made through
20 plaintiff’s website, the TOU are appended to the bottom of the response. If, however, a query is made
21 through an automated computer system known as Port 43 (which is how defendant queried the register),
22 the TOU appeared at the top of the response. In both situations, the contract terms are revealed only
23 after a query is made and plaintiff has provided the requested information.

24 ⁶ Defendant also argues that the contract fails for lack of consideration and indefiniteness and
25 that plaintiff waived its right to enforce any agreement that did exist. Consideration is any act,
26 forbearance, or return promise given in exchange for defendant’s agreement not to download all or parts
27 of the .nz register into a shadow database. King v. Riveland, 125 Wn. 500, 505 (1994). Continued access
28 to plaintiff’s service or website is adequate consideration in the circumstances presented here. The Court
also finds that the relevant terms of the TOU are sufficiently definite that the Court can decide what they
mean when fixing the rights and obligations of the parties. Keystone Land & Dev. Co. v. Xerox Corp.,
152 Wn.2d 171, 178 (2004). The goal of all of these contract formation requirements - mutual assent,

1 commerce on the Internet has exposed courts to many new situations, it has not fundamentally
2 changed the principles of contract” (Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 403 (2d Cir.
3 2004)), and mutual manifestation of assent remains the touchstone of the analysis (Nguyen v.
4 Barnes & Nobel Inc., 763 F.3d 1171, 1175 (9th Cir. 2014)). Plaintiff has chosen to utilize a form
5 of contract known as “browsewrap,” where the website’s TOU are simply posted (sometimes
6 through a hyperlink), with no requirement that the user click an “I agree” button or otherwise
7 make an affirmative indication of assent to the terms. When browsewrap is deemed sufficient to
8 form a contract, it is generally under the theory that a party manifests assent to the terms by
9 using the website and/or accessing the services provided. This theory can be validly applied only
10 where the circumstances suggest an intent or willingness on the user’s part to be bound,
11 however. Courts have been willing to draw such an inference when the user has actual or
12 constructive knowledge of the TOU and understands that its access to the services, information,
13
14

15 _____
16 consideration, and definiteness - is to “avoid trapping parties in surprise contract obligations.” Id.
17 (quoting Teachers Ins. & Annuity Ass’n v. Tribune Co., 670 F. Supp. 491, 497 (S.D.N.Y. 1987)). The
18 real contract formation issue in this case - discussed in the text - is whether there was mutual assent.

19 As for waiver, the only evidence defendant cites is plaintiff’s two-year delay in bringing this
20 action after learning in mid-2016 that defendant was effectively downloading the .nz register. Waiver is
21 the intentional and voluntary relinquishment of a known right, which can be proven by an express
22 agreement or by an inference arising from circumstances indicating an intent to waive. Pellino v.
23 Brink’s Inc., 164 Wn. App. 668, 696-97 (2011). At the time plaintiff discovered defendant’s actions, it
24 was engaged in an extensive review of privacy issues related to its data, including public comments
25 regarding its current practices and customer expectations. Starting in November 2017, plaintiff initiated
26 contact with defendant and spent months attempting to resolve this dispute informally. Under
27 Washington law, plaintiff had six years to file suit for breach of contract. RCW 4.16.040. It waited a
28 little over a year to make clear that it intended to enforce the TOU and, when its informal efforts proved
unsuccessful, filed this lawsuit two years after discovering the breach. If simply delaying suit for two
years were enough to constitute a waiver, the limitations period would have no meaning. There is no
reasonable inference that plaintiff intended to relinquish its rights under the TOU.

None of these arguments is weighty enough to adversely impact plaintiff’s likelihood of success
on the contract claim.

1 or applications within the website is conditioned on its agreement to those terms. Nguyen, 763
2 F.3d at 1176.

3 If defendant were a one-time or sporadic user of plaintiff's services, it would be very
4 difficult to find mutual assent based on the existing record. Such a user would likely have no
5 idea that his or her ability to query the website was subject to any terms or conditions. A domain
6 search can be accomplished from the landing page without any indication that a contract is in the
7 offing. It is not until information is returned in response to a query that the TOU are presented
8 and the user is informed that by submitting the request, he or she entered into an agreement. At
9 that point it is too late to undo the transaction or to avoid onerous terms, and it is unlikely that
10 the TOU would be enforceable against such a user.
11

12
13 Defendant is not, however, a one-time or sporadic user. Rather, it has been querying
14 plaintiff's system for years, and the responses have all included the TOU and a clear notification
15 that submitting a query results in a contract with plaintiff on the specified terms. When
16 defendant produces .nz register data to its own customers, it excises the TOU. There is,
17 therefore, significant evidence that defendant was aware of the TOU, and it has not denied
18 knowledge in this litigation. The Second Circuit dealt with this exact scenario and reasoned:
19

20 The situation might be compared to one in which plaintiff P maintains a roadside
21 fruit stand displaying bins of apples. A visitor, defendant D, takes an apple and
22 bites into it. As D turns to leave, D sees a sign, visible only as one turns to exit,
23 which says "Apples – 50 cents apiece." D does not pay for the apple. D believes he
24 has no obligation to pay because he had no notice when he bit into the apple that
25 50 cents was expected in return. D's view is that he never agreed to pay for the
26 apple. Thereafter, each day, several times a day, D revisits the stand, takes an
27 apple, and eats it. D never leaves money.
28

1 P sues D in contract for the price of the apples taken. D defends on the ground that
2 on no occasion did he see P's price notice until after he had bitten into the apples.
3 D may well prevail as to the first apple taken. D had no reason to understand upon
4 taking it that P was demanding the payment. In our view, however, D cannot
5 continue on a daily basis to take apples for free, knowing full well that P is
6 offering them only in exchange for 50 cents in compensation, merely because the
7 sign demanding payment is so placed that on each occasion D does not see it until
8 he has bitten into the apple.

9 Register.com, 356 F.3d at 401. Every time defendant submitted a query to obtain .nz register
10 data, it received the requested data with notice of the terms on which plaintiff makes the data
11 available. It cannot reasonably argue that when it made its 100th or 10,000th query, it was
12 unaware that plaintiff offered access and the requested information with restrictions. Defendant
13 "is no more free to take [plaintiff's] data without being bound by the terms on which [plaintiff]
14 offers it, than D was free, in the example, once he became aware of the terms of P's offer, to take
15 P's apples without obligation to pay the 50 cent price at which P offered them." Id. at 402.

16 When applied to the facts in the existing record,⁷ the law clearly favors plaintiff on the
17 merits of its contract claim. Defendant's access to the information in the .nz register was subject
18 to certain limitations, including a prohibition on using "multiple" or "high volume" queries to
19 download (*i.e.*, copy from one computer system to another) part or all of the register. Plaintiff
20 will likely be able to show that defendant violated the TOU when it downloaded plaintiff's data
21

22
23 ⁷ In its motion for expedited discovery, defendant requests an opportunity to inquire into the
24 ownership and technical details of the .nz servers. Defendant has not shown how these facts would
25 impact, much less alter, the contract claim analysis. Any contract that arose was between plaintiff and
26 defendant, regardless whether a third party has some interest or rights in the .nz register. To the extent
27 defendant intends to argue that plaintiff could have taken technical steps to prevent defendant from
28 downloading all or parts of the .nz register, it offers no case law suggesting that plaintiff had any duty to
assume that defendant would breach its contractual obligations and take additional steps to avoid harm.

1 to create a private version of the register. Once defendant became aware of the amended TOU,
2 its downloads and use of the stored data in its products and services constituted additional
3 violations.

4 **2. Likelihood of Irreparable Harm**

5
6 The next issue is whether plaintiff is likely to suffer irreparable harm if an injunction is
7 not issued. A number of plaintiff's alleged harms have either not been proven (plaintiff has not
8 shown that it ever made a promise to registrants that it would retract or otherwise undo past
9 disclosures) or are not irreparable (funds and time expended in investigating and curtailing
10 defendant's actions could be compensated with a monetary award). Plaintiff has, however,
11 shown that it faces irreparable harm to its customer base and business prospects – in short, its
12 ability to attract individuals and entities to the .nz domain – if it is unable to enforce its TOU and
13 provide the privacy upgrades the market is demanding. In October 2015, plaintiff began a review
14 of its practice of providing personal information about a registrant in response to a query of the
15 .nz register. The review was prompted by an increasing awareness that New Zealanders were
16 concerned about on-line privacy issues and believed that personal information was too readily
17 available. The review involved five consultative processes where plaintiff took and considered
18 comments from the public. Plaintiff came to understand that, in addition to general concerns
19 regarding privacy, at-risk and vulnerable people feared for their personal safety if their contact
20 information were publicized. Plaintiff concluded that it was no longer appropriate to compel the
21 public disclosure of contact information for individual registrants: in November 2017, it created
22 an option for non-commercial registrants to request that their information not be available. At
23 oral argument, plaintiff represented that more than 23,000 registrants chose to enroll in the
24
25
26
27

1 program during its first nine months.

2 The record shows that plaintiff's ability to attract and retain registrants depends, at least
3 in part, on responding adequately to the market demand for more privacy when using the .nz
4 domain. Plaintiff was told by current registrants and the public at large that its public disclosure
5 of contact information had prompted or would prompt customers to choose a different domain,
6 one which allowed registration by proxy and/or did not disclose contact information when
7 queried. See Dkt. # 4 at 165-177. By way of example, one former .nz registrant stated, "I
8 canceled my .nz domains a while ago when I realized the consequences of you publishing far too
9 much of my personal information . . . The current system, with proposed changes, makes it far
10 too dangerous for me to consider having a .nz domain again and means I will continue to
11 recommend people not to use it." Dkt. # 4 at 174. Plaintiff has taken steps to remedy the privacy
12 and safety concerns of its customers and potential customers, and over 23,000 individual
13 registrants requested more stringent privacy controls when given the option. Defendant is
14 sabotaging plaintiff's efforts by continuing to publish the contact information and historic data it
15 collected in violation of the TOU. Plaintiff has shown that it is likely to suffer irreparable harm
16 to its business interests if defendant is not enjoined from using the information stored in its
17 database.
18

19
20
21 Defendant argues that it needs to take discovery regarding whether its activities have had
22 any impact on .nz registrants' perception of plaintiff and/or plaintiff's ability to register .nz
23 domains. Dkt. # 9 at 9. The proposed interrogatories and requests for production that relate to
24 these issues seek:
25
26
27

- 1 ● the identity of and contact information for .nz registrants in Washington;⁸
- 2 ● a list of Washington registrants who have opted for more stringent privacy controls,
- 3 expressed privacy concerns, or complained about defendant's actions;
- 4 ● the identity of and contact information for other entities who access plaintiff's query
- 5 service;
- 6 ● survey data generated by the New Zealand Privacy Commissioner; and
- 7 ● any representations or agreements plaintiff made regarding the privacy of registration
- 8 information.
- 9

10 Dkt. # 11-1 at 21-26; # 11-2 at 2-7. Defendant also seeks a half day 30(b)(6) deposition to probe
11 plaintiff's allegations of irreparable harm. Dkt. # 11-3 at 4. While some of the requested
12 information may be relevant to determining the extent of the harm plaintiff suffers as a result of
13 defendant's violations of the TOU, it does not alter the fact that plaintiff has shown a likelihood
14 of irreparable injury. The evidence shows that the publication of personal data has affected
15 consumer choice in the past, and it is no leap to conclude that, if plaintiff cannot enforce the
16 TOU and defendant continues to publish the information it collected over the years, the
17 disclosures will continue to adversely impact plaintiff's ability to obtain and retain registrants. A
18 showing that irreparable harm is likely in the absence of an injunction is all that is required to
19 satisfy the second element of the Winter analysis.
20
21

22
23
24 ⁸ Defendant filed a sur-reply objecting to evidence plaintiff provided with its reply
25 memorandum, including a declaration stating the number of registrants who have opted for privacy
26 controls on their information. Defendant argues that plaintiff should not be permitted to submit
27 "evidence on this crucial point- whether there is irreparable harm" - while denying its request for
28 expedited discovery. Dkt. # 35 at 3. Defendant's written discovery was limited to Washington residents,
however, and would not allow defendant to test or contradict the declarant's statement.

3. Balance of Hardships

Defendant argues that it would face severe hardship if a preliminary injunction is granted. In support, it offers the declaration of its vice president of research and development who states:

Deleting all data obtained from [plaintiff's] service from [defendant's] database would require significant engineering and technical resources. It would take months to disaggregate .nz registrant . . . data and would cause significant disruption to [defendant's] normal operations. In order to identify what data would need to be disaggregated, [defendant] would need to know the identities of every .nz registrant, because for many individuals, they registered domains with numerous registries or registrants. That means the [defendant] may have the same information for a particular individual [sic] or organization from multiple sources. [Defendant] would need to rework terabytes of database files and file pointers and would also need to modify its product code.

Dkt. # 24 at ¶ 15. Defendant's proposed course of action is overly complicated. Plaintiff is not seeking the deletion of all .nz data from defendant's database, so the assertion that an order requiring deletion would cause hardship is unhelpful. In addition, there does not appear to be any need to individually review .nz registrations or to determine whether information linked to the .nz register was also obtained from other registries. Plaintiff seeks an injunction precluding defendant from (a) accessing the .nz register while its authorization to do so is revoked and (b) publishing any of the non-current or historical .nz register data defendant had previously downloaded and stored in its databases. This request for relief would essentially require defendant to adjust its search criteria or, in the alternative, scrub from search results any and all information with a .nz top level domain. Defendant can presumably filter the .nz data using relatively simple database tools. If defendant obtained the same information from another top

1 level domain - if, for example, plaintiff had not only registered at <http://www.dcn.org.nz> but had
2 also registered at <http://www.dcn.info> - the injunction would not apply to whatever registrant
3 information was produced by the .info register because it was not obtained in violation of the
4 TOU.

5
6 Defendant obliquely argues that it would be inequitable for plaintiff to allow defendant to
7 collect and store .nz register information for years and then compel defendant to spend
8 “thousands of person-hours to disaggregate this publicly-available data.” Dkt. # 23 at 30.
9 Defendant makes no attempt to establish the elements of a waiver or estoppel defense and, as
10 discussed above, complying with the proposed injunction would not require an extraordinary
11 amount of time.

12
13 Finally, defendant argues that a preliminary injunction in this case could start an
14 avalanche of litigation as other registers attempt to protect the privacy of their registrants. If
15 defendant built a business by downloading, storing, and using data from other registers in
16 violation of the terms that governed its access to that data, defendant may be correct - other
17 registers may be encouraged to pursue a breach of contract claim if plaintiff is successful here. It
18 would be ironic, however, if a plaintiff who has shown a likelihood of success and irreparable
19 injury were deprived of preliminary relief simply because defendant may have acted wrongfully
20 toward others as well.

22 **4. Public Interest**

23 With regard to the fourth element of the Winter analysis, defendant argues that the
24 products it creates from its meticulously collected register data are critical cybersecurity
25 resources and that the public interest would be harmed if the reports provided to government,
26

1 financial, and law enforcement entities were incomplete because the .nz data were excised. The
2 .nz register is comparatively small, however (approximately 710,000 domains compared with
3 over 135,000,000 .com domains), and the defendant and its customers can access the registration
4 information directly through plaintiff's website if it appears that a bad actor is using an .nz
5 domain. On the other hand, the .nz registrants' privacy and security interests are compromised as
6 long as defendant is publishing non-current or historical .nz information out of its database. The
7 Court finds that the public has an interest in the issuance of an injunction.

9 **C. Statutory Claims**

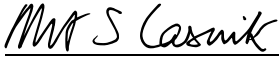
10 Because an injunction is warranted on the breach of contract claim, the Court need not
11 consider whether plaintiff is likely to succeed on the merits of its Computer Fraud and Abuse
12 Act or Consumer Protection Act claims.

14 **D. Bond**

15 Defendant requests that the Court require a \$3.5 million bond to compensate it for the
16 time it will spend reviewing each .nz registrant, cross-referencing other registries and registrars,
17 and reworking database files and file pointers to ensure that .nz data is not provided to
18 customers. As discussed above, the individual record review and cross-referencing that are
19 driving defendant's calculation should not be necessary. Defendant will undoubtedly incur some
20 costs in altering its search parameters and/or scrubbing .nz data from search results. It may also
21 lose customers because its reports will be less complete if it cannot produce its stored .nz data.
22 Defendant provides no way to estimate these costs, however, and the Court declines to guess. A
23 nominal bond of \$1,000 will be required.

1 For all of the foregoing reasons, plaintiff's motion for a preliminary injunction (Dkt. # 2)
2 is GRANTED and defendant's motion for expedited discovery (Dkt. # 9) is DENIED. Defendant
3 DomainTools, LLC, and its officers, agents, servants, employees, and all others acting in active
4 concert with them who receive actual notice of this order are hereby enjoined from accessing the
5 .nz register while DomainTools' limited license remains revoked and/or publishing any .nz
6 register data DomainTools had stored or compiled in its own databases while this action remains
7 pending or until further order of the Court. Plaintiff shall obtain a bond of \$1,000.
8

9
10 Dated this 12th day of September, 2018.
11

12 
13 _____

14 Robert S. Lasnik
15 United States District Judge
16
17
18
19
20
21
22
23
24
25
26
27