

No. 18-35850

IN THE
United States Court of Appeals for the Ninth Circuit

DOMAIN NAME COMMISSION LIMITED,
Plaintiff-Appellee,

v.

DOMAINTOOLS, LLC,
Defendant-Appellant.

On Appeal from the United States District Court
for the Western District of Washington
No. 2:18-cv-00874-RSL
Hon. Robert S. Lasnik

**BRIEF FOR DEFENDANT-APPELLANT
DOMAINTOOLS, LLC**

Aravind Swaminathan
ORRICK, HERRINGTON &
SUTCLIFFE LLP
701 Fifth Avenue, Suite 5600
Seattle, WA 98104

Brian P. Goldman
ORRICK, HERRINGTON &
SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105
(415) 773-5700
brian.goldman@orrick.com

Marc R. Shapiro
Abigail Colella
ORRICK, HERRINGTON &
SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019

Counsel for Defendant-Appellant

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, DomainTools, LLC, hereby states that it is a wholly-owned subsidiary of DomainTools SARL, a privately held corporation. No publicly held corporation owns 10% or more of DomainTools SARL's stock.

Date: December 7, 2018 ORRICK, HERRINGTON & SUTCLIFFE LLP

s/Brian P. Goldman

Brian P. Goldman

Counsel for Defendant-Appellant

TABLE OF CONTENTS

	Page
CORPORATE DISCLOSURE STATEMENT.....	i
TABLE OF AUTHORITIES.....	iv
INTRODUCTION.....	1
JURISDICTION.....	5
STATEMENT OF THE ISSUE.....	5
STATEMENT OF THE CASE.....	6
The “Domain Name System” Connects Users To Locations On The Internet.....	6
Domain Name Registries Administer Top-Level Domains.....	9
Domain Registries And Registrars Have Collected And Published Registrants’ “WHOIS” Information Since The Beginning Of The Internet.....	11
DomainTools Pioneers The Use Of Publicly Available WHOIS Information, Combined With Other Domain Data, To Create Cyber Crime-Fighting Tools.....	18
DomainTools’ Investigative Instruments Help Governments And Enterprises Fight Cyber Threats.....	20
Like Registries Generally, New Zealand’s DNCL Makes WHOIS Information Publicly Available.....	26
DNCL Begins Limiting Access To WHOIS Information.....	31
DNCL Directs DomainTools To Stop Accessing Its Servers And Files This Lawsuit.....	33
The District Court Grants A Preliminary Injunction On DNCL’s Contract-Law Claim.....	34
SUMMARY OF THE ARGUMENT.....	37
STANDARD OF REVIEW.....	40
ARGUMENT.....	42
I. DNCL’s Contract Claim Lacks Merit.....	42

- A. There was no mutual assent to DNCL’s “browsewrap” terms of use. 42
 - 1. “Browsewrap” agreements are generally unenforceable..... 43
 - 2. Terms sent solely via a computer-to-computer channel not designed for human consumption do not provide adequate notice. 46
 - 3. The district court’s analysis was flawed..... 50
- B. At a minimum, both versions of DNCL’s terms of use are too ambiguous to support injunctive relief..... 56
- II. DNCL Failed To Establish Irreparable Harm..... 60
 - A. DNCL supplied no evidence that DomainTools’ use of .nz WHOIS information affects, much less irreparably harms, DNCL’s business..... 60
 - B. The district court’s irreparable harm determination is inconsistent with this Court’s case law. 68
- III. Any Harm To DNCL Is Significantly Outweighed By The Harm An Injunction Poses To The Public Interest And DomainTools..... 70
- CONCLUSION 77
- STATEMENT OF RELATED CASES
- CERTIFICATE OF COMPLIANCE

TABLE OF AUTHORITIES

	Page(s)
Federal Cases	
<i>adidas Am., Inc. v. Skechers USA Inc.</i> , 890 F.3d 747 (9th Cir. 2018).....	39, 40, 60, 61, 62, 68, 69
<i>Alliance for the Wild Rockies v. Cottrell</i> , 632 F.3d 1127 (9th Cir. 2011).....	40
<i>Am. Passage Media Corp. v. Cass Commc'ns, Inc.</i> , 750 F.2d 1470 (9th Cir. 1985).....	63
<i>Cervantes v. Countrywide Home Loans, Inc.</i> , 656 F.3d 1034 (9th Cir. 2011).....	50
<i>Citadel Inv. Grp., L.L.C. v. Citadel Capital Co.</i> , 699 F. Supp. 2d 303 (D.D.C. 2010).....	17
<i>Coalition for ICANN Transparency, Inc. v. VeriSign, Inc.</i> , 464 F. Supp. 2d 948 (N.D. Cal. 2006).....	7, 10
<i>Del Webb Cmtys., Inc. v. Partington</i> , 652 F.3d 1145 (9th Cir. 2011).....	49, 50
<i>Douglas v. U.S. Dist. Court for Cent. Dist. of Cal.</i> , 495 F.3d 1062 (9th Cir. 2007).....	55
<i>Fox Broad. Co. v. Dish Network L.L.C.</i> , 747 F.3d 1060 (9th Cir. 2014).....	61, 65
<i>Garcia v. Google, Inc.</i> , 786 F.3d 733 (9th Cir. 2015).....	41, 50
<i>Gordon v. Virtumundo, Inc.</i> , 575 F.3d 1040 (9th Cir. 2009).....	17
<i>Gucci Am., Inc. v. Huoqing</i> , No. C-09-05969 JCS, 2011 WL 31191 (N.D. Cal. Jan. 3, 2011)	17

Herb Reed Enters., LLC v. Fla. Entm’t Mgmt., Inc.,
736 F.3d 1239 (9th Cir. 2013)..... 40, 61, 62, 70

Kwan v. Clearwire Corp.,
No. C09-1392JLR, 2012 WL 32380 (W.D. Wash. Jan. 3,
2012) 46

Long v. Live Nation Worldwide, Inc.,
No. C16-1961 TSZ, 2017 WL 5194978 (W.D. Wash. Nov. 8,
2017) 49, 56

Los Angeles Mem. Coliseum Comm’n v. Nat’l Football League,
634 F.2d 1197 (9th Cir. 1980)..... 61, 62

Miller v. Cal. Pac. Med. Ctr.,
991 F.2d 536 (9th Cir. 1993)..... 68

*Name.Space, Inc. v. Internet Corp. for Assigned Names &
Numbers*,
795 F.3d 1124 (9th Cir. 2015)..... 8, 10, 11

Nguyen v. Barnes & Noble Inc.,
763 F.3d 1171 (9th Cir. 2014)..... 37, 42, 43, 44, 45, 46, 47, 53

Nicosia v. Amazon.com, Inc.,
834 F.3d 220 (2d Cir. 2016) 43

Office Depot Inc. v. Zuccarini,
596 F.3d 696 (9th Cir. 2010)..... 6, 7, 8, 9, 10, 11

Register.com, Inc. v. Verio, Inc.,
356 F.3d 393 (2d Cir. 2004) 37, 51, 52, 66

Reno v. ACLU,
521 U.S. 844 (1997) 6, 7

Richey v. Metaxpert LLC,
407 F. App’x 198 (9th Cir. 2010) 57

Seven Words LLC v. Network Sols.,
260 F.3d 1089 (9th Cir. 2001)..... 12

<i>Solid Host, NL v. NameCheap, Inc.</i> , 652 F. Supp. 2d 1092 (C.D. Cal. 2009)	12
<i>Specht v. Netscape Commc'ns Corp.</i> , 306 F.3d 17 (2nd Cir. 2002)	44, 45, 48
<i>Stanley v. Univ. of S. Cal.</i> , 13 F.3d 1313 (9th Cir. 1994)	41
<i>Tagged, Inc. v. Doe</i> , No. C 09-01713 WHA, 2010 WL 370331 (N.D. Cal. Jan. 25, 2010)	17
<i>Titaness Light Shop, LLC v. Sunlight Supply, Inc.</i> , 585 F. App'x 390 (9th Cir. 2014)	68, 69, 70
<i>Torres v. Goodyear Tire & Rubber Co.</i> , 867 F.2d 1234 (9th Cir. 1989)	49
<i>United States v. Tisthammer</i> , 484 F. App'x 198 (9th Cir. 2012)	18
<i>Weinstein v. Islamic Republic of Iran</i> , 831 F.3d 470 (D.C. Cir. 2016)	13
<i>Winter v. Nat. Res. Def. Council, Inc.</i> , 555 U.S. 7 (2008)	41, 71
State Cases	
<i>City of Tacoma v. City of Bonney Lake</i> , 173 Wash. 2d 584 (2012)	59
<i>Crafts v. Pitts</i> , 161 Wash. 2d 16 (2007)	61
<i>Gaglidari v. Denny's Rests., Inc.</i> , 117 Wash. 2d 426 (1991)	55
<i>Hedges v. Hurd</i> , 47 Wash. 2d 683 (1955)	57

<i>Johnson v. Nasi</i> , 50 Wash. 2d 87 (1957).....	53
<i>Kruse v. Hemp</i> , 121 Wash. 2d 715 (1993).....	57
<i>In re Marriage of Obaidi & Qayoum</i> , 154 Wash. App. 609 (2010)	48
<i>Mayer v. Pierce Cty. Med. Bureau, Inc.</i> , 80 Wash. App. 416 (1995)	56
<i>Puget Sound Fin., LLC v. Unisearch, Inc.</i> , 146 Wash. 2d 428 (2002).....	59
<i>Yakima Cty. (W. Valley) Fire Prot. Dist. No. 12 v. City of Yakima</i> , 122 Wash. 2d 371 (1993).....	48
Statutes	
28 U.S.C. § 1292(a)(1).....	5
28 U.S.C. § 1331.....	5
28 U.S.C. § 1332.....	5
28 U.S.C. § 1367.....	5
Other Authorities	
DotGov, https://home.dotgov.gov/about/ (last visited Dec. 5, 2018)	10
ICANN, <i>About ccTLD Compliance</i> , https://www.icann.org/resources/pages/cctld-2012-02-25- en (last visited Dec. 5, 2018).....	13
ICANN, <i>Registry Listings</i> , https://www.icann.org/resources/pages/listing-2012-02-25- en (last visited Dec. 5, 2018).....	10

ICANN Generic Top-Level Domains (gTLD): Hearing Before the Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary, 112th Cong. 112-37 (2011) (statement of Rep. Mel Watt), https://judiciary.house.gov/_files/hearings/printers/112th/12-37_66155.PDF 18

Internet Assigned Numbers Authority, *Root Zone Database*, <https://www.iana.org/domains/root/db> (last visited Dec. 5, 2018) 8, 10

InternetNZ, *Whois Protocol*, <https://docs.internetnz.nz/whois/> (last visited Dec. 5, 2018)..... 46

IP Enforcement in the Digital World (2d ed. 2017)
 § 2.05..... 17
 Appx. A 16

Mark A. Lemley, *Terms of Use*, 91 Minn. L. Rev. 459 (2006)..... 44

Letter from Assistant Secretary of Commerce David J. Redl to Cherine Chalaby, Chair, ICANN Board of Directors (Apr. 16, 2018), https://www.ntia.doc.gov/files/ntia/publications/redl_to_ican_on_registrar_issues_april_2018_1.pdf 75

Ernst-Jan Louwers & Stephen Y. Chow, *International Computer Law* § 1.06 (2018) 6

Paul D. McGrady, *McGrady on Domain Names* (2015)
 § 1.06..... 14
 § 1.08..... 9
 §§ 10-355..... 9

Deborah Morley & Charles S. Parker, *Understanding Computers: Today and Tomorrow* (16th ed. 2017) 30

Milton L. Mueller & Farzaneh Badiei, *Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top-Level Domains*, 18 Colum. Sci. & Tech. L. Rev. 435 (2017) 9

Ellen Nakashima, <i>Russian spies hacked the Olympics and tried to make it look like North Korea did it</i> , U.S. officials say, Wash. Post (Feb. 24, 2018), https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html	24
Remarks of Assistant Secretary Redl at ICANN 61 (March 12, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61	73
Remarks of Assistant Secretary Redl at ICANN 63 (Oct. 22, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-63	72
Remarks of Assistant Secretary Redl at State of the Net 2018 (Jan. 29, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-state-net-2018	18
Restatement (Second) of Contracts § 360 (1981)	61
<i>Thematic Challenges in the IG Ecosystem: Cybercrime, Data Protection and Privacy</i> , ICANN63 (Oct. 22, 2018), https://63.schedule.icann.org/meetings/901615	73
Uniform Computer Information Transactions Act (UCITA) § 112 cmt. 3(c)	48
§ 113 cmt. 2	48
U.S. Chamber of Commerce, <i>ICANN WHOIS Database and GDPR</i> (June 19, 2018), https://www.uschamber.com/letter/USCC-ICANN-WHOIS	74, 75

U.S. Gov't Accountability Office, GAO-06-165, Prevalence of
False Contact Information for Registered Domain Names
(2005), <https://www.gao.gov/new.items/d06165.pdf> 12

World Intellectual Property Organization, *ccTLD Database*,
http://www.wipo.int/amc/en/domains/cctld_db/index.html
(last visited Dec. 5, 2018)..... 13

INTRODUCTION

Since before the internet was called the internet, owners of online sites have had to disclose who they are to the public. That information, called “WHOIS” information, has been essential to the safety and stability of the internet. Just as the White Pages does for phone numbers, WHOIS information serves as a public directory that allows users to contact other “domain name” operators—for example, to report technical malfunctions, fraud, or security threats. New Zealand’s own internet authority put it best: “Registering a domain name is a public act, for provision of a useful service on the public Internet.” ER176.

WHOIS information has been a particularly critical tool for cybersecurity professionals responding to cyberattacks. Law enforcement agencies rely on it to identify nefarious actors on the internet and disable the threats they pose. So too do information technology teams across the public and private sectors, who use WHOIS information to protect their networks, their employees, their customers, and their data. DomainTools is a leading provider of analytical tools that these law enforcement and cybersecurity professionals use every

day. Its customers include dozens of local, state, federal, and international agencies, as well as hundreds of companies.

This suit was brought by Domain Name Commission Limited (DNCL), the entity that administers New Zealand’s “.nz” domain names—essentially, all website addresses that end with a .nz. Until recently, DNCL made the WHOIS information for operators of .nz domain names public, just as its peers do around the world. It supplied that information on its website and over “Port 43,” a dedicated channel used across the internet for computers to make automated requests for WHOIS information. In late 2017, however, DNCL announced it would limit some access to WHOIS information in response to a small number of customer concerns about privacy.

Limiting that access was DNCL’s right, contrary though it was to decades-old norms of internet transparency. But DNCL sought to go further. It not only wanted to *prospectively* block access to the WHOIS information it maintained, but also to *retroactively* block researchers and organizations like DomainTools from using the WHOIS information that DNCL had already sent them. So, without warning, DNCL began interpreting the “terms of use” that it had appended to WHOIS

information (which primarily prohibited collecting WHOIS information for use in commercial solicitations) as having barred the commonplace acquisition and use of WHOIS information all along. And it sued DomainTools for breaching that past “agreement.” It was as if the phone company suddenly reinterpreted fine print in the White Pages that prohibited commercial uses of the directory to also bar libraries and others from merely keeping and referencing old phone books already in their possession—and then sued to demand that the old editions be destroyed or removed from circulation.

DNCL’s contract claim is meritless. No contract was formed with DomainTools in the first place because DNCL sent its terms of use only to computers gathering WHOIS information over Port 43, not to humans at DomainTools. The district court failed to acknowledge this important detail. Instead, it assumed without basis that DomainTools knew of and assented to the terms. The terms do not bar DomainTools’ conduct in any event. The different versions of DNCL’s terms of use variously prohibit disruptive access to and use of bulk WHOIS information (e.g., for commercial solicitations), not the long-accepted use of WHOIS information for cybersecurity purposes.

Moreover, *injunctive* relief is plainly unwarranted for DNCL’s novel “breach of contract” claim. The harm the district court identified—lost business opportunities—is not irreparable. Like all consequential damages for breaches of contract, it is traditionally remedied by a monetary award. And DNCL has not shown that the harm is even real. After all, DNCL is a monopoly; anyone desiring a New Zealand-branded “.nz” domain name has no choice but to go through DNCL. Nor has DNCL shown that any harm is caused by DomainTools; it points only to a few complaints aimed at *DNCL itself* for making WHOIS information public—complaints that have nothing to do with use of that data for cybersecurity purposes, by DomainTools or anyone else. The district court relied on pure speculation, not concrete evidence, when it concluded that enjoining DomainTools was necessary to prevent harm to DNCL.

In contrast, the harm to the public from allowing DNCL to retroactively suppress the information it made public is very real: The injunction impairs a critical tool that law enforcement and organizations depend on to combat cyber threats. DNCL can continue trying to prove up its unlikely claim to a permanent injunction in

district court. But in the meantime, DomainTools should be permitted to continue protecting consumers', employees', and companies' private data from malicious cyberattacks. The preliminary injunction should be reversed.

JURISDICTION

The district court had jurisdiction under 28 U.S.C. §§ 1331, 1332, and 1367. On September 12, 2018, the district court issued a preliminary injunction. ER14. DomainTools filed a timely notice of appeal on October 12, 2018. ER77. This Court has jurisdiction under 28 U.S.C. § 1292(a)(1).

STATEMENT OF THE ISSUE

The district court granted a mandatory preliminary injunction on a breach-of-contract claim involving a novel form of agreement transmitted computer-to-computer, with no indication of human involvement and to which no human assented. Moreover, DNCL offered no evidence that DomainTools' conduct was harming its business opportunities, the presumptive form of relief would be money damages anyway, and the public interest strongly favors access to critical

information about cybersecurity threats. Did the district court abuse its discretion?

STATEMENT OF THE CASE

DomainTools is a leading provider of cybersecurity products and services to law enforcement agencies and private enterprises seeking to protect against and respond to cyberattacks. This case involves DNCL’s challenge to DomainTools’ use of WHOIS data—important, publicly available information about the ownership of domain names. To explain the subject of the dispute, we begin by discussing how the internet’s “Domain Name System” works.

The “Domain Name System” Connects Users To Locations On The Internet

The internet is a worldwide system of interconnected computer networks that communicate using a shared set of rules, known as protocols. *Reno v. ACLU*, 521 U.S. 844, 850-52 (1997); 1 Ernst-Jan Louwers & Stephen Y. Chow, *International Computer Law* § 1.06 (2018). The Domain Name System is the protocol that translates easy-to-remember “domain names,” like *uscourts.gov*, into numerical “Internet Protocol (IP) addresses,” like 199.107.22.255, which are assigned to every computer connected to the internet. *Office Depot Inc.*

v. Zuccarini, 596 F.3d 696, 698 (9th Cir. 2010) (citing *Coalition for ICANN Transparency, Inc. v. VeriSign, Inc.*, 464 F. Supp. 2d 948, 951-53 (N.D. Cal. 2006)); ER18. By “provid[ing] an alphanumeric shorthand” for the IP addresses that computers use to route data, the Domain Name System helps people identify and find different places on the internet. *Office Depot*, 596 F.3d at 698 (quoting *Coalition for ICANN Transparency*, 464 F. Supp. 2d at 951-53).

Internet users encounter domain names most often when navigating the World Wide Web—the part of the internet that people use to view and create websites. *See Reno*, 521 U.S. at 852; ER18. To access a particular website, users generally open a web browser (like Internet Explorer or Chrome) and type in the desired website’s Uniform Resource Locator (URL). The URL functions “like a telephone number,” allowing users to reach the associated website. *Reno*, 521 U.S. at 852. To check the news of the day, for example, a user might visit www.latimes.com. Or to learn about the federal courts, she could enter www.uscourts.gov. In each case, the first part of the URL, “www,” stands for “World Wide Web.” The part of the URL that follows is the website’s “domain name.” ER18. Domain names are also commonly

found after the “@” in email addresses. ER18. So, when a reader sends a message to customerservice@latimes.com, the system knows to transmit that data to the customer service “mailbox” on the *Los Angeles Times*’ email server.

In all these contexts, the domain name is composed of two parts, a “top-level domain” name and a “second-level domain” name. ER18-19. The portion to the right of the last period, “.com” and “.gov” in these examples, is the top-level domain. The portion to the left of the last period, like “latimes” and “uscourts,” is the second-level domain. ER19; *Office Depot*, 596 F.3d at 698.

There are over 1,000 top-level domains in use today. *See* Internet Assigned Numbers Authority, *Root Zone Database*, <https://www.iana.org/domains/root/db> (last visited Dec. 5, 2018). These include “generic” top-level domains like .com, .org, .law, and .travel; “sponsored” top-level domains like .gov and .edu, which are “restricted to users who meet specified criteria”; and “country-code” top-level domains like .uk (United Kingdom) and—relevant here—.nz (New Zealand), that are operated by or on behalf of independent nations. *Name.Space, Inc. v. Internet Corp. for Assigned Names & Numbers*, 795

F.3d 1124, 1127 (9th Cir. 2015); 1 Paul D. McGrady, McGrady on Domain Names § 1.08 (2015); ER18-19. Country-code top-level domains are often managed by non-governmental entities and made available for use by the public. See 2 McGrady on Domain Names §§ 10-355; Milton L. Mueller & Farzaneh Badiei, *Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top-Level Domains*, 18 Colum. Sci. & Tech. L. Rev. 435, 443-46 (2017). Many companies use country-code top-level domains for versions of their websites featuring country-specific content and languages, such as www.citi.cn (Citigroup China) and www.youtube.fr (YouTube France).

Domain Name Registries Administer Top-Level Domains

When somebody wants to use a particular domain name for a new website, she must first register the domain name. “Registration” is the process of allocating and administering domain names. Because “[e]ach domain name is unique and thus can only be registered to one entity,” the registration process ensures that web browsers will connect to *her* website when users type in that domain name, not someone else’s—just as a phone company must ensure that it does not issue the same number to two subscribers. *Office Depot*, 596 F.3d at 698 (quoting

Coalition for ICANN Transparency, 464 F. Supp. 2d at 952). This process involves three parties: registries, registrars, and registrants.

Each top-level domain is administered by an entity called a “registry,” which “operate[s] a database for all domain names within the scope of [its] authority.” *Office Depot*, 596 F.3d at 699; ER19. The registry maintains the master list of all domain names registered within that top-level domain, as well as the location on the internet that each domain name points to. *Office Depot*, 596 F.3d at 698; *Name.Space*, 795 F.3d at 1127. The General Services Administration, for instance, is the registry for the .gov top-level domain, just as it is the landlord for the government’s physical property. *See DotGov*, <https://home.dotgov.gov/about/> (last visited Dec. 5, 2018); *see also Root Zone Database, supra*. And Verisign, a private company, is the registry for the internet’s most popular top-level domain, .com. *Office Depot*, 596 F.3d at 699; ICANN, *Registry Listings*, <https://www.icann.org/resources/pages/listing-2012-02-25-en> (last visited Dec. 5, 2018).

Registries do not usually sell domain names directly to the public. Instead, “registries approve registrars, such as godaddy.com, to sell

domain names incorporating those [top-level domains],” as retail brokers. *Name.Space*, 795 F.3d at 1127; see *Office Depot*, 596 F.3d at 699. The individuals and organizations who buy domain names are called “registrants.” *Office Depot*, 596 F.3d at 699; ER19.

Prospective registrants start the process by going to a registrar’s website. There, they can search for available domain names across several top-level domains. After selecting a unique domain name to register (say, wewritebriefs.com), a prospective registrant must pay a fee and provide the registrar with her name and contact information, as well as information for technical and administrative contacts. ER246. The registrar then informs the registry—in this hypothetical, Verisign, because it is a .com domain—that internet traffic to the domain name should be routed to the registrant’s website. *Office Depot*, 596 F.3d at 698. This is like the activation of a new phone number, which tells the telephone company to start routing calls to a particular physical line.

Domain Registries And Registrars Have Collected And Published Registrants’ “WHOIS” Information Since The Beginning Of The Internet

Just as subscribers to a new landline must provide identifying information that is ordinarily published in the White Pages, the contact

information that registrants submit when registering a new domain name is made publicly available in “WHOIS” databases maintained by registries and registrars. *See* ER20; *Solid Host, NL v. NameCheap, Inc.*, 652 F. Supp. 2d 1092, 1095 (C.D. Cal. 2009).

This WHOIS service originated in the 1970s as a way for technicians on ARPANET, an early version of the internet, to identify and contact each other to report technical problems involving each other’s domains. U.S. Gov’t Accountability Office, GAO-06-165, *Prevalence of False Contact Information for Registered Domain Names* 8 (2005), <https://www.gao.gov/new.items/d06165.pdf>; ER226. The “Identification Data Base” was “accessible across the ARPANET” and provided the “full name, ... U.S. mailing address, ... telephone [number], and [email address]” for ARPANET users. ER226.

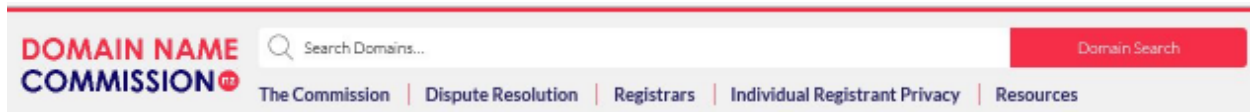
As the internet grew and entered everyday life, a publicly available WHOIS service remained a constant. In the 1990s, responsibility for overseeing the Domain Name System transferred from the U.S. government to a newly created, not-for-profit entity called the Internet Corporation for Assigned Names and Numbers (ICANN). *Seven Words LLC v. Network Sols.*, 260 F.3d 1089, 1092 (9th Cir. 2001).

ICANN contractually mandates that every registry and registrar for generic top-level domains collect WHOIS information and operate a publicly available WHOIS service. ER20.

ICANN does not directly regulate country-code top-level domains like .nz. *See Weinstein v. Islamic Republic of Iran*, 831 F.3d 470, 476 (D.C. Cir. 2016) (describing ICANN's relationship to country-code top-level domains), *abrogated on other grounds by Rubin v. Islamic Republic of Iran*, 138 S. Ct. 816 (2018); ICANN, *About ccTLD Compliance*, <https://www.icann.org/resources/pages/cctld-2012-02-25-en> (last visited Dec. 5, 2018). Nevertheless, most country-code top-level domain managers, including .nz's, have long followed the WHOIS convention, requiring registrars to collect WHOIS information and then making that information available in a public WHOIS service. ER21; ER46; ER176; *see* World Intellectual Property Organization, *ccTLD Database*, http://www.wipo.int/amc/en/domains/cctld_db/index.html (last visited Dec. 5, 2018). Accordingly, there is no global repository of WHOIS information. Instead, WHOIS information is decentralized across independent databases run by individual registries and registrars.

Under this established practice, WHOIS information is made publicly available in two ways: (1) through a “search” function on a webpage designed for human viewing, which allows individuals to perform one-by-one look-ups, and (2) through a direct, computer-to-computer channel called Port 43, which allows automated programs to retrieve WHOIS information on a larger scale and with greater efficiency. ER21-22; 1 McGrady on Domain Names § 1.06, at n.19.

To search WHOIS information for a given domain name, anyone can visit the relevant top-level domain’s WHOIS search website, type in a domain name, and click “search” to get the associated WHOIS information. The search function on the website for the .nz domain (www.dnc.org.nz), for example, looks like this:



ER57. The results returned typically include the registrant’s name, email address, street address, and phone number, as well as the administrative and technical contacts for the domain and other information about the domain’s history, as illustrated on the next page.

"dnc.org.nz" (Active)

Query Date Time	18 June 2018 9:56 am
Domain Name	dnc.org.nz
Query Status	Active
Domain Date Registered	23 April 2002 12:00 am
Domain Date Billed Until	28 June 2018 12:00 am
Domain Date Last Modified	23 May 2018 11:32 am
Domain Delegate Requested	yes
Domain Signed	no
Registrar Name	Domain Name Commissioner
Registrar Address	PO Box 11881
Registrar City	Wellington
Registrar Country	NZ (NEW ZEALAND)
Registrar Phone	+64 4 472 1600
Registrar Fax	+64 4 495 2115
Registrar Email	info@dnc.org.nz
Registrant Name	Domain Name Commission Ltd
Registrant Contact Address	PO Box 11881
Registrant Contact City	Wellington
Registrant Contact Postal Code	6142
Registrant Contact Country	NZ (NEW ZEALAND)
Registrant Contact Phone	+64 4 472 1600
Registrant Contact Email	info@dnc.org.nz
Admin Contact Name	Domain Name Commission Ltd
Admin Contact Address	PO Box 11881
Admin Contact City	Wellington
Admin Contact Postal Code	6142
Admin Contact Country	NZ (NEW ZEALAND)
Admin Contact Phone	+64 4 472 1600
Admin Contact Email	info@dnc.org.nz
Technical Contact Name	Domain Name Commission Ltd
Technical Contact Address	PO Box 11881
Technical Contact City	Wellington
Technical Contact Postal Code	6142
Technical Contact Country	NZ (NEW ZEALAND)
Technical Contact Phone	+64 4 472 1600
Technical Contact Email	info@dnc.org.nz
NS Name	a.ns.internetnz.net.nz
NS Name	b.ns.internetnz.net.nz
NS Name	c.ns.internetnz.net.nz

ER57; see also ER21.

WHOIS information can also be accessed by querying Port 43, a channel that is designated by internet protocols to be used solely for WHOIS requests. ER222. Every registry and registrar has a server that “listens” on Port 43 for WHOIS requests. ER222. When the WHOIS server receives a request, it replies with the relevant identifying information. ER222. While humans can manually query Port 43 by sending a request in computer code through their computer’s “command line interface,” Port 43 is typically used for WHOIS queries by automated computer programs, which can perform searches more efficiently than human users looking up domains one-at-a-time. ER222.

In addition to the WHOIS services run by registries and registrars, WHOIS information can be accessed through dozens of third-party services, tools, and platforms, including those offered by DomainTools. ER185-86; *see also* 1-A IP Enforcement in the Digital World Appx. A (2nd ed. 2017) (listing WHOIS investigative tools). These organizations generally aim to cure the decentralization of WHOIS information by aggregating it and offering tools to search across multiple top-level domains.

Public access to WHOIS information remains the norm decades after its ARPANET origins. Not only do technical issues still arise that require contacting domain name operators, but also WHOIS information plays an important role in providing order and deterring misconduct in the otherwise-anonymous expanse of the internet:

- **Prospective registrants** use WHOIS information to identify “cybersquatters” who have registered domain names using their trademarks or company names. 1 IP Enforcement in the Digital World § 2.05 (2d ed. 2017) (“The most basic tool for domain name enforcement research is the WHOIS search.”); *see, e.g., Citadel Inv. Grp., L.L.C. v. Citadel Capital Co.*, 699 F. Supp. 2d 303, 318 n.11 (D.D.C. 2010).
- **Intellectual property owners** also rely on WHOIS information to identify and communicate with registrants whose websites are being used for improper purposes, like trafficking in counterfeit goods. *See, e.g., Gucci Am., Inc. v. Huoqing*, No. C-09-05969 JCS, 2011 WL 31191, at *2 (N.D. Cal. Jan. 3, 2011) (noting use of DomainTools’ WHOIS searches to identify seller of knock-off handbags).
- **Companies and individuals** use WHOIS information to identify the source of online abuse, from malicious ransomware to phishing attacks to spam. *See, e.g., Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1064 (9th Cir. 2009); *Tagged, Inc. v. Doe*, No. C 09-01713 WHA, 2010 WL 370331, at *2 (N.D. Cal. Jan. 25, 2010) (describing use of DomainTools’ WHOIS searches to identify the source of spam messages).
- And **law enforcement agencies** use WHOIS information to gather investigative leads about spam, fraud, and other

more harmful kinds of cybercrime. *See, e.g., United States v. Tisthammer*, 484 F. App'x 198, 200 (9th Cir. 2012) (noting use of WHOIS information in child pornography prosecution).

Precisely because WHOIS information is essential to keeping the internet safe and secure, the United States government has remained committed to free, publicly available WHOIS information, even after getting out of the business of running the Domain Name System.¹

DomainTools Pioneers The Use Of Publicly Available WHOIS Information, Combined With Other Domain Data, To Create Cyber Crime-Fighting Tools

DomainTools was founded in Seattle in 2002. ER221. It collects and aggregates publicly available WHOIS information, as well as other publicly available information about internet domains, to develop and

¹ *See, e.g.,* Remarks of Assistant Secretary Redl at State of the Net 2018 (Jan. 29, 2018), <https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-state-net-2018> (“[WHOIS] information is often the starting point for law enforcement agencies when investigating malicious online activity, and for private-sector and government actors seeking to protect critical systems from dangerous cyberattacks.... [T]he U.S. government expects this information to continue to be made easily available through the WHOIS service.”); *ICANN Generic Top-Level Domains (gTLD): Hearing Before the Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary*, 112th Cong. 112-37 (2011) (statement of Rep. Mel Watt), https://judiciary.house.gov/_files/hearings/printers/112th/112-37_66155.PDF.

maintain a comprehensive picture of the internet and domain registrations. DomainTools' products and services are built on sophisticated analyses of this data. Governments, law enforcement agencies, and companies rely on DomainTools' analytics tools to protect their digital assets and to investigate cyber threats. ER182-83; ER221.

DomainTools' products and services center on two critical cybersecurity functions: correlation and attribution. "Correlation" is the process of identifying potential cyber threats by drawing associations among multiple sets of data, including information about domain names across different top-level domains. ER192. An investigation might begin, for instance, by accessing the WHOIS record of a domain engaged in suspicious activity. DomainTools' system will match portions of that WHOIS record with similar WHOIS information across the internet (e.g., other domains registered to the same email address), thereby allowing investigators to identify additional domain names controlled by the same entity—like building off a single puzzle piece by finding other pieces that share the same pattern or contours. ER192-93.

"Attribution" is the process of identifying the real-world individual or organization behind an attack, which enables victims and law

enforcement agencies to pursue legal relief. ER194. Unless the WHOIS record for the initial, suspicious domain provides complete and accurate information about the perpetrators—which is unlikely—attribution also requires cross-referencing among data sets to find granules of accurate information that can lead to a positive identification.

In short, by aggregating publicly available information about internet domains, DomainTools’ enterprise products allow cybersecurity professionals to correlate among various data points, identify the source of an attack, attribute the attack to real-world entities, and preemptively block related attacks.

DomainTools’ Investigative Instruments Help Governments And Enterprises Fight Cyber Threats

To understand how these services work in practice, consider a hypothetical “phishing” attack in which a criminal lures a target into providing sensitive data by “spoofing” a trusted source: A nefarious actor sends federal employees an email from message@tsp-gov.us asking them to click a link to log in to their Thrift Savings Plan (TSP) retirement account to update their contact information. The message is a fake, because TSP’s actual email address is message@tsp.gov. But because the “spoofed” variant is close, many employees may mistakenly

believe that they have received a legitimate email from TSP. When they click on the link, they arrive at a fake webpage designed to look identical to TSP's actual webpage. And when they then type in their usernames and passwords to "log in" to the spoof website, they unwittingly hand the attackers the credentials needed to access their real TSP accounts. From there, the attackers could learn sensitive personal details (like contact information and beneficiary designations) or even withdraw employees' retirement funds or take out loans against their retirement accounts.

The government, including federal law enforcement, would surely want to investigate. It might use DomainTools' products to examine how the attack unfolded and to help identify the real-world actors behind the attack. ER194-95. Investigators could begin by taking the basic step of looking up the WHOIS record for tsp-gov.us, the domain from which the phishing emails were sent. That WHOIS record might contain sufficient information to enable law enforcement to identify, further investigate, and prosecute the actors involved. The government might also send a domain "takedown notice" to the registrar identified

in the WHOIS record in an effort to disable future attacks from that source.

But attribution of online attacks is often more complicated, because WHOIS information may be incomplete or attackers may have taken steps to mask their identities. If the current WHOIS record for `tsp-gov.us` did not provide sufficient identifying data, investigators could still use breadcrumbs of information within the WHOIS record to help lead them to the real-world person or organization behind the attack. They might see that the IP address associated with `tsp-gov.us` is also associated with a known criminal organization and focus their investigation accordingly. Or, by locating *historical* WHOIS records, they might find the attackers' contact information in a record created before the attackers took steps to avoid detection. ER194-95.

The government would probably want to preempt future attacks too. It could use DomainTools' products to identify additional domain names that might be lying in wait for use in spoofing TSP in the future—like `tsp-gov.com`, `tsp.gw`, and `thriftsavingsplan.com`. It could also set up automated searches that would send alerts anytime someone registers a new look-alike domain name, so the government could

promptly investigate whether that new domain is a potential threat. ER215-19.

Meanwhile, investigators would want to look for other domain names connected to the attackers. A domain might be connected because it was registered using the same email address, lists the same administrative contact, or directs to the same IP address. ER192-93. That search might uncover hundreds of additional domain names, many seemingly designed to spoof other governmental bodies or financial institutions. IT professionals could then use the technical information associated with those domains to block further attacks before they happen.

This kind of threat analysis was recently used to identify the source of cyberattacks that disrupted the 2018 Olympic Games in South Korea. ER192. By correlating WHOIS information with other data sets, security researchers were able to link the 2018 Olympics attacks to Russian attacks on anti-doping agencies two years earlier. ER192. This allowed them to identify Russian military hackers as the likely perpetrators, even though “the GRU sought to make it appear as though the intrusions were the work of North Korean hackers by using

North Korean IP addresses.” Ellen Nakashima, *Russian spies hacked the Olympics and tried to make it look like North Korea did it*, U.S.

officials say, Wash. Post (Feb. 24, 2018),

[https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-](https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html)

[376b4fe57ff7_story.html](https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html). These methods have also enabled “law enforcement[] investigation, takedown, and prosecution of illegal internet pharmacies.” ER242.

Investigations like these would be nearly impossible without services like DomainTools’, even though they are based entirely on publicly available information. That is because WHOIS information is highly decentralized, yet cybersecurity investigations depend on piecing together small clues across vast records. It is impracticable for investigators to search WHOIS records one-by-one to identify connections between malicious domain names in different top-level domains—especially where time is of the essence to respond to a cyberattack or to prevent the second phase of an attack. ER183; ER191. Additionally, registries and registrars do not make available *historical*

WHOIS information that can be used to track domain ownership over time. WHOIS servers maintained by registries (and their corresponding search functions) provide only current information. Only services like DomainTools, which do maintain records of historical WHOIS information, might have the critical identifying clues from a time when a given attacker may have been less careful in covering his tracks. *See* ER205. DomainTools and others thus assist by maintaining, cross-referencing, and analyzing these huge quantities of public data so that they can be searched and acted upon quickly when needed.

DomainTools' cybersecurity products and services are used by law enforcement, government agencies, and the military, as well as by banks, technology companies, the aerospace industry, and professional services firms. ER185. Before allowing any company to access its comprehensive enterprise products, DomainTools verifies that the company has a legitimate security need. ER185.²

² DomainTools also offers a free, public WHOIS lookup service on its website. ER183. This service is one of many free, public services on the Internet to look up basic, current WHOIS information, such as MyToolbox, WHOis.net, and—most importantly—the free, public


Like Registries Generally, New Zealand’s DNCL Makes WHOIS Information Publicly Available

InternetNZ, a nonprofit organization, is the official registry for “.nz,” the country-code top-level domain for New Zealand. ER20. In 2007, InternetNZ created Domain Name Commission Limited (DNCL) and then delegated to DNCL the responsibility for administering .nz domain names. ER20. Like other registries, DNCL requires registrants to provide personal contact information. ER246. And, until recently, DNCL always provided that information to the public through a free WHOIS lookup service on the DNCL website, as well as via Port 43, the channel designed for automated computer inquiries. ER21-22; ER248.

WHOIS lookup services operated by ICANN and registries themselves. ER183-84. DomainTools limits users of its public WHOIS lookup to ten queries a day. ER183. In addition, DomainTools offers a low-fee service for individuals to conduct a small number of simple inquiries that go beyond the most basic WHOIS information. Individuals can access historical WHOIS data for a given domain (up to 25 domains a month) or search for domains that are associated with a particular name, email address, or other characteristic (up to 5 “reverse WHOIS” searches a month). ER184; ER207; ER429, 438. These searches are particularly helpful in cybersquatting and phishing cases. *See supra* 17-18.

DNCL explicitly tells its registrants that their registration information will be “available to all as a matter of public record,” including for “law enforcement” purposes. ER152, 155. Similarly, InternetNZ’s “frequently asked questions” explains that “[r]egistering a domain name is a public act, for provision of a useful service on the public Internet.” ER176. For that reason, InternetNZ’s stated position is that “[a]ll [top-level domains] should maintain a public and free register lookup service (such as WHOIS), so that members of the public can contact a registrant or their registrar for technical, operational or other reasons.” ER176.

After a user queries the .nz WHOIS server, whether on the website or through Port 43, DNCL transmits the responsive WHOIS records along with terms of use purportedly governing the user’s search. If a user searches via DNCL’s website, the terms of use will appear at the bottom of the results page, below the results themselves, like this:



Domain Search

The Commission
Dispute Resolution
Registrars
Individual Registrant Privacy
Resources

.nz Query

Whitelisting

Recent Changes

"dnc.org.nz" (Active)

Query Date Time	23 June 2018 9:56 am
Domain Name	dnc.org.nz
Query Status	Active
Domain Date Registered	23 April 2002 12:00 am
Domain Date Billed Until	23 June 2018 12:00 am
Domain Date Last Modified	23 May 2018 11:32 am
Domain Delegate Requested	yes
Domain Signed	no
Registrar Name	Domain Name Commission
Registrar Address	PO Box 12881
Registrar City	Wellington
Registrar Country	NZ (NEW ZEALAND)
Registrar Phone	+64 4 472 1600
Registrar Fax	+64 4 472 2124
Registrar Email	info@dnc.org.nz
Registrant Name	Domain Name Commission Ltd
Registrant Contact Address	PO Box 12881
Registrant Contact City	Wellington
Registrant Contact Postal Code	6142
Registrant Contact Country	NZ (NEW ZEALAND)
Registrant Contact Phone	+64 4 472 1600
Registrant Contact Email	info@dnc.org.nz
Admin Contact Name	Domain Name Commission Ltd
Admin Contact Address	PO Box 12881
Admin Contact City	Wellington
Admin Contact Postal Code	6142
Admin Contact Country	NZ (NEW ZEALAND)
Admin Contact Phone	+64 4 472 1600
Admin Contact Email	info@dnc.org.nz
Technical Contact Name	Domain Name Commission Ltd
Technical Contact Address	PO Box 12881
Technical Contact City	Wellington
Technical Contact Postal Code	6142
Technical Contact Country	NZ (NEW ZEALAND)
Technical Contact Phone	+64 4 472 1600
Technical Contact Email	info@dnc.org.nz
NS Name	ans.internetnz.net.nz
NS Name	bnz.internetnz.net.nz
NS Name	canz.internetnz.net.nz

Status Types

- ▼ Active
Means the domain name has already been registered.
- ▶ Pending Release
- ▶ Available
- ▶ Prohibited
- ▶ Conflicted
- ▶ Resolved

Consultations

There are no open consultations.

News

DNC Newsletter May 2018
06 June 2018

Domain Name Commission Limited Board Meeting – 26 April 2018
24 May 2018

Terms of Use: By submitting a WHOIS query you are entering into an agreement with Domain Name Commission Ltd on the following terms and conditions, and subject to all relevant .nz Policies and procedures as found at <https://dnc.org.nz/>. It is prohibited to:

- Send high volume WHOIS queries with the effect of downloading part or all of the .nz Registrar or collecting registrar data or records;
- Access the .nz Registrar in bulk through the WHOIS service (ie. where a user is able to access WHOIS data other than by sending individual queries to the database);
- Use WHOIS data to allow, enable, or otherwise support mass unsolicited commercial advertising, or mass solicitations to registrants or to undertake market research via direct mail, electronic mail, SMS, telephone or any other medium;
- Use WHOIS data in contravention of any applicable data and privacy laws, including the Unsolicited Electronic Messages Act 2007;
- Store or compile WHOIS data to build up a secondary register of information;
- Publish historical or non-current versions of WHOIS data; and
- Publish any WHOIS data in bulk.

Copyright Domain Name Commission Limited (a company wholly-owned by Internet New Zealand (incorporated) which may enforce its rights against any person or entity that undertakes any prohibited activity without its written permission. The WHOIS service is provided by NZRS Limited.

ER57 (red brackets added to highlight terms of use).

28

If a user instead searches via Port 43, the terms of use are transmitted to the receiving computer, prefaced by “%” symbols. Here is the text transmitted over Port 43 displayed in a human-readable format:

```

annamouw — -bash — 116x59
Last login: Tue Jun 12 07:20:36 on ttys000
Annas-MacBook:~ annamouw$ whois dnc.org.nz
% Terms of Use
%
% By submitting a WHOIS query you are entering into an agreement with Domain
% Name Commission Ltd on the following terms and conditions, and subject to
% all relevant .nz Policies and procedures as found at https://dnc.org.nz/.
%
% It is prohibited to:
% - Send high volume WHOIS queries with the effect of downloading part of or
% all of the .nz Register or collecting register data or records;
% - Access the .nz Register in bulk through the WHOIS service (ie. where a
% user is able to access WHOIS data other than by sending individual queries
% to the database);
% - Use WHOIS data to allow, enable, or otherwise support mass unsolicited
% commercial advertising, or mass solicitations to registrants or to
% undertake market research via direct mail, electronic mail, SMS, telephone
% or any other medium;
% - Use WHOIS data in contravention of any applicable data and privacy laws,
% including the Unsolicited Electronic Messages Act 2007;
% - Store or compile WHOIS data to build up a secondary register of
% information;
% - Publish historical or non-current versions of WHOIS data; and
% - Publish any WHOIS data in bulk.
%
% Copyright Domain Name Commission Limited (a company wholly-owned by Internet
% New Zealand Incorporated) which may enforce its rights against any person or
% entity that undertakes any prohibited activity without its written
% permission.
%
% The WHOIS service is provided by NZRS Limited.
%
version: 8.0
query_datetime: 2018-06-13T02:21:42+12:00
domain_name: dnc.org.nz
query_status: 200 Active
domain_datelastmodified: 2018-05-23T23:32:41+12:00
domain_delegaterequested: yes
domain_signed: no
%
registrar_name: Domain Name Commissioner
registrar_address1: PO Box 11881
registrar_city: Wellington
registrar_country: NZ (NEW ZEALAND)
registrar_phone: +64 4 472 1600
registrar_fax: +64 4 495 2115
registrar_email: info@dnc.org.nz
%
ns_name_01: a.ns.internetnz.net.nz
ns_name_02: b.ns.internetnz.net.nz
ns_name_03: c.ns.internetnz.net.nz
%
% Additional information may be available at https://www.dnc.org.nz/whois/search?domain_name=dnc.org.nz
%
Annas-MacBook:~ annamouw$

```

ER60 (red brackets added to highlight terms of use); ER442.

The “%” symbols identify “comment lines” and instruct the receiving computer that the text need not be processed or executed. *See* Deborah Morley & Charles S. Parker, *Understanding Computers: Today and Tomorrow* 450 (16th ed. 2017) (“Comments are usually preceded by a specific symbol ...; the symbol used depends on the programming language being used. Comment lines are ignored by the computer.”).

The content of DNCL’s terms of use has changed over time. Until June 2016, the terms of use prohibited “[u]sing multiple WHOIS queries ... to enable or effect a download of part or all of the .nz Register” and using WHOIS information “to attempt a targeted contact campaign with any person.” ER23. The terms of use did not prohibit anyone from publishing current or historical WHOIS information in any form. ER23.

Then, in June 2016, DNCL replaced its terms of use with new terms, which provide:

By submitting a WHOIS query you are entering into an agreement with Domain Name Commission Ltd on the following terms and conditions, and subject to all relevant .nz Policies and procedures as found at <https://dnc.org.nz/>. It is prohibited to:

- Send high volume WHOIS queries with the effect of downloading part of or all of the .nz Register or collecting register data or records;
- Access the .nz Register in bulk through the WHOIS service (i.e. where a user is able to access WHOIS data other than by sending individual queries to the database);
- Use WHOIS data to allow, enable, or otherwise support mass unsolicited commercial advertising, or mass solicitations to registrants or to undertake market research via direct mail, electronic mail, SMS, telephone or any other medium;
- Use WHOIS data in contravention of any applicable data and privacy laws, including the Unsolicited Electronic Messages Act 2007;
- Store or compile WHOIS data to build up a secondary register of information;
- Publish historical or non-current versions of WHOIS data; and
- Publish any WHOIS data in bulk.

ER22-23.

DNCL Begins Limiting Access To WHOIS Information

In November 2017, DNCL announced a new program called the Individual Registrant Privacy Option (IRPO). ER27. The IRPO gives many individual .nz registrants (as opposed to corporate registrants) the choice to withhold their telephone number and street address from publicly available .nz WHOIS records. ER27; ER251. Notwithstanding

that the IRPO gives certain registrants this choice, DNCL's policy still states (and registrants are still advised) that core registration information—name, email address, and country—will be “available to all as a matter of public record.” ER152; *see* ER27.

DNCL's change in approach came on the heels of discussions within ICANN, which sets policy for generic top-level domains, about the privacy of WHOIS information. ER24-25. While DNCL was not required to follow ICANN's lead, it decided to join the nascent movement to revise longtime WHOIS policies and began soliciting input from the public regarding potential WHOIS policy changes. ER26-27. The feedback it received—a small number of registrant requests for an option to keep some individual information private—led DNCL to create the IRPO.

On the eve of announcing the IRPO, in November 2017, DNCL notified DomainTools for the first time that DNCL construed its existing terms of use to prohibit DomainTools' queries. ER36; ER66-67. DNCL has acknowledged that it became aware of DomainTools' collection of .nz WHOIS information nearly a year and a half prior (in the summer of 2016), but it took no action then. ER234.

In April 2018, DNCL chose to stop making available *all* registrant contact information, technical contact information, and administrative contact information over Port 43. ER24; ER247-48. As a result, information available over Port 43 is now limited to basic information about the domain itself, such as whether it is available and when it was last modified. ER24; ER247-48. Full registration information for individuals who have not opted in to the IRPO remains publicly available only via the search function on the DNCL website. ER247-48.

DNCL Directs DomainTools To Stop Accessing Its Servers And Files This Lawsuit

On June 6, 2018, DNCL sent DomainTools a cease and desist letter revoking DomainTools' permission to use the public .nz WHOIS service. ER36-37; ER72-75. DomainTools initiated technical changes to comply with that demand, completing those changes on June 14.

ER221.

DNCL filed this suit the next day. *See* ER520-47. It alleged that DomainTools' use of the .nz WHOIS service (1) was a breach of contract because it violated DNCL's terms of use, (2) violated the Computer Fraud and Abuse Act, and (3) violated the Washington Consumer Protection Act. *See* ER542-45. DNCL requested damages, injunctive

relief barring DomainTools from accessing, storing, or “publishing” .nz WHOIS information, and an order requiring DomainTools to permanently delete all previously collected .nz WHOIS records in its databases. ER546.

DNCL also moved for a preliminary injunction to bar DomainTools from accessing .nz WHOIS servers (which DomainTools had already stopped accessing on June 14) and to require DomainTools to reconfigure its systems to avoid using previously collected, publicly available .nz WHOIS information in its cybersecurity products. ER2.

The District Court Grants A Preliminary Injunction On DNCL’s Contract-Law Claim

The district court granted a preliminary injunction. ER14. The court rested the injunction solely on DNCL’s breach-of-contract claim. It concluded that DNCL was likely to succeed on its claim that DomainTools had violated provisions of DNCL’s terms of use, specifically the most recent terms of use that prohibit “high volume” queries, accessing the .nz register “in bulk,” “publishing historical or non-current versions of the register data,” and “publishing register data in bulk.” ER3-8. The court acknowledged that so-called “browsewrap” agreements like DNCL’s terms of use are not enforceable unless “the

user has actual or constructive knowledge of the [terms of use].” ER5. In the court’s view, however, DomainTools’ repeat queries established sufficient knowledge. ER7. The court did not address the fact that all those queries were conducted by an automated program on a dedicated computer-to-computer channel acting without human intervention.

Turning to the other preliminary injunction factors, the court held that DNCL had established a likelihood of irreparable harm because some .nz registrants had recently complained that their WHOIS information was publicly available on DNCL’s own website—complaints that then prompted DNCL to create the IRPO. ER8-9. DNCL had not shown that customers knew about DomainTools, complained about DomainTools, or would penalize DNCL for DomainTools’ use of the public data for cybersecurity purposes. And the court acknowledged that DNCL had not shown “that it ever made a promise to registrants that it would retract or otherwise undo past disclosures.” ER8. The court nevertheless concluded that DNCL was “likely to suffer irreparable harm to its business interests if [DomainTools] is not enjoined from using the information stored in its database.” ER9. The court also held that DNCL’s business risk outweighed the hardship on

DomainTools of “scrub[bing] from search results any and all information with a .nz top level domain.” ER11.

With respect to the public interest, the court discounted the effect of an injunction on DomainTools’ customers, including “law enforcement entities.” ER12-13. Ignoring the evidence that cybersecurity investigations depend on correlation *across* data sets, the court noted that “[t]he .nz register is comparatively small” and posited that law enforcement could conduct one-by-one manual queries on DNCL’s website. ER13.

Based on this reasoning, the court enjoined DomainTools from “accessing the .nz register while DomainTools’ limited license remains revoked and/or publishing any .nz register data DomainTools had stored or compiled in its own databases.” ER14.

DomainTools timely appealed. ER77.³

³ DNCL has since filed a first amended complaint. *See* ER15-42. The amended complaint makes only minor stylistic edits to the allegations on DNCL’s breach-of-contract claim and does not affect either the preliminary injunction or this appeal.

SUMMARY OF THE ARGUMENT

The district court abused its discretion in issuing a mandatory preliminary injunction.

I. DNCL will not be able to succeed on the merits of its contract-law claim for two reasons. First, DNCL has not shown that it is likely to prove the existence of a valid contract between the parties. DNCL's terms of use are a "browsewrap" agreement—a type of agreement that purports to be binding even absent any affirmative manifestation of assent (like clicking an "I agree" button). Browsewrap agreements are unenforceable unless the defendant admits actual knowledge of the terms of the agreement or the terms are conspicuous enough to put users on inquiry notice. *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176-79 (9th Cir. 2014). But here, DomainTools has not admitted any knowledge and the terms were transmitted only over Port 43—a computer-to-computer channel. The district court erred in relying on *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004), a case involving a defendant with admitted, actual knowledge of terms of use—the very basis on which this Court already distinguished that case in *Nguyen*. Absent any indication that Washington would extend its

law of contract formation to sweep in such tenuous “agreements,” DNCL cannot show a likelihood of success on the merits.

Second, even if the terms of use were enforceable, DNCL has little chance of proving that DomainTools breached them. DNCL reads its terms to bar the use of Port 43 for its intended purpose (computer-generated queries) and to bar the use of WHOIS information for its traditional purpose (publicly identifying domain name registrants). That is not how any consumers of WHOIS information would understand the terms to apply. Instead, read more naturally, they prohibit only extremely high-frequency searches that would clog the channel and disrupt others’ access, as well as publication of WHOIS information for improper purposes like selling the data to commercial solicitors wishing to target registrants with advertising. At a minimum, the terms lack the clarity required for *injunctive* relief under both Washington contract law and federal procedural law.

II. DNCL also failed to establish that it would suffer irreparable harm absent an injunction. The presumptive remedy for breach of contract is money damages, not injunctive relief. And DNCL has not come close to showing why any business injury it might eventually

prove could not be remedied by damages. Moreover, no “concrete evidence in the record” supports DNCL’s claim that DomainTools is causing it any injury at all. *adidas Am., Inc. v. Skechers USA Inc.*, 890 F.3d 747, 756 (9th Cir. 2018). The only evidence DNCL submitted involved a few complaints about the fact that *DNCL* was making WHOIS information fully public—something DNCL has since addressed with its IRPO offering and by ceasing to publish *any* individual registrant data via Port 43. Those complaints are not relevant to DomainTools: DNCL pointed to no existing or prospective registrant who complained about DomainTools specifically, nor about the dozens of other third-party services that access .nz WHOIS information, nor about any cybersecurity specialists’ use of historical, publicly available WHOIS information.

III. Any harm to DNCL is significantly outweighed by the harm an injunction poses to the public interest and to DomainTools.

DomainTools is a critical cybersecurity partner to law enforcement as well as to businesses responsible for protecting customer data and user privacy. Disabling DomainTools’ ability to make use of already-public WHOIS information provides scant (if any) benefit to registrant privacy,

while impairing DomainTools' ability to engage in the correlation and attribution analyses that help keep the internet safe for all users.

STANDARD OF REVIEW

This Court reviews a decision granting a preliminary injunction for abuse of discretion. *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011). A district court abuses its discretion if its decision rests on an erroneous legal standard or “resulted from a factual finding that was illogical, implausible, or without support in inferences that may be drawn from the facts in the record.” *Herb Reed Enters., LLC v. Fla. Entm't Mgmt., Inc.*, 736 F.3d 1239, 1247, 1250 (9th Cir. 2013) (finding an abuse of discretion and reversing a preliminary injunction where the district court “rel[ied] on unsupported and conclusory statements regarding harm [the plaintiff] might suffer”) (internal quotation marks omitted). A court's “legal conclusions” are reviewed de novo. *adidas*, 890 F.3d at 753.

In considering whether a district court abused its discretion, this Court examines the district court's application of the preliminary injunction standard: “A plaintiff ... must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the

absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest.” *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008).

Where an injunction is a “mandatory injunction” that requires affirmative action rather than merely preserving the status quo, however, this Court applies a more exacting standard: It asks whether the plaintiff “establish[ed] that the law and facts *clearly favor* [its] position, not simply that [it] is likely to succeed.” *Garcia v. Google, Inc.*, 786 F.3d 733, 740 (9th Cir. 2015) (en banc). That is because mandatory injunctions are “particularly disfavored.” *Stanley v. Univ. of S. Cal.*, 13 F.3d 1313, 1320 (9th Cir. 1994). That higher standard applies here because, as the district court recognized, its injunction is a mandatory one, ER3: It requires DomainTools to take affirmative action to remove the .nz WHOIS information that is already in its databases from the tools and services it currently offers customers. ER14.

ARGUMENT

I. DNCL's Contract Claim Lacks Merit.

A. There was no mutual assent to DNCL's "browsewrap" terms of use.

"While new commerce on the Internet has exposed courts to many new situations, it has not fundamentally changed the principles of contract." *Nguyen*, 763 F.3d at 1175 (internal quotation marks omitted). "Mutual manifestation of assent" remains the "touchstone." *Id.* (internal quotation marks omitted). In the 21st century as in the 18th, no contract is formed unless (1) the offeror "provide[s] reasonable notice" of the proposed terms, and (2) the offeree "unambiguously manifest[s] assent" to those terms. *Id.* at 1173.

DNCL argues that DomainTools is bound by the terms of use because those terms were appended to the results of WHOIS queries made via Port 43. But DNCL's system gave users no opportunity to review the terms prior to using the WHOIS service or to provide assent, such as by clicking an "I agree" box. Moreover, there is no reason to believe DomainTools should have been on notice of the terms (much less the newer, June 2016 version) since they were ultimately communicated through a channel used for automated queries. The

district court made an error of law by ignoring these basic principles of contract law, and by wrongly relying on the Second Circuit's *Register.com* decision, a case in which (unlike here) the defendant had admitted actual knowledge of the website's terms of use.

1. “Browsewrap” agreements are generally unenforceable.

As this Court explained in *Nguyen*, online contracting comes in two main “flavors”: “clickwrap” agreements, which are often enforceable, and “browsewrap” agreements, which are often not. 763 F.3d at 1175-76. In a clickwrap agreement, users are first presented with the terms of use and then asked to click on an “I agree” box, as anyone who has signed up for a new online account or updated her smartphone has encountered. Only after clicking “I agree” can users access the website governed by the terms of use. *Id.* Because a user who completes a clickwrap has both actual notice of the terms and has affirmatively assented to those terms, terms presented in a clickwrap style are generally enforceable contracts. *Id.*; see *Nicosia v.*

Amazon.com, Inc., 834 F.3d 220, 233 (2d Cir. 2016) (analyzing online agreements under Washington law).⁴

Browsewrap agreements, in contrast, lack affirmative expressions of assent. In a typical browsewrap agreement, the terms of use are simply posted somewhere on a website. Those terms will “contain a notice that—by merely using the services of, obtaining information from, or initiating applications within the website—the user is agreeing to and is bound by the site’s [terms of use].” *Nguyen*, 763 F.3d at 1176 (internal quotation marks omitted). Because “no affirmative action is required by the website user to agree to the terms of a contract other than his or her use of the website,” such agreements have only been enforced when the offeree has “actual knowledge of the agreement,” or when the website makes the terms and conditions so conspicuous that the website is deemed to put a “reasonably prudent person on inquiry notice.” *Id.* at 1176-77 (internal quotation marks omitted) (declining to enforce a browsewrap agreement); *Specht v. Netscape Commc’ns Corp.*, 306 F.3d 17, 30-32 (2d Cir. 2002) (Sotomayor, J.) (same); *see also* Mark

⁴ The district court held that Washington law governs. ER3 n.4. For purposes of this appeal, DomainTools assumes without conceding that this is correct.

A. Lemley, *Terms of Use*, 91 Minn. L. Rev. 459, 477 (2006) (“Courts may be willing to overlook the utter absence of assent only when there are reasons to believe that the [website user] is aware of the [website owner’s] terms.”).

Accordingly, where “there is no evidence that the website user had actual notice of the agreement”—and DNCL offered none below—“the validity of the browsewrap agreement turns on” an assessment of the “design and content of the website.” *Nguyen*, 763 F.3d at 1177. In *Specht*, for instance, the Second Circuit declined to enforce a browsewrap contract where users had to scroll to the bottom of the screen to see the hyperlink leading to the terms of use. 306 F.3d at 20. “[A] reference to the existence of license terms on a submerged screen,” the court explained, “is not sufficient to place consumers on inquiry or constructive notice of those terms.” *Id.* at 32.

In *Nguyen*, this Court approved of *Specht* and went even further. Even though a blue, underlined, “Terms of Use” hyperlink appeared at the bottom of every screen, “directly below the relevant button a user must click on to proceed,” this Court found the notice insufficient because the website did not explicitly direct users to review the terms.

763 F.3d at 1178-79. This Court affirmed that “the onus must be on website owners to put users on notice of the terms to which they wish to bind consumers.” *Id.* at 1179; *see also Kwan v. Clearwire Corp.*, No. C09-1392JLR, 2012 WL 32380, at *9 (W.D. Wash. Jan. 3, 2012) (applying Washington law).

2. Terms sent solely via a computer-to-computer channel not designed for human consumption do not provide adequate notice.

Here, the terms of use were even more hidden than those in *Nguyen*. Because “DomainTools acquired WHOIS data only from DNCL’s Port 43 service,” ER222—not from DNCL’s website—the terms were only communicated in “comment lines” prefaced with a percentage sign that indicated that the receiving computer could ignore the text. *See supra* 29-30. In this way, DNCL specifically designed the response to help the querying computer take *no* action with the terms of use (rather than alerting human users to their presence).⁵

⁵ Indeed, .nz’s own WHOIS documentation provides expressly that comments sent over Port 43 like the terms of use “need not be decoded by a program interacting with the whois server.” InternetNZ, *Whois Protocol*, <https://docs.internetnz.nz/whois/> (last visited Dec. 5, 2018).

This mode of transmitting terms, standing alone, cannot be enough to put users of the Port 43 service on inquiry notice. As noted above (at 16), Port 43 is a dedicated channel for WHOIS data communications. ER222. While it is technically possible for a human being to access Port 43 through a “command-line-interface” on his or her computer, Port 43 is most “commonly used today for automated machine WHOIS queries.” ER222. If “the onus [is] on website owners to put users on notice of the terms,” *Nguyen*, 763 F.3d at 1179, DNCL cannot have provided sufficient notice by placing human-readable text in a response sent via a channel for computer inquiries that it knows no human beings are likely to see.

Indeed, holding that a contract was formed because a computer received text it could not interpret would be like holding that a contract was formed where, at the end of a fax transmission, a recording of a human voice declared in English (and thus unintelligibly to the fax machine) what could and could not be done with the document just faxed. Under Washington contract law, there is no mutual assent if a party is “deprived of the opportunity to read the contract” or “would not have been capable of understanding [the contract] if they had read it.”

Yakima Cty. (W. Valley) Fire Prot. Dist. No. 12 v. City of Yakima, 122 Wash. 2d 371, 389 (1993); *see also In re Marriage of Obaidi & Qayoum*, 154 Wash. App. 609, 617 (2010) (no mutual assent to agreement written in a language one party did not understand).

This contracting situation is contemplated by the Uniform Computer Information Transactions Act (UCITA), a model code “resembling UCC Article 2 in many respects but drafted to reflect emergent practices in the sale and licensing of computer information.” *Specht*, 306 F.3d at 29 n.13, 34 n.17 (relying on the UCITA as persuasive authority in browsewrap contract case). The UCITA provides that an electronic agent, like a computer gathering information over Port 43, can be deemed to manifest assent to a term by mere continued operation only if that term was presented in such a way “that a reasonably configured electronic agent could react to it.” UCITA § 112 cmt. 3(c). “The capability of an automated system to react and an assessment of the implications of its actions are the only appropriate measures of assent.” *Id.*; *see also* UCITA § 113 cmt. 2. But nothing about DNCL’s Port 43 service was configured to ensure that the terms would trigger a response by an automated program, much less ensure

that the terms would be seen by a human. DNCL could have, for example, programmed its WHOIS service to reject Port 43 inquiries originating from any IP address that had not been preauthorized for access—a “sign-up” process that could have required affirmatively assenting to terms—but it took no such step.

At a minimum, enforcing a browsewrap agreement where the only possible inquiry notice is a transmission to an automated computer program would be a dramatic expansion of Washington contract law to a novel technological context. “Federal courts should ‘hesitate prematurely to extend the law ... in the absence of an indication from the [state] courts or the [state] legislature that such an extension would be desirable.’” *Del Webb Cmtys., Inc. v. Partington*, 652 F.3d 1145, 1154 (9th Cir. 2011) (quoting *Torres v. Goodyear Tire & Rubber Co.*, 867 F.2d 1234, 1238 (9th Cir. 1989)). Here, there is no such indication. To the contrary, even everyday browsewrap agreements remain suspect under Washington law. *See Long v. Live Nation Worldwide, Inc.*, No. C16-1961 TSZ, 2017 WL 5194978, at *3 (W.D. Wash. Nov. 8, 2017) (declining to extend the enforceability of browsewrap or clickwrap agreements to a novel context involving distinct but related websites).

Indeed, where “[t]he consistent trend across the country is toward limiting, not expanding” the enforcement of browsewrap agreements, adopting an “expansive” view of what state law would allow is especially unwarranted. *Del Webb*, 652 F.3d at 1156-57. “Although a federal court exercising diversity jurisdiction is at liberty to predict the future course of a state’s law, plaintiffs choosing the federal forum are not entitled to trailblazing initiatives under state law.” *Cervantes v. Countrywide Home Loans, Inc.*, 656 F.3d 1034, 1043 (9th Cir. 2011) (internal punctuation omitted).

The novel aspects of DNCL’s contract claim at least indicate that its success on the merits is not *likely*. Certainly, “the law and facts” do not so “clearly favor [DNCL’s] position” as to satisfy the “doubly demanding” burden imposed on parties requesting a mandatory injunction. *Garcia*, 786 F.3d at 740.

3. The district court’s analysis was flawed.

The district court’s contrary holding turned on two errors of law.

First, the court relied on *Register.com*, a Second Circuit case enforcing a browsewrap agreement. But the reasoning in *Register.com* is inapplicable here because DomainTools, unlike the defendant in

Register.com, has *not* admitted actual knowledge of DNCL’s terms of use.

In *Register.com*, the defendant, Verio, queried Register’s WHOIS database to collect addresses and phone numbers for use in mass marketing efforts targeted at registrants—conduct that directly harmed Register’s customers. 356 F.3d at 396-97. Register argued that Verio’s conduct violated its terms of service, which prohibited use of the WHOIS data for commercial solicitations. Verio acknowledged that it was fully aware of those terms, but nonetheless argued that it never became contractually bound by them because it never affirmatively assented to the terms (as in a clickwrap agreement). Instead, Verio argued that no contract existed because, “in the case of each query Verio made, the [terms] did not appear until after Verio had submitted the query and received the WHOIS data.” *Id.* at 401.

The Second Circuit rejected this intrepid argument. It explained that a browsewrap agreement can be enforceable when a plaintiff “admits that it knew perfectly well what terms” were imposed, even if the notice was provided only after the query in any given transaction. *Id.* at 401. The court analogized the scenario to a visitor to “a roadside

fruit stand” who eats an apple without paying, then “sees a sign, visible only as one turns to exit, which says ‘Apples—50 cents apiece,’” and then continues claiming ignorance of the requirement to pay on subsequent visits by asserting that “on each occasion” he did not see the sign until after he’d eaten the fruit. *Id.*

The district court thought this case was similar because, like Verio, DomainTools queried DNCL’s WHOIS service repeatedly over a period of years. ER6. But while Verio admitted actual knowledge of Register’s terms of use, DomainTools has not. Nor has DNCL made any showing that DomainTools was *ever* aware of either version of its terms of use, given the hidden way in which the terms were sent. (Indeed, DNCL did not even exist until 2007, ER20, *after* DomainTools set up its automated queries of the .nz WHOIS server, then maintained by InternetNZ.) And DNCL’s inclusion of the percentage signs, which indicate that the computer can disregard the terms of use, serves the opposite purpose of informing Port 43 users that the marked terms are a critical condition of the transaction. This roadside fruit stand’s sign was written in invisible ink.

This Court has already distinguished *Register.com* on just this ground. As noted above (at 45-46), *Nguyen* held that a browsewrap agreement was unenforceable because, *unlike in Register.com*, there was no “evidence in the record that Nguyen had actual notice of the Terms of Use.” 763 F.3d at 1176.

The district court nevertheless found *Register.com* on point because the court simply assumed that DomainTools, like Verio, had actual knowledge. *See* ER6-7. That assumption was improper. It shifted the burden to DomainTools to *disprove* the formation of a contract. But under Washington law, the burden is on DNCL to prove every element of its claim. *Johnson v. Nasi*, 50 Wash. 2d 87, 91 (1957). Indeed, in the district court, *DomainTools* urged the court to allow for limited discovery on issues relevant to the preliminary injunction motion, but *DNCL* resisted any discovery, *see* ER238-40. DNCL should not have been allowed to benefit from having facts assumed in its favor when it both bore the burden of proof and resisted development of the record.

The district court elaborated that there is “significant evidence that [DomainTools] was aware of the [terms of use]” because “[w]hen

[DomainTools] produces .nz register data to its own customers, it excises the [terms of use].” ER6. But no evidence supported that characterization of how DomainTools processes data. And the suggestion that DomainTools is actively reviewing the terms of use when it queries .nz’s WHOIS service and then surreptitiously excising them is simply wrong. Rather, when DomainTools processes WHOIS records, its computer software is pre-programmed to automatically set aside *any* data marked by the WHOIS server with computer code instructing the querying computer to ignore it.

Second, the district court failed to recognize that there is not just one contract at issue. There are at least two. First are the terms of use that existed before June 2016, which prohibited only “[u]sing multiple WHOIS queries ... to enable or effect a download of part or all of the .nz Register.” ER23. Second are the terms that were transmitted with WHOIS information after June 26, 2016. Those terms prohibited sending “high volume” WHOIS queries, storing WHOIS data “to build up a secondary register of information,” and publishing “historical or non-current versions of WHOIS data” or “any WHOIS data in bulk.” ER22-23.

The district court erred by not distinguishing between the two different sets of access and use restrictions. But they must be considered separately, especially before issuing sweeping injunctive relief. Assent to one contract does not indicate assent to the other, because “[p]arties to a contract have no obligation to check the terms on a periodic basis to learn whether they have been changed by the other side.” *Douglas v. U.S. Dist. Court for Cent. Dist. of Cal.*, 495 F.3d 1062, 1066 (9th Cir. 2007); *see also Gaglidari v. Denny’s Rests., Inc.*, 117 Wash. 2d 426, 435 (1991) (holding employee was not bound by unilateral changes to company policy because she did not receive reasonable notice of changes). As a result, even if DomainTools had actual or inquiry notice with respect to the *pre*-June 2016 terms, DNCL must still prove notice of the June 2016 terms, which it has not shown it can do.⁶

⁶ DomainTools does not dispute that it had notice of the terms of use as of a few months before DNCL filed this lawsuit, when DNCL first contacted DomainTools with a demand letter that expressly referenced the terms. ER36. But any resulting contract would govern only information downloaded in the narrow period after that point, and neither DNCL nor the district court has drawn any such distinction into DNCL’s claims.

That is significant because if only one set of terms is enforceable, then only one set of WHOIS information (defined by when DomainTools accessed it) is subject to any contract. *See Long*, 2017 WL 5194978, at *3 (declining to extend a browsewrap agreement beyond the transaction that gave rise to the agreement). But the district court did not tailor its injunction accordingly. Instead, it retroactively applied the June 2016 terms of use to *all* .nz WHOIS information, requiring DomainTools to stop using *all* of it, even though the new terms were in no way attached to the earlier data DNCL transmitted to DomainTools via Port 43. This overbreadth should also weigh against sustaining the injunction.

B. At a minimum, both versions of DNCL’s terms of use are too ambiguous to support injunctive relief.

Even if DomainTools had been on sufficient notice of either version of DNCL’s terms of use, though, DNCL is unlikely to prove they were *breached* because the terms do not apply to DomainTools’ conduct.

“A contract provision is ambiguous when its terms are uncertain or when its terms are capable of being understood as having more than one meaning.” *Mayer v. Pierce Cty. Med. Bureau, Inc.*, 80 Wash. App. 416, 421 (1995). And in Washington, “[w]hen specific performance is sought, rather than legal damages, a higher standard of proof must be

met: ‘clear and unequivocal’ evidence that ‘leaves no doubt as to the terms, character, and existence of the contract.’” *Kruse v. Hemp*, 121 Wash. 2d 715, 722 (1993); *see also Hedges v. Hurd*, 47 Wash. 2d 683, 687-88 (1955) (holding that a seller’s breach justified a damages award, but that the contract was too vague to permit specific performance).

Federal procedural law similarly requires a higher level of clarity before a mandatory injunction can issue. *See supra* 41. Thus, in *Richey v. Metaxpert LLC*, 407 F. App’x 198, 200 (9th Cir. 2010), for example, this Court upheld a denial of preliminary injunctive relief where it was ambiguous whether the scope of a non-compete clause extended to the defendant’s new employment. This Court agreed that, before any mandatory injunction would be appropriate, a more developed record was necessary to establish that the disputed term indeed applied. *Id.*

Similarly here, the pre-June 2016 version’s bar on “[u]sing multiple WHOIS queries, or using the output of multiple WHOIS queries in conjunction with any other facility or service, to enable or effect a download of part or all of the .nz Register” does not clearly apply to DomainTools. ER23. On Port 43, every query results in a download of *some* “part” of the .nz Register, and it cannot be that DNCL

was seeking to prohibit use of the very channel it sent its terms over. The terms are instead read more naturally in connection with the clause that follows: the ban on using WHOIS information “to attempt a targeted contact campaign with any person.” ER23. Indeed, accessing WHOIS information to bombard all registrants with ads for internet services is exactly the harm that Verio imposed on Register and its customers. In other words, DNCL’s terms prohibit the internet equivalent of photocopying an entire phone book and reselling the contact information to telemarketers. The terms say nothing about—and certainly do not prohibit—accessing WHOIS information for its intended internet-safety purposes, which DNCL has itself publicly touted.

Nor do the June 2016 version’s bars on “high volume” queries, publication of “bulk” WHOIS data, and publication of “historical or non-current” WHOIS information clearly apply in this context. ER22-23. These prohibitions appear to bar high-*frequency* searches that could tie up access to Port 43 and block other WHOIS requests, as well as the use of WHOIS data for “mass unsolicited commercial advertising.” ER23. On their face, these terms do not give clear notice that they prohibit

ordinary access to WHOIS information via Port 43, which is specifically designed to enable automated computer queries at significant scale. *See, e.g.*, ER22 (noting that DNCL responds to over 10 million WHOIS queries each month). Nor do they clearly bar the ordinary use of WHOIS information, whose very purpose is to be shared publicly to facilitate the security and stability of the internet.

DNCL's new privacy-centric interpretation of its terms of use is all the more farfetched when viewed against the backdrop of the industry-standard WHOIS protocol, which declares that "WHOIS-based services should only be used for information which is non-sensitive and intended to be accessible to everyone." ER222; ER231. How contract terms are commonly used in the "[t]rade" generally, and in the "course of dealing" between the parties specifically, is "relevant to interpreting a contract and determining the contract's terms." *Puget Sound Fin., LLC v. Unisearch, Inc.*, 146 Wash. 2d 428, 434 (2002); *see, e.g., City of Tacoma v. City of Bonney Lake*, 173 Wash. 2d 584, 591 (2012).

Here, DNCL's revisionist gloss on its terms of use imports novel privacy concepts into them that no one in the field would originally have understood them to include. Even DNCL did not suggest the terms

extended to conduct like DomainTools' until late 2017, when DNCL sought to promote its new IRPO offering. DNCL may adopt unusually stringent protections of WHOIS information, like its near-shuttering of Port 43. *See supra* 32-33. But it may not *retroactively* read those concepts into either its pre-June 2016 or June 2016 terms of use, which speak only of prohibiting "spam"-like use of WHOIS data, not of ordinary uses of this important public information.

Because DNCL has not demonstrated that its terms of use *unambiguously* prohibited DomainTools' conduct, it has not shown that it will clearly be entitled to a permanent mandatory injunction, and so the district court should not have granted preliminary relief.

II. DNCL Failed To Establish Irreparable Harm.

The district court also erred in concluding that DNCL would suffer irreparable harm absent an injunction.

A. DNCL supplied no evidence that DomainTools' use of .nz WHOIS information affects, much less irreparably harms, DNCL's business.

To justify a preliminary injunction, a movant must use "concrete evidence in the record" to show a likely irreparable injury. *adidas*, 890 F.3d at 756. Conclusory or speculative allegations are not enough.

Herb Reed Enterprises, 736 F.3d at 1250. That is doubly true in a contract case, where the presumptive remedy for a breach is money damages, not injunctive relief. *See Crafts v. Pitts*, 161 Wash. 2d 16, 23-24 (2007) (citing Restatement (Second) of Contracts § 360 (1981)).

Because “[m]onetary injury is not normally considered irreparable,” *Fox Broad. Co. v. Dish Network L.L.C.*, 747 F.3d 1060, 1072-73 (9th Cir. 2014) (internal punctuation omitted), this Court has deemed it an abuse of discretion to “grant[] a preliminary injunction on the basis of [a] threatened [economic] injury.” *Los Angeles Mem. Coliseum Comm’n v. Nat’l Football League*, 634 F.2d 1197, 1202 (9th Cir. 1980).

Here, the district court abused its discretion by (1) failing to address why DNCL’s claimed harm is irreparable, (2) crediting DNCL’s speculative allegations of harm, and (3) hypothesizing a connection between the alleged harm and DomainTools’ actions, despite the absence of any “concrete evidence” supporting such a link. *adidas*, 890 F.3d at 756.

First, the harm DNCL alleges is not irreparable. The injury the district court identified—lost business opportunities from privacy-conscious registrants, *see* ER8-10—is one that is classically remedied by

an award of damages. *Los Angeles Mem. Coliseum*, 634 F.2d at 1202. But the district court did not address whether or why “legal remedies, such as money damages, are inadequate” to redress the economic harm of lost or canceled registrations. *Herb Reed Enterprises*, 736 F.3d at 1250. That failure to apply the proper legal standard was itself an abuse of discretion. *Id.*

Second, the “concrete evidence in the record” does not support the district court’s conclusion that DNCL is likely to suffer a loss in business (or any other harm) without an injunction. *adidas*, 890 F.3d at 756. All DNCL has shown is that some consumers were unhappy with DNCL’s previous policy requiring full WHOIS disclosure—complaints addressed only to DNCL, not any third party, and which DNCL has since remedied.

The district court pointed to a handful of comments submitted by registrants and members of the public during DNCL’s review of its then-existing policy of public WHOIS disclosure. ER260-63. These comments did not complain about DomainTools, Port 43, “bulk” queries, or “historical” data. Rather, they argued that *DNCL* should not require registrants to make their data publicly available in the first place—

criticisms that ultimately led DNCL to adopt the IRPO and stop publishing any registrant data over Port 43. ER260-63. And the comments DNCL received—all twelve of them—came in response to DNCL’s request for public submissions on “[w]hy .nz registrant data should/should not be publicly available.” ER320; *see* ER320-38 (reporting additional questions for the public). This limited response hardly establishes that WHOIS privacy has a significant impact on DNCL’s ability to attract and retain registrants.

The only evidence directly linking DNCL’s business prospects to WHOIS availability is a mere five comments indicating that an individual either canceled or decided not to register a .nz domain because of DNCL’s previous policy of full WHOIS disclosure. This Court has held that evidence of such isolated impact is insufficient to show irreparable harm. *Am. Passage Media Corp. v. Cass Commc’ns, Inc.*, 750 F.2d 1470, 1473 (9th Cir. 1985) (“Even if the evidence showed that four advertisers were unwilling to do business with [plaintiff] ... this would be insufficient evidence of irreparable harm.”). Indeed, five lost registrations out of over 710,000 .nz domains cannot demonstrate that DNCL will suffer *irreparable* harm absent an injunction—even if

they were in any way traceable to DomainTools, rather than to DNCL itself.

DNCL's assertions about registrant privacy imperatives are further undercut by the lackluster response to its IRPO privacy program. In the time since DNCL announced the IRPO, about 3.5% of registrants have chosen to withhold their personal information. ER28; ER254. This limited adoption of a free privacy service demonstrates that privacy concerns are not major drivers of DNCL's business. All that DNCL can muster are two "tweets" and two emails expressing support for the IRPO after it was adopted. ER255. None of this indicates that DNCL's business prospects are meaningfully tied to WHOIS privacy issues—especially given that DNCL has a monopoly over .nz domains, so prospective registrants cannot simply take their business across the street. Indeed, DNCL's counsel acknowledged that DNCL had become "more popular now than ever" in the months prior to the issuance of the preliminary injunction, so DomainTools' continued use of .nz registry data was not threatening irreparable harm to DNCL's popularity. ER142.

Third, none of this minimal evidence links DomainTools' specific conduct to any of the harms DNCL fears. That should have been fatal to DNCL's claim of irreparable harm. *See, e.g., Fox Broad. Co.*, 747 F.3d at 1072-73 (finding no irreparable harm where "the harms [the plaintiff] identified—including loss of control over its copyrighted works and loss of advertising revenue—did not flow from the [alleged breach of contract and copyright infringement]" (internal quotation marks omitted)).

The district court opined that "[t]he evidence shows that the publication of personal data has affected consumer choice in the past, and it is no leap to conclude that, if ... defendant continues to publish the information it collected over the years, the disclosures will continue to adversely impact plaintiff's ability to obtain and retain registrants." ER10. But that *is* a leap, and no evidence supports it. The evidence shows, at best, that *DNCL's former policy* of requiring public disclosure of WHOIS information had some minute effect on customer choice. And, as noted above, DNCL has now changed its own approach. But none of the comments mention collection or publication of WHOIS information by DomainTools or any of the many other companies that

collect and publish historical WHOIS information. Nor do they tie a third party's use of .nz WHOIS information for legitimate security purposes to a registrant's decision to forego a .nz domain. Only speculation supports DNCL's theory.

This stands in contrast to *Register.com*, in which Verio used the WHOIS data it collected to send solicitations to Register's customers and "made explicit reference to their recent registration through Register." *Register.com*, 356 F.3d at 397. Register then began to receive complaints from "the recipients of Verio's solicitations," who mistakenly "believe[d] the solicitation was initiated by Register." *Id.* Here, there is no indication that DNCL's customers even know about DomainTools, much less that they have misattributed DomainTools' actions to DNCL. There is also no support for the idea that registrants will think less of DNCL if it is unable to demand deletion of data it previously made public—nor is DNCL's desire to put the genie back in the bottle an appropriate basis for a preliminary injunction.

DNCL further posited (and the district court accepted) that DNCL's "ability to attract and retain registrants" relies on its ability to "respond[] adequately to the market demand for more privacy." ER9.

In the district court’s view, DomainTools is “sabotaging” DNCL’s efforts to provide improved privacy protection (such as through its IRPO offering) by continuing to use the .nz WHOIS records that DNCL made available online over the past decade. ER9. The court thought this would cause irreparable harm to DNCL’s “customer base and business prospects” because it prevents DNCL from “provid[ing] the privacy upgrades the market is demanding.” ER8.

But DNCL did not show, and the district court certainly did not explain, how DomainTools’ conduct in any way prevents DNCL from implementing the IRPO or limits DNCL’s “ability to attract and retain registrants.” ER9. And more fundamentally, it makes no sense to say that use of the already-public, pre-IRPO data that DNCL broadcast to the world would compromise the demand for privacy protections on *new*, not-yet-disclosed WHOIS information—particularly where DNCL made no promises to the public that the IRPO would “claw back” previously published data. Moreover, now that DNCL has cut off DomainTools’ *prospective* access to .nz WHOIS information, there is no basis for assuming that, going forward, individuals will decline to pursue and secure .nz domains because of anything to do with DomainTools.

Finally, the fact that DNCL waited over a year to raise the WHOIS access issue with DomainTools indicates that DomainTools' actions did not actually pose any imminent threat. While not determinative, delay by the party seeking relief is highly "relevant in determining whether relief is truly necessary." *Miller v. Cal. Pac. Med. Ctr.*, 991 F.2d 536, 544 (9th Cir. 1993).

B. The district court's irreparable harm determination is inconsistent with this Court's case law.

The lack of concrete evidence tying DomainTools to any future harm is reason enough to reverse the preliminary injunction, as *adidas*, *Herb Reed Enterprises*, and *Titaness Light Shop, LLC v. Sunlight Supply, Inc.*, 585 F. App'x 390, 391 (9th Cir. 2014), all show.

In *adidas*, the district court had granted adidas a preliminary injunction against a competitor, Skechers, that was selling a similar-looking shoe. 890 F.3d at 756. The alleged irreparable harm was that consumers would think less of adidas if they saw people wearing Skechers's lookalike shoe because "adidas is viewed by consumers as a premium brand while Skechers is viewed as a lower-quality, discount brand." *Id.* at 759. But "adidas did not set forth evidence probative of Skechers's allegedly less favorable reputation" and did not present

evidence showing that consumers would “associate [Skechers’s allegedly] lesser-quality products with adidas.” *Id.* at 759-60. This Court therefore reversed the preliminary injunction, noting that it was improper to “assume that [confusion between products] will cause adidas irreparable harm where, as here, adidas has failed to provide concrete evidence that it will.” *Id.* at 761.

Similarly, in *Titaness Light Shop, LLC v. Sunlight Supply, Inc.*, 585 F. App’x 390, 391 (9th Cir. 2014), this Court reversed a preliminary injunction premised on a claim of irreparable reputational harm. The movant, Sunlight, argued that Titaness Light Shop was selling similarly named products on a website that catered to marijuana growers. But this Court concluded that there was no *concrete* evidence establishing that “Sunlight’s customers [were] aware of the website, would associate the products on the site with marijuana, or would stop purchasing Sunlight products if they mistakenly believed that Sunlight was marketing to marijuana growers.” *Id.* Stressing the high bar a party seeking a preliminary injunction must meet, this Court concluded that “[t]he fact that Sunlight’s reputation *might* be harmed by the

marketing of TLS's products did not establish that irreparable harm to Sunlight's reputation is *likely*." *Id.*

And in *Herb Reed Enterprises*, the district court's reliance on "platitudes" about the harms of trademark infringement and on pure "speculation on future harm" was an abuse of discretion; where the plaintiff fails to "proffer evidence sufficient to establish a likelihood of irreparable harm," a preliminary injunction is improper. 736 F.3d at 1250-51. There, as here, "[t]he district court's analysis of irreparable harm [was] cursory and conclusory, rather than being grounded in any evidence." *Id.* at 1250.

Because DNCL put forward no concrete evidence showing that DomainTools causes it irreparable harm or that money damages would not remedy any injury it can ultimately prove, reversal is warranted here too.

III. Any Harm To DNCL Is Significantly Outweighed By The Harm An Injunction Poses To The Public Interest And DomainTools.

In contrast to the speculative harms DNCL asserts, the harm to DomainTools' customers, including national law enforcement agencies, is immediate and significant. "Courts of equity should pay particular

regard for the public consequences in employing the extraordinary remedy of injunction,” all the more so where “the preliminary injunction would impose [a burden] on the public interest in national defense.” *Winter*, 555 U.S. at 24 (internal quotation marks omitted) (vacating a preliminary injunction).

As is explained more fully in the Statement above (at 18-25), DomainTools enhances security on the internet because it supplies law enforcement and security researchers with the tools and resources they need to analyze and cross-reference a large set of WHOIS data. Working with a comprehensive and up-to-date roster of domain name information enables law enforcement to quickly and effectively draw connections between criminal activities across the internet and going back in time.

That ability to correlate WHOIS information with data about previous attacks has allowed cybersecurity professionals to respond to everything from individual phishing schemes to sophisticated cyberattacks on nation-states. *See supra* 23-24. In yet another example, the ability to track historical WHOIS information across many domains allowed one security expert to identify the hacker behind the

2013 Target data breach that resulted in the disclosure of millions of credit card numbers. ER194.

So, although .nz is only a small corner of the internet, lifting those records out of DomainTools' database risks undermining the ability of investigators to trace bad actors elsewhere. A .nz WHOIS record could be the missing piece that allows law enforcement to connect two separate attacks or to attribute a different domain name to a particular individual.

It is for this reason that the United States government has taken a strong stance on maintaining comprehensive, open access to WHOIS information. *See supra* 18. The head of the National Telecommunications and Information Administration recently emphasized, for example, that “WHOIS is a vital tool for cybersecurity, law enforcement, consumer protection and the enforcement of intellectual property rights.” Remarks of Assistant Secretary Redl at ICANN 63 (Oct. 22, 2018), <https://www.ntia.doc.gov/speechttestimony/2018/remarks-assistant-secretary-redl-icann-63>. Earlier this year, he similarly cautioned that “[t]he United States will not accept a situation in which WHOIS

information is not available or is so difficult to gain access to that it becomes useless for the legitimate purposes that are critical to the ongoing stability and security of the Internet.” Remarks of Assistant Secretary Redl at ICANN 61 (March 12, 2018), <https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61>.

This position is shared by Europol, the European Union’s lead law enforcement agency, which has specifically emphasized the importance of using “correlation” techniques with WHOIS information (*see supra* 19): “The idea of linking those registered domains [is] hugely important” to fighting cybercrime (including “serious organized crime, child abuse, high-level IP crime and money laundering”) and to Europol’s “counterterrorism” efforts. *Thematic Challenges in the IG Ecosystem: Cybercrime, Data Protection and Privacy*, ICANN63 (Oct. 22, 2018), at 18:35, <https://63.schedule.icann.org/meetings/901615> (providing link to audio). That is why “WHOIS is the starting point for most of [Europol’s] investigations.” *Id.*

The district court thus missed the mark when it suggested that barring use of .nz records would not create a cybersecurity risk because

“[DomainTools] and its customers can access the registration information directly through [DNCL’s] website if it appears that a bad actor is using an .nz domain.” ER13. One-off lookups are only effective if you know which of the roughly 330 million existing domain names to search for. ER20. And if law enforcement cannot cross-reference .nz WHOIS information with WHOIS information from other top-level domains, they have no way of knowing which .nz domains, if any, might merit a closer look. *See supra* 19, 22-24. To say that one-by-one manual lookups provide an adequate substitute for those trying to respond rapidly to cyberattacks is to simply misunderstand how this critical investigative tool works.

The harm to private organizations is also stark. In connection with ICANN’s own study of limiting access to WHOIS information, the U.S. Chamber of Commerce has explained that a public WHOIS system “allows access to critical information that helps identify and address malicious or fraudulent online activity, such as finding and taking down websites that are involved in cyber theft or sell counterfeit goods that could risk the health and safety of consumers.” U.S. Chamber of Commerce, *ICANN WHOIS Database and GDPR* (June 19, 2018),

<https://www.uschamber.com/letter/USCC-ICANN-WHOIS>. WHOIS information also protects the public interest by allowing companies to combat “online scams,” “online piracy and counterfeiting,” “online sale of dangerous counterfeit medications,” “phishing, malware, ransomware, identity theft,” “distributed denial of service attacks, bot nets, data breaches,” and “trafficking of child abuse images.” *Id.*

Even more pressingly, the district court’s order lays the groundwork for other registries and registrars around the world to thwart law enforcement and security professionals’ collection, storage, and use of WHOIS information for investigations—despite the crucial and historical availability of such information. The Department of Commerce recognized the possibility of this trend in its own recent letter to ICANN, explaining that each new registrar or registry that limits WHOIS access or masks WHOIS information “compound[s] the problems these actions create.” Letter from Assistant Secretary of Commerce David J. Redl to Cherine Chalaby, Chair, ICANN Board of Directors (Apr. 16, 2018),

https://www.ntia.doc.gov/files/ntia/publications/redl_to_icann_on_registrar_issues_april_2018_1.pdf. While all gaps in knowledge of WHOIS

information create some risk, more gaps and bigger gaps make the problem exponentially worse.

Requiring DomainTools to stop use of all .nz register data—including data collected before DNCL’s terms of use changed and before the IRPO was even proposed—has virtually no countervailing benefits for registrant privacy. It will not undo the fact that DNCL made the information public in the first place, and it will not erase that information from the internet. It will simply impair an important cybersecurity tool used to protect the privacy of all internet users.

CONCLUSION

The district court's order granting a preliminary injunction should be reversed.

Respectfully submitted,

s/Brian P. Goldman

Aravind Swaminathan
ORRICK, HERRINGTON &
SUTCLIFFE LLP
701 Fifth Avenue, Suite 5600
Seattle, WA 98104

Brian P. Goldman
ORRICK, HERRINGTON &
SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105
(415) 773-5700

Marc R. Shapiro
Abigail Colella
ORRICK, HERRINGTON &
SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019

Counsel for Defendant-Appellant

December 7, 2018

**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

Form 17. Statement of Related Cases Pursuant to Circuit Rule 28-2.6

Instructions for this form: <http://www.ca9.uscourts.gov/forms/form17instructions.pdf>

9th Cir. Case Number(s) 18-35850

The undersigned attorney or self-represented party states the following:

I am unaware of any related cases currently pending in this court.

I am unaware of any related cases currently pending in this court other than the case(s) identified in the initial brief(s) filed by the other party or parties.

I am aware of one or more related cases currently pending in this court. The case number and name of each related case and its relationship to this case are:

Signature s/Brian P. Goldman **Date** Dec. 7, 2018
(use "s/[typed name]" to sign electronically-filed documents)

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: <http://www.ca9.uscourts.gov/forms/form08instructions.pdf>

9th Cir. Case Number(s) 18-35850

I am the attorney or self-represented party.

This brief contains **13666** words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief (*select only one*):

[X] complies with the word limit of Cir. R. 32-1.

[] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[] complies with the longer length limit permitted by Cir. R. 32-2(b) because (*select only one*):

[] it is a joint brief submitted by separately represented parties;

[] a party or parties are filing a single brief in response to multiple briefs; or

[] a party or parties are filing a single brief in response to a longer joint brief.

[] complies with the length limit designated by court order dated _____.

[] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/Brian P. Goldman Date Dec. 7, 2018
(use "s/[typed name]" to sign electronically-filed documents)