

73391-5

73391-5

No. 73391-5-I

DIVISION I, COURT OF APPEALS
OF THE STATE OF WASHINGTON

THE REPUBLIC OF KAZAKHSTAN,

Plaintiff/Respondent

v.

DOES 1-100, inclusive,

Defendants

v.

LLC MEDIA-CONSULT,

Third-Party/Appellant

ON APPEAL FROM KING COUNTY SUPERIOR COURT
(Hon. Mariane C. Spearman)

BRIEF OF RESPONDENT

Ryan P. McBride, WSBA 33280
Abraham K. Lorber, WSBA 40668
LANE POWELL PC
1420 Fifth Avenue, Suite 4200
Seattle, WA 98111-9402
Tel: 206.223.7000
Fax: 206.223.7107

Robert N. Phillips, CASBN 120970
Pro Hac Vice
David J. de Jesus, CASBN 260716
Pro Hac Vice
REED SMITH LLP
101 Second Street, Suite 1800
San Francisco, CA 94105
Tel: 415.543.8700
Fax: 415.391.8269

FILED
COURT OF APPEALS DIV 1
STATE OF WASHINGTON
2015 AUG 10 9 AM 2:42

Attorneys for Respondent The Republic of Kazakhstan

ORIGINAL

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. COUNTERSTATEMENT OF THE ISSUES	5
III. COUNTERSTATEMENT OF THE CASE.....	5
A. 2012-2014: After An English Court Finds That Mukhtar Ablyazov Committed Multi-Billion Dollar Fraud Against A Kazakh Bank, He Is Arrested In France And Faces Extradition; Attorneys And Government Authorities Find Their Emails And Text Messages Hacked	5
B. 2015: Email Accounts Of Senior Officials In Kazakhstan’s Ministry Of Justice Are Hacked; Privileged And Sensitive Documents, Including Documents Related To Ablyazov, Are Stolen And Posted Online; Kazakhstan Turns To U.S. Courts To Help Identify The Hackers	8
C. LMC Moves To Quash Under Washington’s Shield Laws, Claiming The Subpoena Sought Information About LMC’s Confidential Sources; The Trial Court Denies The Motion.	11
D. LMC Appears In The New York Action To Challenge The Preliminary Injunction And Claims That It Obtained The Stolen Materials From A Public Website.	15
IV. ARGUMENT.....	17
A. Standard Of Review	17
B. LMC’s “Claim-Splitting” Argument Was Not Raised Below And Is Wrong In Any Event.....	18
C. LMC Did Not And Cannot Show That Washington’s Shield Law Applies.....	22
1. LMC Has The Prima Facie Burden Of Establishing The Shield Law Applies.....	22

2.	RCW 5.68.010(1) Does Not Apply Because The Subpoena Is Not Directed At A Media Entity.....	24
3.	RCW 5.68.010(3) Does Not Apply Because Kazakhstan’s Subpoena Does Not Directly Or Indirectly Seek Identification Of A Confidential Source	25
a.	LMC Did Not And Cannot Meet Its Prima Facie Burden Of Showing The Statute Applies	25
b.	LMC’s Arguments Lack Merit	33
D.	The Subpoena Is Not Burdensome Or Oppressive	38
V.	CONCLUSION	45

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Brown Bag Software v. Symantec Corp.</i> , 960 F.2d 1465 (9th Cir. 1992)	39
<i>Bruno & Stillman, Inc. v. Globe Newspaper Co.</i> , 633 F.2d 583 (1st Cir. 1980).....	23
<i>Cabell v. Zorro Prods., Inc.</i> , 294 F.R.D. 604 (W.D. Wash. 2013)	39
<i>Clampitt v. Thurston Cnty.</i> , 98 Wn.2d 641, 658 P.2d 641 (1983).....	28
<i>Cont'l Cablevision, Inc. v. Storer Broadcasting Co.</i> , 583 F. Supp. 427 (D.C. Mo. 1984)	32
<i>Davis v. Cox</i> , 180 Wn. App. 514, 325 P.3d 255 (2014) (reversed, 183 Wn.2d 269, 351 P.3d 862 (2015)).....	27
<i>Ensley v. Pitcher</i> , 152 Wn. App. 891, 222 P.3d 99 (2009)	20, 21
<i>Eugster v. City of Spokane</i> , 121 Wn.App. 799, 91 P.3d 117 (2004).....	22
<i>Fellows v. Moynihan</i> , 175 Wn.2d 641, 285 P.3d 864 (2012).....	22
<i>Guillen v. Pierce Cty.</i> , 144 Wn.2d 696 31 P.3d 628 (2001).....	22
<i>Hisle v. Todd Pacific Shipyards Corp.</i> , 151 Wn.2d 853, 93 P.3d 108 (2004).....	20, 21
<i>Howell v. Spokane & Inland Empire Blood Bank</i> , 117 Wn.2d 619, 818 P.2d 1056 (1991).....	42, 43

<i>In re Application of the United States of America for an Order Pursuant to 18 U.S.C. §2703(d),</i> 830 F. Supp. 2d 114 (2011)	34
<i>In re Indiana Newspapers Inc.,</i> 963 N.E.2d 534 (Ind. App. 2012)	27
<i>In re Madden,</i> 151 F.3d 125 (3d Cir. 1998).....	23
<i>In re Michael G. Venezia,</i> 922 A.2d 1263 (N.J. 2007).....	33
<i>Karlberg. v. Otten,</i> 167 Wn. App. 522, 280 P.3d 1123 (2012)	20
<i>King v. Olympic Pipeline Co.,</i> 104 Wn.App. 338, 16 P.3d 45 (2000).....	38, 39
<i>Landry v. Luscher,</i> 95 Wn. App. 779, 976 P.2d 1274 (1999).....	20
<i>New York Times v. Gonzales,</i> 459 F.3d 160 (2d Cir. 2006).....	35
<i>Pierce County, Wash. v. Guillen,</i> 535 U.S. 1033 (2002).....	22
<i>Pierce v. San Mateo Cty. Sherriff's Dep't.,</i> 232 Cal. App. 4th 995 (2014)	40
<i>Rhinehart v. Seattle Times,</i> 98 Wn.2d 226, 654 P.3d 673 (1982).....	39
<i>Senear v. Daily Journal Am.,</i> 27 Wn. App. 454, 618 P.2d 536 (1980)	28
<i>Smith v. Maryland,</i> 442 U.S. 735, 99 S. Ct. 2577 (1979).....	34

<i>Snedigar v. Hoddersen</i> , 53 Wn. App. 476, 768 P.2d 1 (1989) (affirmed in part and reversed in part on other grounds, 114 Wn.2d 153, 170, 786 P.2d 781 (1990))	23
<i>Soter v. Cowles Publ'g Co.</i> , 162 Wn.2d 716, 174 P.3d 60 (2007)	22
<i>State v. Delgado</i> , 148 Wn.2d 723, 733, 63 P.3d 792 (2003)	35
<i>State v. J.P.</i> , 149 Wn.2d 444, 69 P.3d 318 (2003)	34
<i>State v. Lewis</i> , 115 Wn.2d 294, 298–99, 797 P.2d 1141 (1990)	18
<i>State v. Rinaldo</i> , 102 Wn.2d 749, 689 P.2d 392 (1984)	28, 38
<i>State v. Rinaldo</i> , 36 Wn. App. 86, 673 P.2d 614 (1983)	37, 44
<i>T.S. v. Boy Scouts of Am.</i> , 157 Wn.2d 416, 138 P.3d 1053 (2006)	17
<i>U.S. v. Hively</i> , 202 F. Supp. 2d 886 (E.D. Ark. 2002)	31
<i>U.S. v. Sterling</i> , 724 F.3d 482 (4th Cir. 2013)	27
<i>United States v. Miller</i> , 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976)	34
Statutes	
10 Del. Code Ann. Tit 10, § 4320(5)	29
735 Ill. Comp. Stat. § 8-902(c)	29
Cal. Civ. Proc. Code § 474	40

Conn. Gen. Stat § 52-146t.....	27
Me. Rev. Stat. Ann. tit. 16, § 61(3).....	27
Mich. Comp. Laws Ann. § 767.5a.....	29
Wash. Rev. Code § 5.51.020.....	19
Wash. Rev. Code § 5.51.050.....	19
Wash. Rev. Code § 5.68.010.....	24, 25, 35
Wash. Rev. Code § 5.68.010(1).....	24, 25
Wash. Rev. Code § 5.68.010(1)(a)	26
Wash. Rev. Code § 5.68.010(1)(b)	27
Wash. Rev. Code § 5.68.010(3).....	24, 25

Other Authorities

Adam L. Penenberg, <i>NYU Journalism Handbook for Students</i> at http://journalism.nyu.edu/assets/PageSpecificFiles/Ethics/ NYU-Journalism-Handbook-for-Students.pdf	28
<i>Confidential Source</i> , Black’s Law Dictionary (10th ed. 2014)	28
<i>Informant</i> , Black’s Law Dictionary (10th ed. 2014).....	29
<i>The Wall Street Journal Glossary of Terms: Journalism</i> at http://info.wsj.com/college/glossary/journalism.pdf	27

Legislative History

Laws of 2007, ch. 196, H.B. 1366, Final Bill Report, eff. July 22, 2007.....	26, 27
Laws of 2012, ch. 95, H.B. 2195, Final Bill Report, eff. June 7, 2012	19

I. INTRODUCTION¹

This case is not about muzzling the press. It is not about protecting journalists' confidential sources or suppressing political opposition. This case is about a third-party document subpoena issued to a domain name registrar—a company that manages website names—asking for information about who registered the website www.respublika-kaz.info. And that is all this case is about.

The website in question is one of several websites that posted attorney-client privileged and highly sensitive documents, which someone stole by hacking into the email accounts of numerous senior officials in Kazakhstan's Ministry of Justice. Kazakhstan suspected the theft and publication of these materials were traceable to supporters of a Kazakh national named Mukhtar Ablyazov, who was found liable in England of defrauding a Kazakh bank of billions of dollars and currently sits in a French jail awaiting extradition based on that fraud. To assist in identifying the hackers, Kazakhstan filed suit in California state court and then obtained the subpoena in Washington.

LMC, which operated the website, sought to quash the subpoena under the Shield Law, claiming the website was the online version of the

¹ We refer to appellant LLC-Media Consult as "LMC" and respondent The Republic of Kazakhstan as "Kazakhstan".

newspaper Respublika and the subpoena sought confidential journalist sources. LMC also claimed that the subpoena was unduly burdensome and oppressive because Kazakhstan would use the information received to target opposition journalists. Not coincidentally, LMC's owner was one of Ablyazov's principal supporters and Kazakhstan suspected she was working on Ablyazov's behalf to disseminate the stolen materials in order to detract from the fact that Ablyazov had been found liable for multi-billion dollar fraud.

At any rate, the trial court ruled that the Shield Law did not apply because Kazakhstan's subpoena did not seek journalistic sources. At Kazakhstan's suggestion, the trial court limited the scope of the subpoena to exclude financial and billing information, as well as information regarding the website's privacy technology. Also at Kazakhstan's suggestion, the trial court limited production of any documents to attorneys' eyes only—meaning that Kazakhstan's attorneys were not allowed to share with Kazakhstan information produced in response to the subpoena. This ruling was not an abuse of discretion.

As a threshold matter, LMC failed to meet its prima facie burden of proving that the Shield Law applies. Again, Kazakhstan's subpoena sought information regarding the person (called a "domain name registrant") who registered the name of the website in question. And yet,

LMC never explained how that person was a confidential source of news or otherwise provided the stolen materials to Respublika’s journalists. On appeal, LMC says only that *Respublika* “may have” received the stolen materials from the hacker or that *Respublika* “may have” received them from intermediaries who received them from the hacker. But how Respublika received the information is a complete red herring—the question is whether Respublika established that the *domain name registrant* is the confidential source. It failed to do so.

But there is more. After the trial court issued its order, and right before LMC filed its opening brief, Respublika specially appeared in a parallel New York federal court proceeding regarding the stolen materials and stated that it acquired them “the same way the rest of the world did”—from one of the other websites that posted the stolen materials.² So putting aside that LMC never explained to Washington’s courts how the domain registrant was a confidential source, Respublika has told a different court that its journalists *did not receive the stolen materials from a confidential source at all*—they simply pulled them from another

² Concurrently with this respondent’s brief, Kazakhstan has filed a motion requesting that the Court consider evidence of LMC’s representations in the federal court proceeding that were made after the trial court denied its motion to quash in this case.

publicly-available third-party website. Under the circumstances, the trial court committed no error.

The trial court also deftly handled LMC's accusations that Kazakhstan's subpoena was intended to target opposition journalists—accusations that Kazakhstan denied. In addition to recognizing that the subpoena was for the limited purpose of identifying a domain name registrant, the trial court narrowed the subpoena's scope in critical respects. It precluded Kazakhstan from receiving the domain name registrant's financial information or information regarding the website's privacy protection service. And most critically, the trial court ordered that Kazakhstan's attorneys could not share with Kazakhstan information produced in response to the subpoena. In this way, the trial court properly balanced Kazakhstan's discovery needs with LMC's stated concerns. That is the hallmark of any good discovery order.

LMC's opening brief reads like a political manifesto, but settling disputes over Kazakhstan's internal politics is far beyond the scope of this narrow discovery proceeding. The issue is whether a third-party subpoena regarding the identity of a domain name registrant runs afoul of discovery limits. Because it does not, the order should be affirmed in all respects.

II. COUNTERSTATEMENT OF THE ISSUES

1. Did the trial court properly exercise its discretion in ruling that the Shield Law did not apply because Kazakhstan's subpoena did not seek information that tended to identify a confidential source?

2. Did the trial court properly exercise its discretion in permitting discovery of the requested information, where it narrowed the scope of the subpoena and restricted dissemination of the materials produced to "attorneys' eyes only"?

III. COUNTERSTATEMENT OF THE CASE

A. **2012-2014: After An English Court Finds That Mukhtar Ablyazov Committed Multi-Billion Dollar Fraud Against A Kazakh Bank, He Is Arrested In France And Faces Extradition; Attorneys And Government Authorities Find Their Emails And Text Messages Hacked**

The story begins with a Kazakh national named Mukhtar Ablyazov. In February 2012, Ablyazov faced allegations in an English court that he defrauded a Kazakh bank of billions of dollars. (CP 206 ¶20) The day before the English court was slated to rule on a contempt of court charge against Ablyazov, he fled England using a false passport. (CP 206 ¶21) The English court ultimately sentenced Ablyazov to 22 months in prison for contempt. (*Id.*)

Ablyazov remained a fugitive for the next 17 months, until French authorities arrested him in Provence in July 2013. (CP 206 ¶22) Since the

time Ablyazov fled England, the English court has entered two separate judgments against him finding that he did, in fact, defraud the Kazakh bank of billions of dollars. (CP 206 ¶¶20; CP 223-26) A French court authorized Ablyazov's extradition to Russia or Ukraine to face criminal proceedings regarding his bank fraud scheme, but the French government has not yet reached a final decision on extradition. (CP 206 ¶¶22)

Ablyazov owns a global media network that has been prolific in its criticism of the Kazakhstan government. (CP 207-08 ¶¶31-35) He has maintained close ties with two individuals, Muratbek Ketebayev and his wife Irina Petrushova. (CP 204-05 ¶¶12-19; CP 207 ¶¶26-29) Ketebayev administers Ablyazov's media network and owns an English company that licensed content from Ablyazov's network. (CP 207 ¶¶31-32) Petrushova is the editor-in-chief of an online Russian-language newspaper named Respublika. (CP 77 ¶3) She also co-owns LMC with her brother Alexander Petrushov. (CP 78 ¶4) LMC, in turn, operates the online version of Respublika, whose main website is www.respublika-kaz.info. (CP 77 ¶3) Respublika has published articles asserting that the Ablyazov's pursuit and conviction in an English court for the bank fraud scheme, as well as the related extradition proceedings after he fled England, are politically motivated. (CP 209 ¶¶40-44)

During Ablyazov's extradition proceedings, French newspapers reported that someone hacked the email and voicemail accounts of attorneys connected with the matter. (CP 206-07 ¶¶25; CP 228-238) Communications—including voicemails, text messages, and emails—between attorneys and French and Ukrainian authorities regarding the extradition were stolen and then published on a website named trust.ua. (CP 231-32; CP 237-38) According to a July 2014 newspaper article, Ablyazov then filed a series of complaints against the French magistrates who approved his extradition, pointing to the stolen communications posted on the website as proof that the magistrates were engaged in some sort of collusion. (CP 237-38) Another article reports that a French attorney victimized by the hackers suspected Ablyazov's supporters to be responsible and filed a complaint in French court to investigate the event.³ (CP 231-32)

Kazakhstan has shared these suspicions. Kazakhstan believes that the hacking and theft of attorney and government documents in the extradition proceedings were part of a broader attempt to sway public opinion in Ablyazov's favor and minimize the fact that a court has found

³ The stolen documents posted on the trust.ua website were also re-published by a Polish nongovernmental organization named ODF. Kazakhstan believes that Ablyazov has funded ODF with the money he stole from the Kazakh bank and that Petrushova is in charge of ODF's media presence. (CP 209-10 ¶¶45-53)

Ablyazov to have committed billions of dollars' worth of fraud against a Kazakh bank. (CP 206 ¶23; CP 209-11 ¶¶40-44, 55-56)

B. 2015: Email Accounts Of Senior Officials In Kazakhstan's Ministry Of Justice Are Hacked; Privileged And Sensitive Documents, Including Documents Related To Ablyazov, Are Stolen And Posted Online; Kazakhstan Turns To U.S. Courts To Help Identify The Hackers

In January 2015, Kazakhstan discovered that unidentified hackers had broken into the email accounts of high-ranking officials in Kazakhstan's Ministry of Justice and stole thousands of emails and documents. (CP 202-03 ¶4) The stolen materials included attorney-client privileged communications between Kazakhstan and its outside counsel—including outside counsel practicing in the United States—as well as documents containing highly sensitive matters of state. (CP 203 ¶5; Complaint in *The Republic of Kazakhstan v. Does 1-100 Inclusive*, No. 1:15-cv-1900-ER (“Complaint”), attached as Appendix B to Op. Brf. at 3-4 ¶¶13-16) The documents were not intended for public viewing, but only for viewing by and between the sender and recipient. (CP 203 ¶5)

Many of the stolen documents related to the fraud and extradition proceedings against Ablyazov. (CP 210 ¶55) These documents were then posted on third-party websites, including <https://kazaword.wordpress.com>, www.respublika-kaz-info, and www.facebook.com. (CP 202-03 ¶4) Based on what happened in France, Kazakhstan suspected that Ablyazov

and his supporters were also behind this latest hacking and theft as part of their continued efforts to draw attention away from Ablyazov's bank fraud conviction and to paint the extradition proceedings as politically motivated. (CP 210)

Kazakhstan turned to the United States courts to help identify the hackers. Because Google (the provider for several of the email accounts) and Facebook (one of the websites on which the stolen materials were posted) were headquartered in Northern California, Kazakhstan filed a complaint in February 2015 against Doe defendants in the Superior Court of California. (CP 50-57; Tr. 13) The complaint alleged violations of the California Comprehensive Computer Data Access and Fraud Act [Cal. Penal Code §§ 502 *et seq.*] and the federal Computer Fraud and Abuse Act [18 U.S.C. § 1030 *et seq.*]. (CP 52-54)

The next month, Kazakhstan also filed suit in the U.S. District Court for the Southern District of New York against numerous Doe defendants, seeking injunctive relief and damages under the federal Computer Fraud and Abuse Act.⁴ (Complaint at 1-7) About a week later,

⁴ The stolen communications included numerous emails either directed to or including attorney Jacques Semmelman, outside counsel for Kazakhstan at the law firm of Curtis, Mallet-Provost, Colt & Mosle LLP. (Complaint at 3-4 ¶¶14-15) Mr. Semmelman's office is in New York, and he is licensed to practice in New York and a member of the Southern District of New York bar. (Complaint at 4 ¶15)

the federal court issued a preliminary injunction finding good cause to believe that the defendants illegally hacked into Kazakhstan's computers, had no right to the stolen materials, and their activities had caused and will continue to cause irreparable harm to Kazakhstan. (CP 197-99 ¶¶16-25) The district court prohibited the defendants from disclosing or disseminating the stolen materials and directed defendants to (1) return the stolen materials to Kazakhstan, and (2) provide the court with any proceeds the defendants received as a result of their theft. (CP 200 ¶¶1-3)

In connection with the California action, Kazakhstan issued several subpoenas duces tecum to several entities in an effort to gather documents identifying the hackers. Among others, Kazakhstan subpoenaed documents from Google and Microsoft [Tr. 13-14], as well as from Black Lotus [CP 203 ¶8]. Black Lotus produced documents identifying Ketebayev as the primary contact for www.respublika-kaz.info, along with Alexander Petroshov and someone named "Valeri". (CP 203-04 ¶10; CP 214)

Kazakhstan also subpoenaed documents from eNom, a company in Kirkland and the domain name registrar for www.respublika-kaz.info.⁵ (CP 1-16) Kazakhstan requested the King County Superior Court clerk to

⁵ A domain name registrar is an accredited organization that manages and controls the reservation of internet domain names. (CP 34-35 ¶¶6-8)

issue the subpoena under RCW 5.51.010 *et seq.* (the Uniform Interstate Discovery and Depositions Act). (CP 12-16) The eNom subpoena sought (1) documents sufficient to identify the current and former registrants of the domain name with which the Respublika website operates, (2) documents sufficient to show the dates, times and corresponding IP Addresses and/or Mac Addresses from which the domain name was registered, created or modified, (3) all personally identifying information related to any person who purchased, used, or implemented eNom's identity protection service in connection with the registration, purchase, or use of the domain name, (4) documents sufficient to show all contact information for the person who used eNom's identity protection service in connection with Respublika's website, and (5) documents sufficient to show all contact information for eNom's identity protection service. (CP 16)

C. LMC Moves To Quash Under Washington's Shield Laws, Claiming The Subpoena Sought Information About LMC's Confidential Sources; The Trial Court Denies The Motion.

LMC—not eNom—appeared and moved to quash the subpoena. LMC contended that the subpoena was (1) improper under Washington's Shield Law because it sought information about journalists' confidential news sources, and (2) unduly burdensome and oppressive because

Kazakhstan would use the documents to target opposition journalists and their sources. (CP 21-31)

In support, LMC proffered a declaration from Petrushova. (CP 77-90) Most of the declaration set forth Petrushova's belief that Kazakhstan had persecuted her and other journalists. (CP 77-87) She asserted that Kazakhstan was seeking the domain registrant's identity because it intended to pursue unfounded criminal charges against him or her. (CP 88-90 ¶¶45-53) Petrushova, however, nowhere discussed the stolen materials that were posted on Respublika's website or how Respublika received those materials, much less that Respublika received those materials from a confidential source. (*See* CP 77-90) Nor did Petrushova assert that the person who registered the domain name for Respublika's website was the confidential source of the stolen materials or received the stolen materials from a confidential source. (*See* CP 77-90)

Kazakhstan opposed, asserting that the Shield Law did not apply because the subpoena (1) was not directed at journalists or news media organizations, and (2) did not seek confidential news sources. (CP 173-83) Rather, its subpoena sought information regarding who had registered the website's name, as well as the IP addresses for the computers used in that effort. (CP 180-82) These materials, Kazakhstan explained, were relevant because they would help identify who illegally hacked into the

email accounts and stole the confidential materials. (*Id.*) For the same reasons, the subpoena was not unduly burdensome or oppressive because it did not “target” any journalists. (CP 176-79)

Kazakhstan proffered the declaration of Marat Beketayev, the Executive Secretary of the Ministry of Justice of the Republic of Kazakhstan. (CP 202-396) Beketayev explained Ablyazov’s bank fraud judgment and the relationships between Petrushova, Ketebayev, and Ablyazov that led Kazakhstan to believe the three were behind the hacking incident in France and the one leading to its eNom subpoena. (CP 206-10) Beketayev denied Petrushova’s accusations that Kazakhstan targeted opposition journalists. (CP 205 ¶16)

At the hearing on LMC’s motion, Kazakhstan explained that its purpose in subpoenaing eNom was twofold. First, the subpoena was not aimed at journalists’ news sources, but sought to identify the individual or entity that applied for Respublika’s internet domain name. (Tr. 15) Second, it sought the IP address of the computer registering that domain name because it was a small but important piece of evidence in determining the hackers’ identity. (*Id.*) According to Kazakhstan, an IP address was akin to a computer’s geographic footprint—it reveals where a computer is located, but does not reveal other identifying information such as the computer’s user or serial number. (*Id.*) Through Kazakhstan’s

subpoenas to other entities, Kazakhstan received a list of IP addresses of the computers that had accessed Kazakhstan's illegally hacked email accounts. (*Id.*) By cross-referencing that list against the IP addresses received from the eNom subpoena, Kazakhstan would be able to narrow down which IP address belonged to the computer used in the hack—and in particular, narrow the list of suspects down to people connected with registering the domain name for Respublika's website. (*Id.*)

Kazakhstan also proposed some key limitations to diffuse LMC's assertions about potential targeting of opposition journalists. Foremost, Kazakhstan agreed that eNom's document production would be "For Attorneys' Eyes Only"—that is to say, Kazakhstan's counsel would be under court order *not* to share the identity of the domain registrant with Kazakhstan officials. (Tr. 20-21) Additionally, Kazakhstan conceded that some of the document requests were unnecessary or repetitive and further agreed that it did not need the domain name registrant's billing or credit card information, but that the identity of the registrant would suffice. (Tr. 18-19)

The trial court (Hon. Mariane Spearman) agreed with Kazakhstan that its subpoena did not seek information regarding a confidential source and therefore was not precluded under Washington's Shield Laws. (Tr. 26) It issued an order denying LMC's motion to quash and directed eNom

to produce documents under three limitations: (1) eNom needed to produce documents only regarding request numbers 1 and 2, (2) eNom was not required to produce “billing information,” and (3) the produced documents were for attorneys’ eyes only. (CP 412) The trial court further reminded counsel that it would retain jurisdiction over the matter “if there’s any violation of that order.” (Tr. 31)

D. LMC Appears In The New York Action To Challenge The Preliminary Injunction And Claims That It Obtained The Stolen Materials From A Public Website.

Meanwhile, in the New York proceeding, Kazakhstan took steps to enforce the district court’s preliminary injunction order. Because Respublika posted the stolen materials on its Facebook page, Kazakhstan advised Respublika about the preliminary injunction and requested that Respublika remove the offending content. Although Respublika initially complied, it resumed posting the stolen materials and rejected Kazakhstan’s repeated requests for withdrawal. (June 30, 2015, letter from J. Semmelman to Hon. E. Ramos (“June 30 letter”), attached as Exhibit B to Motion to Permit Additional Evidence on Review, at 1-2)

Kazakhstan likewise contacted Black Lotus—Respublika’s web host, discussed above—regarding the continued posting of the stolen materials on Respublika’s website. Because Black Lotus had no control over individual website posts, it asked Respublika to remove the stolen

materials. Although Respublika initially withdrew the materials, it reposted the stolen materials shortly thereafter and then backdated the posts to make it appear that they were never removed. It was only after Respublika's reposting and backdating efforts that Kazakhstan discussed with Black Lotus whether shutting down the entire website was a possibility. Black Lotus declined to do so, but assured Kazakhstan it would continue requesting that Respublika withdraw individual posts with stolen materials. (June 30 letter at 2-3)

Respublika then appeared in the Southern District of New York action and asked the district court for a pre-motion conference to discuss the scope of its preliminary injunction order. (June 25, 2015, letter from J. Rosenfeld to Hon. E. Ramos ("June 25 letter"), attached as Exhibit A to Motion to Permit Additional Evidence on Review, at 1) Respublika denied that it authorized or encouraged anyone to hack into Kazakhstan's computer system and steal the confidential and privileged materials. Rather, it stated:

Respublika found the documents the same way the rest of the world did—after 69 gigabytes of documents were anonymously posted to kazaword.wordpress.com. Respublika reported on the information contained within some of those documents, as did many other media outlets around the world. [June 25 letter at 2]

This was startling. The whole thrust of LMC's objections to Kazakhstan's subpoena under Washington's Shield Law was that Kazakhstan sought the identity of Respublika's confidential source of the stolen materials. And yet, in a different court, Respublika asserted that it did not obtain them from a confidential source at all, but from a public website.

IV. ARGUMENT

A. Standard Of Review

“An appellate court reviews a trial court's discovery order for an abuse of discretion.” *T.S. v. Boy Scouts of Am.*, 157 Wn.2d 416, 423, 138 P.3d 1053 (2006). “An appellate court will find an abuse of discretion only ‘on a clear showing’ that the court's exercise of discretion was ‘manifestly unreasonable, or exercised on untenable grounds, or for untenable reasons.’” *Id.* (citation omitted). “A trial court's discretionary decision is based on untenable grounds or made for untenable reasons if it rests on facts unsupported in the record or was reached by applying the wrong legal standard.” *Id.* at 423-24 (internal quotations and citation omitted). “A court's exercise of discretion is manifestly unreasonable if the court, despite applying the correct legal standard to the supported facts, adopts a view that no reasonable person would take.” *Id.* at 424

(internal quotations omitted; citing *State v. Lewis*, 115 Wn.2d 294, 298–99, 797 P.2d 1141 (1990)).

There was no abuse of discretion. The trial court’s discovery order correctly found that Kazakhstan’s subpoena did not seek information that directly or indirectly identified journalists’ confidential sources and, in any event, narrowed the scope of discovery and restricted dissemination of the information produced to “attorneys’ eyes only.” Its decision was firmly tethered to the law and the record and should be affirmed.

B. LMC’s “Claim-Splitting” Argument Was Not Raised Below And Is Wrong In Any Event

LMC first contends that reversal of the trial court’s discovery order is required because the doctrine of res judicata prevents Kazakhstan from splitting its claim between the New York and California actions. (Op. Brf. 22-23) This argument need not detain this Court.

The merits of affirmative defenses like res judicata and claim-splitting in the New York and California actions lay well beyond the purview of this limited discovery proceeding.⁶ This matter arose in Washington’s courts when Kazakhstan availed itself of Washington’s Uniform Interstate Depositions and Discovery Act. (CP 12-16) The Act creates a streamlined procedure by which a litigant in an out-of-state

⁶ Of course, Kazakhstan does not concede that these defenses would succeed in the New York or California actions.

action can invoke the jurisdiction of Washington courts, obtain an enforceable discovery subpoena in aid of that out-of-state action, and then serve it on a Washington resident. *See* RCW 5.51.020; *see also* Laws of 2012, ch. 95, H.B. 2195, Final Bill Report, eff. June 7, 2012) (adopting Uniform Depositions and Discovery Act to “create[] a uniform mechanism by which litigants may present the clerk of a court located in the state in which discovery is sought with a subpoena issued by a court in the trial state”). The party seeking the subpoena need not initiate a civil action or assert any causes of action; it simply applies to the clerk of the court for issuance of the subpoena. RCW 5.51.020. The statutes provide only for a procedure to challenge the subpoena through a motion for a protective order. RCW 5.51.050.

Under this statutory scheme, the only issue is whether the subpoena to eNom passed muster under Washington’s discovery rules. Kazakhstan never placed the merits of its claims at issue and courts are nowhere empowered to issue any ruling on the merits. Whether Kazakhstan’s claims are subject to defenses of claim splitting or res judicata is for the New York or California courts to decide. LMC’s argument fails for this reason alone.

In any event, res judicata and claim splitting do not result in the dismissal of Kazakhstan’s claims in New York or California, much less

the limited discovery proceeding here in Washington. For one thing, LMC fails to explain how Washington’s law on this issue could somehow control dismissal of actions in New York or California that were brought under federal and California state statutes. But even if Washington law applied, LMC’s argument fails.

“Claim-splitting”—that is to say, “[f]iling two separate lawsuits based on the same event”—is another way of describing the doctrine of res judicata. *Ensley v. Pitcher*, 152 Wn. App. 891, 898, 222 P.3d 99 (2009). “[R]es judicata prohibits the relitigation of claims or issues that were litigated, or could have been litigated, in a prior action.” *Karlberg v. Otten*, 167 Wn. App. 522, 535, 280 P.3d 1123 (2012). Under this rule, “if an action is brought for part of a claim, a judgment obtained in the action precludes the plaintiff from bringing a second action for the residue of the claim.” *Landry v. Luscher*, 95 Wn. App. 779, 782, 976 P.2d 1274 (1999). The doctrine is intended to “curtail multiplicity of actions by parties, participants or privies who have had an opportunity to litigate the same matter in a former action in a court of competent jurisdiction.” *Karlberg*, 167 Wn. App. at 536.

“The threshold requirement of res judicata is a final judgment on the merits in the prior suit.” *Hisle v. Todd Pacific Shipyards Corp.*, 151 Wn.2d 853, 865, 93 P.3d 108 (2004); *see also Karlberg*, 167 Wn. App. at

536 (res judicata “requires a final judgment on the merits.”); *Ensley*, 152 Wn. App. at 899 (“The threshold requirement of res judicata is a valid and final judgment on the merits in a prior suit.”). For that final judgment to have res judicata effect, moreover, the doctrine “requires sameness of subject matter, cause of action, people and parties, and ‘the quality of the persons for or against whom the claim is made.’” *Hisle*, 151 Wn.2d at 866-67.

The threshold requirement of a final judgment has not been satisfied. Neither the California nor New York actions have resulted in any adjudication on the merits, much less a final judgment, that would have preclusive effect under res judicata or otherwise prevent “claim-splitting.” At most, moreover, any final judgment would affect only the New York and California actions and only the parties or their privies named in those respective actions. LMC has not been named as a party in either the New York or California actions (nor has Respublika, for that matter). Viewed from any angle, LMC’s claim-splitting argument lacks merit and is no reason to reverse the trial court’s limited discovery order.

C. LMC Did Not And Cannot Show That Washington’s Shield Law Applies

1. LMC Has The Prima Facie Burden Of Establishing The Shield Law Applies

Though caselaw has yet to discuss the burdens of proof under the Shield Law, cases in similar contexts consistently hold that the party asserting any privilege has the prima facie burden of showing it applies. *See, e.g., Fellows v. Moynihan*, 175 Wn.2d 641, 649, 285 P.3d 864 (2012) (“The burden of establishing entitlement to nondisclosure rests with the party resisting discovery.”); *Soter v. Cowles Publ’g Co.*, 162 Wn.2d 716, 745, 174 P.3d 60 (2007) (party asserting attorney-client privilege has the burden of showing attorney-client relationship materials contain privileged communications); *Guillen v. Pierce Cty.*, 144 Wn.2d 696, 716, 31 P.3d 628 (2001) (“The burden of showing that a privilege applies in any given situation rests entirely upon the entity asserting the privilege.”) (reversed in part on other grounds in *Pierce County, Wash. v. Guillen*, 535 U.S. 1033 (2002)).

This holds true in the First Amendment context. *See Eugster v. City of Spokane*, 121 Wn.App. 799, 807, 91 P.3d 117 (2004) (party associating First Amendment associational privilege has the prima facie burden of showing “some probability that the requested disclosure will harm its First Amendment rights”). As with other privileges, “the party

asserting the privilege must make an initial showing that disclosure of the materials requested would in fact impinge on First Amendment rights....” *Snedigar v. Hoddersen*, 53 Wn. App. 476, 483, 768 P.2d 1 (1989) (addressing First Amendment associational privilege) (affirmed in part and reversed in part on other grounds, 114 Wn.2d 153, 170, 786 P.2d 781 (1990)); *see also Bruno & Stillman, Inc. v. Globe Newspaper Co.*, 633 F.2d 583, 597 (1st Cir. 1980) (media defendant “has the burden of establishing need for preserving confidentiality” of journalist sources); *In re Madden*, 151 F.3d 125, 131 (3d Cir. 1998) (“individuals claiming the protections of the journalist’s privilege must demonstrate the concurrence of three elements”).

“Once this preliminary showing of privilege is made, the burden then shifts to the party seeking discovery to establish the relevancy and materiality of the information sought, and to make a showing that reasonable efforts to obtain the information by other means have been unsuccessful” *Snedigar*, 53 Wn. App. at 483.

As we explain next, LMC has failed to meet their prima facie burden of showing that the Shield Law applies.

2. RCW 5.68.010(1) Does Not Apply Because The Subpoena Is Not Directed At A Media Entity

Washington's Shield Law divides into two main parts: (1) discovery against media entities, and (2) discovery against nonmedia entities who have business relationships with media entities. *See* RCW 5.68.010(1) & (3).

As to media entities, "no judicial, legislative, administrative, or other body with the power to issue a subpoena or other compulsory process may compel the news media to testify, produce, or otherwise disclose ... [t]he identity of a source of any news or information or any information that would tend to identify the source . . . or [a]ny news or information obtained or prepared by the news media in its capacity in gathering, receiving, or processing news or information for potential communication to the public." RCW 5.68.010.

As to nonmedia entities, the statute prohibits "any subpoena issued to, or other compulsory process against, a nonnews media party where such subpoena or process seeks records, information, or other communications relating to business transactions between such nonnews media party and the news media for the purpose of discovering the identity of a source or obtaining news or information." RCW 5.68.010(3).

As a threshold matter, LMC appears to suggest that the subpoena should be quashed under RCW 5.68.010(1)—the provision governing media entities—because LMC and Respublika are news media entities. (Op. Brf. 26-27). That is incorrect. Kazakhstan’s subpoena was not directed at news media. It was directed at the domain name registrant, eNom, which is not a media entity. (CP 12) The subpoena asked eNom—*not* LMC or Respublika—to produce information relating to the domain name registrant’s identity. (CP 12-14) Consequently, Kazakhstan’s subpoena invokes the part of the statute addressing discovery against a nonmedia entity—RCW 5.68.010(3). Any discussion of the Shield Law starts there, rather than RCW 5.68.010(1).

3. RCW 5.68.010(3) Does Not Apply Because Kazakhstan’s Subpoena Does Not Directly Or Indirectly Seek Identification Of A Confidential Source

a. LMC Did Not And Cannot Meet Its Prima Facie Burden Of Showing The Statute Applies

Subsection (3) of RCW 5.68.010 reads in pertinent part:

The protection from compelled disclosure contained in subsection (1) of this section also applies to any subpoena issued to, or other compulsory process against, a nonnews media party where such subpoena or process seeks records, information, or other communications relating to business transactions between such nonnews media party and the news media for the purpose of discovering the identity of a source or obtaining news or information described in subsection (1) of this section.

Subsection (1), in turn, prohibits the compelled disclosure of “the identity of a source or any information that would tend to identify the source where such source has a reasonable expectation of confidentiality....” RCW 5.68.010(1)(a).

Effective in 2007, the Shield Law codified what was then a common law “qualified privilege for reporters against compelled disclosure of confidential source information in both civil and criminal cases....” Laws of 2007, ch. 196, H.B. 1366, Final Bill Report, eff. July 22, 2007. Under the Shield Law, journalists enjoy an absolute “privilege from being compelled to testify, produce, or disclose the identity of a source of news or information, or any information that would tend to identify the source, if the source has a reasonable expectation of confidentiality.” *Id.* Journalists enjoy a qualified privilege for “any news or information obtained or prepared in the course of gathering, receiving, or processing news or information for potential communication to the public.” *Id.*

Apart from protecting journalists against compelled disclosure, the Shield Law also was intended to protect a “nonnews media party ... from compelled disclosure of records or information relating to business transactions with the news media where the purpose of seeking the records

is to discover the identity of a source or other information protected from disclosure.” *Id.*

No cases discuss the Shield Law in a manner that illuminates these provisions.⁷ In particular, neither the statute nor its legislative history defines a “source” or “confidential source.” Other authorities, however, are instructive.

In journalist parlance, the word “source” is a “term of art[.]” *In re Indiana Newspapers Inc.*, 963 N.E.2d 534 (Ind. App. 2012). It refers to “a person, record, document, or event that gives information to a reporter in order to help write or decide to write a story.” *Id.* (citation omitted); see also *The Wall Street Journal Glossary of Terms: Journalism* at <http://info.wsj.com/college/glossary/journalism.pdf> (defining “source” as “Person, record, document or event that provides the information for the story.”) (visited August 7, 2015); Adam L. Penenberg, *NYU Journalism*

⁷ Only two cases cite the Shield Law. *U.S. v. Sterling*, 724 F.3d 482, 532 (4th Cir. 2013), cites it as part of the broader proposition that thirty-nine states plus the District of Columbia have statutory journalist’s privileges. In *Davis v. Cox*, 180 Wn. App. 514, 547 n.11, 325 P.3d 255 (2014) (reversed, 183 Wn.2d 269, 351 P.3d 862 (2015)), this Court explained that the Shield Law permits disclosure of journalist work *product*—such as notes, photos, video, etc.—where there is a clear and convincing showing of need. See RCW 5.68.010(1)(b) (addressing journalist work product).

Although most states have some form of statutory journalist’s privilege, only Maine and Connecticut appear to share Washington’s provision governing nonmedia entities. See Me. Rev. Stat. tit. 16 §61(3); Conn. Gen. Stat. §52-146t. The courts in those two states have not addressed these provisions, either.

Handbook for *Students* at

<http://journalism.nyu.edu/assets/PageSpecificFiles/Ethics/NYU-Journalism-Handbook-for-Students.pdf> (defining “human source” as “a person who contributes information to a piece of reportage”) (visited August 7, 2015).

Similarly, Black’s Law Dictionary defines “confidential source” as “[s]omeone who provides information to a law-enforcement agency or to a journalist on the express or implied guarantee of anonymity.” *Confidential Source*, Black’s Law Dictionary (10th ed. 2014).

Washington’s pre-Shield Law cases enforce the common-law journalist’s privilege where a party requested from a journalist or newspaper information provided directly from a source to that journalist or newspaper. *See State v. Rinaldo*, 102 Wn.2d 749, 689 P.2d 392 (1984) (defendant sought newspaper’s materials from interviews between journalist and sources); *Clampitt v. Thurston Cnty.*, 98 Wn.2d 641, 658 P.2d 641 (1983) (reversing order compelling reporter to identify the individual who told him about memorandum that formed the basis of reporter’s article); *Senear v. Daily Journal Am.*, 27 Wn. App. 454, 618 P.2d 536 (1980) (plaintiff served the newspaper with interrogatories asking for identification of union members who furnished certain information for a story).

Plus, at least two states whose statutes define “source” embrace this view. In Delaware, for example, source means:

[A] person *from whom a reporter obtained information by means of written or spoken communication or the transfer of physical objects*, but does not include a person from whom a reporter obtained information by means of personal observation unaccompanied by any other form of communication and does not include a person from whom another person who is not a reporter obtained information, even if the information was ultimately obtained by a reporter.

10 Del. Code Ann. Tit 10, § 4320(5) (emphasis added).

Illinois likewise defines “source” to mean “the person or means from or through which the news or information was obtained.” 735 Ill. Comp. Stat. § 8-902(c). Michigan’s statutory privilege uses the word “informant” to refer to the confidential source. Mich. Comp. Laws Ann. § 767.5a. “Informant” connotes the person who supplied confidential information directly to a reporter. *See Informant*, Black’s Law Dictionary (10th ed. 2014) (defining “informant” as someone who “confidentially supplies information to the police about a crime, sometimes in exchange for a reward or special treatment).

Here, Kazakhstan’s subpoena requests from eNom information regarding the identity of current and past domain name registrants—persons who registered the name www.respublika-kaz.info. (CP 12-16) Kazakhstan sought this information as part of its overall investigation into

who hacked into its computer systems and stole confidential documents that were later posted onto LMC's website.

Thus, to invoke the Shield Law's protections, LMC had to make the prima facie showing that current or past domain name registrant(s) provided those stolen materials to journalists in confidence—i.e., that the current or past domain registrants were the confidential "source." Alternately, LMC had to make the prima facie showing that the subpoena would tend to identify their journalists' confidential "source"—that is, the person who provided the stolen materials to the journalist. As the trial court correctly ruled, LMC failed to meet its burden.

The only evidence LMC proffered was Petrushova's declaration, which, while full of accusations about Kazakhstan's political climate, *never* explained how Respublika's journalists came to possess the stolen materials. (CP 77-90) She *never* explained whether or how the domain name registrants provided the stolen materials to Respublika's journalists, much less that the domain name registrants ever possessed those stolen materials. (*Id.*) And she *never* explained how disclosing the domain name registrants' identities would tend to identify the persons who supposedly provided Respublika's journalists with the stolen materials. (*Id.*)

The only thing Petrushova said about the domain "owner" was that he or she is an individual and, Petrushova believed, less "protected" from

purported reprisals than a media company would be. (CP 88 ¶46) She also asserted that disclosure of those identities may place the domain name registrants at risk. (CP 88-89, ¶¶47-51) Although Kazakhstan strongly denies these accusations, the salient point for purposes of the Shield Law analysis is that these accusations of reprisals against the domain name registrants do not explain how disclosure of *their* identities would, in turn, tend to identify who gave Respublika's journalists the stolen materials.

LMC's opening brief is equally coy. LMC says that "someone at Respublika *may* be the hacker," or Respublika "*may* have received" the stolen materials "from a hacker" or Respublika "*may* have received those [materials] from intermediaries who received them from a hacker." (Op. Brf. 33-34) Speculation about how Respublika's journalists "may have" received the stolen materials hardly satisfies LMC's prima facie burden of proof. *See, e.g., U.S. v. Hively*, 202 F. Supp. 2d 886, 889 (E.D. Ark. 2002) ("Movants' bare assertion that certain testimony may implicate confidential sources or information is insufficient to satisfy their burden on this issue. Vague allegations of potential indication of confidential sources will not suffice to support a claimed qualified reporter's privilege. ... Movants must provide the court with particularized allegations or facts to support a privilege claim.") (internal quotations and citations omitted); *Cont'l Cablevision, Inc. v. Storer Broadcasting Co.*, 583 F. Supp. 427, 436

(D.C. Mo. 1984) (a “reporter must, in addition to claiming the privilege in response to specific requests or questions, provide a court with particularized allegations or facts that support his/her claim of privilege”).

More importantly, LMC’s musings about how Respublika’s journalists “may have” received the stolen materials are beside the point. The critical question is what role, if any, did the domain name registrants play in giving the stolen materials to Respublika’s journalists. As the trial court correctly recognized, LMC’s total failure to answer that question or to otherwise draw any connection between the domain name registrant and Respublika’s journalists with respect to the stolen materials correctly doomed their invocation of the Shield Law.

LMC’s recent statements in the New York district court put the exclamation point on this conclusion. There, Respublika asserted that it acquired the stolen materials “the same way the rest of the world did”—from a publicly available, third-party website. (June 25 letter at 2) In other words, Respublika asserted that its journalists did not receive the stolen materials from any confidential source, but simply pulled them off the internet. That assertion explains why LMC has danced around the issue of how Respublika’s journalists acquired the stolen materials—if

LMC had made that same representation here in Washington, it would have swiftly shut the door on any Shield Law protections.⁸

The bottom line is that LMC failed to make its prima facie showing that the Shield Law barred Kazakhstan's subpoena. And given what Respublika has asserted in the New York district court, there is no way LMC can make that prima facie showing, either. The trial court did not abuse its discretion in concluding that the Shield Law did not apply and its order should be affirmed.

b. LMC's Arguments Lack Merit

LMC's principal argument boils down to this. According to LMC, because Kazakhstan's subpoena admittedly is intended to identify the hackers, it *necessarily* means that the information sought tends to identify a confidential source. In other words, LMC appears to argue that the hackers themselves are the "source." (Op. Brf. 33-34) LMC is wrong on any number of levels.

As discussed, LMC has never come out and said that Respublika's journalists received the stolen information from the hackers (or even

⁸ Respublika's revelation was startling, to say the least. A reporter "is not permitted to step from behind the shield as he pleases, sallying forth one moment to make a disclosure to one person and then to seek the shield's protection from having to repeat the same disclosure to another person. A reporter cannot play peek-a-boo with the privilege." *In re Michael G. Venezia*, 922 A.2d 1263, 1273-74 (N.J. 2007).

someone purporting to be the hackers' authorized agent or intermediary). Nor can it, since Respublika has asserted elsewhere that its journalists simply pulled the stolen materials from another publicly-available website. The factual premise of LMC's argument does not exist anywhere in the record and it should be rejected for this reason alone.

Consider, too, the legal ramifications of LMC's view. As LMC would have it, every time Kazakhstan seeks any kind of discovery in Washington that is intended to help identify the hackers, LMC is entitled to quash that effort under the Shield Law. According to LMC, it does not matter whether Respublika's journalists actually received the stolen materials from the hackers. It also does not matter how far removed the hackers are from Respublika's journalists. In LMC's view, the Shield Law would apply even where the hackers gave the stolen materials to six, ten, or twenty different people—one of whom posted the materials on a public website from which Respublika's journalists gathered the stolen materials.⁹ That view stretches the Shield Law beyond the point of absurdity. *State v. J.P.*, 149 Wn.2d 444, 450, 69 P.3d 318 (2003) (“[I]n

⁹ Nobody has a “legitimate expectation of privacy in information he voluntarily turns over to third parties.” See *In re Application of the United States of America For an Order Pursuant to 18 U.S.C. §2703(d)*, 830 F. Supp. 2d 114, 131 (2011) (citation omitted); see also *Smith v. Maryland*, 442 U.S. 735, 743–44, 99 S. Ct. 2577 (1979) (telephone numbers); *United States v. Miller*, 425 U.S. 435, 442, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976) (bank records).

construing a statute, a reading that results in absurd results must be avoided because it will not be presumed that the legislature intended absurd results.”) (quoting *State v. Delgado*, 148 Wn.2d 723, 733, 63 P.3d 792 (2003)).

New York Times v. Gonzales, 459 F.3d 160 (2d Cir. 2006), does not invite a different conclusion. There, in the wake of 9/11, the federal government developed a plan to freeze the assets of organizations it believed were raising money in the U.S. to fund terrorists. *Id.* at 162. Two New York Times reporters discovered the plan and called the organizations for comment, which the government believed endangered the agents conducting the investigation and alerted the terrorists. *Id.* The government began a grand jury investigation and threatened to subpoena the reporters’ phone records. *Id.* The New York Times sought declaratory relief that the common law reporter’s privilege barred the subpoena because it sought the reporters’ confidential sources. *Id.* The Second Circuit held that a qualified journalist’s privilege extended to journalist’s telephone records held by a third party, but the government had overcome the privilege by showing the information was critical to the grand jury’s needs and there were no other means to acquire it. *Id.* at 167-71.

RCW 5.68.010 already codifies the notion in *Gonzales* that third-party business records may fall within the scope of the journalist’s

privilege. If anything, *Gonzalez* shows that the statute has to be interpreted to require some meaningful connection between the third party's business records and the confidential source's identity. It makes sense that telephone records would fall within the privilege because information tending to identify the source—the source's telephone number—is evident from the face of the records produced. But the same cannot be said of Kazakhstan's subpoena regarding the website's domain name registrant. Again, LMC has failed to explain how information identifying Respublika's confidential sources would be evident from any document produced in response to the subpoena. There is no explanation in the record regarding how or from what confidential source Respublika acquired the stolen information—a void that is not surprising, given that Respublika told another court that it acquired the information on a publicly-available website. *Gonzales* does not further LMC's argument; it reinforces that the trial court got it right.

LMC makes two other points that can quickly be dispatched. LMC first asserts that Washington's common-law journalist privilege “supports broad application of the Shield Law.” (Op. Brf. 35-37) It also insists that the Washington Constitution has historically extended greater protection to the press than the federal Constitution and thus prevents Washington courts from chilling free speech and a free press. (Op. Brf. 44-50)

The problem with these arguments is that they assume Kazakhstan's subpoena would result in the disclosure of confidential sources or the suppression of free speech. As discussed at length, it does not. LMC has not demonstrated that the domain name registrant is a confidential source or is otherwise connected to confidential sources. LMC has not demonstrated that the domain name registrant is a journalist. And regardless, the trial court balanced LMC's concerns by narrowing the subpoena and preventing Kazakhstan's attorneys to share information produced in response to the subpoena with Kazakhstan itself. (*See discussion post* at 38-45)

None of the authorities LMC cites in support of these arguments so much as suggests that LMC is relieved from its prima facie burdens or that the trial court loses its discretion to balance discovery needs against claimed side effects of disclosure. Although LMC relies principally on this Court's opinion in *State v. Rinaldo* to argue that Washington's Constitution is more protective of the press [Op. Brf. 46-47], that case does not change the analysis. Based on its review of the Washington Constitution, *Rinaldo* held that the press enjoyed an absolute privilege from disclosing confidential information or sources. *State v. Rinaldo*, 36 Wn. App. 86, 91-100, 673 P.2d 614 (1983). The Supreme Court disagreed, however, holding that this view was "inapposite to all case

law.” *Rinaldo*, 102 Wn.2d at 753. The Legislature then codified an absolute journalists’ privilege regarding the identity of confidential sources. (See discussion *ante* at 26-27) In other words, this Court’s decision in *Rinaldo* does not call for any heightened analysis of these issues because it ends up in the same place as the Shield Law at issue in this appeal. Again, nothing in the Shield Law, its legislative history, or the cases that predate the Shield Law purports to relieve journalists of the prima facie burden of showing the privilege applies in the first instance. The order was correct by any measure and LMC’s incantation of common law privileges and the Washington Constitution is unavailing under the circumstances.

D. The Subpoena Is Not Burdensome Or Oppressive

LMC asserts that the trial court should have quashed the subpoena as unduly burdensome and oppressive because Kazakhstan has manipulated the U.S. judicial system to acquire information and will use it “hunt down” opposition journalists. (Op. Brf. 31 n.9 and 35-44) These arguments fail for several reasons.

Trial courts have “substantial latitude to decide when a protective order is appropriate and what degree of protection is required given the unique character of the discovery process.” *King v. Olympic Pipeline Co.*, 104 Wn.App. 338, 371, 16 P.3d 45 (2000). Courts will not disturb a

protective order that sufficiently balances the right to discovery against any purported side effects of disclosure. *Id.* at 372 (affirming protective order that prevented newspaper from publishing information gathered from court proceeding); *see also Rhinehart v. Seattle Times*, 98 Wn.2d 226, 231, 257, 654 P.3d 673 (1982) (discovery order not abuse of discretion where trial court properly balanced the defendant’s need for discovery against the plaintiff’s risk of exposure); *Brown Bag Software v. Symantec Corp.*, 960 F.2d 1465, 1468-69, 1472 (9th Cir. 1992) (affirming protective order with “attorneys’ eyes only” designations); *Cabell v. Zorro Prods., Inc.*, 294 F.R.D. 604, 607 (W.D. Wash. 2013) (issuing protective order with “attorneys’ eyes only” designation and recognizing that “courts have broad discretion to determine the scope of discovery”).

As a threshold matter, Kazakhstan has not attempted to misuse the U.S. courts. Represented by counsel, Kazakhstan filed suit in California because Google and Black Lotus were in California and the hackers’ conduct violated both California and federal data privacy and fraud laws. (CP 50-57) Kazakhstan could not identify defendants in its complaint because it did not know the hackers’ identities. (CP 51 ¶3) Kazakhstan then embarked on discovery against third parties to try and figure that out,

with the goal of naming defendants once more information was revealed.¹⁰ (*Id.*) As part of this process, and pursuant to Washington’s rules, Kazakhstan lawfully obtained a third-party discovery subpoena and served it on eNom. (CP 12-16) Kazakhstan has proceeded by the book in California and Washington.

Kazakhstan also denies that its subpoena is intended to hunt down opposition journalists. Again, the subpoena seeks the identity of the domain name registrant—the person(s) who registered the website name—and not the identity of any journalists. (CP 12-16) Through its subpoena to Black Lotus, Kazakhstan already knows the primary contacts for the website [CP 203-04 ¶10], and Petrushova disclosed in a declaration in this case that she and her brother own LMC, which in turn owns the website [CP 77-78 ¶¶3-4]. It is unlikely that a person outside that trio is the domain name registrant. But more importantly, LMC’s evidence nowhere indicates that the domain name registrant is a journalist.¹¹

¹⁰ California permits the filing of an action against only Doe defendants. Cal. Civ. Proc. Code § 474 (authorizing complaint against unknown defendants); *Pierce v. San Mateo Cty. Sherriff’s Dep’t.*, 232 Cal. App. 4th 995, 1020 (2014) (“In fact, a complaint can be asserted against only Doe defendants.”).

¹¹ LMC’s brief asserts that eNom “has been Respublika’s domain name registrant for years and therefore has years’ worth of identifying information about Respublika’s journalists, including names, addresses, telephone numbers, email addresses, and all other available information.” Op. Brf. 42) That is not what the record says. Nowhere in the record

That omission exposes a recurring theme in LMC’s position. First, LMC invokes Washington’s Shield Laws and accuses Kazakhstan of trying to identify confidential sources, but it nowhere states that the domain name registrant is a confidential source. Then, LMC claims that Kazakhstan’s subpoena will be used to hunt down opposition journalists, but again, it nowhere states that the domain registrant is a journalist. In other words, LMC levels grave accusations against Kazakhstan and invokes important First Amendment considerations, but LMC’s evidence does not match the weight of those considerations. Its rhetoric is no substitute for evidence.

Nevertheless, the trial court was sensitive to LMC’s concerns and placed significant limits—limits that Kazakhstan proposed—on what eNom was required to produce. At the hearing, Kazakhstan abandoned any request for “billing records” and the trial court included that limitation in its order. (CP 412). Kazakhstan also abandoned any request for information regarding eNom’s privacy service or who used the privacy service and the trial court incorporated those limitations into its order as well. (CP 412) Most importantly, to address LMC’s accusations that

citations provided—or anywhere else in the record—does LMC say that eNom has journalists’ identities. And even if it did, Kazakhstan’s subpoena asks only for the domain name registrant’s identity rather than any journalist’s.

Kazakhstan had ulterior motives for seeking the requested documents—which it does not—the trial court directed that any documents produced would be “For Attorneys’ Eyes Only.” (CP 412) That is to say, Kazakhstan would not be able to review the documents produced—only its attorneys could do so. The trial court further stated that it would retain jurisdiction over the matter to ensure compliance with its order. Given all of this, the trial court’s order was hardly an abuse of discretion.

LMC downplays the significance of the “attorneys’ eyes only” provision, claiming that Kazakhstan could simply dismiss its California action or direct its attorneys to provide them the information orally. (Op. Brf. 20) Neither argument makes sense. Again, at the hearing, the trial court reminded counsel that it retained jurisdiction to police violations of its order. (Tr. 31) So regardless of whether Kazakhstan dismissed its California action, LMC still has an avenue of redress for any violations of the order. Further, to be clear, Kazakhstan’s counsel understands its obligations. If Kazakhstan directs its counsel to circumvent the order and identify the domain name registrant by word of mouth rather than by giving Kazakhstan the documents, counsel would have to decline. That is all there is to it.

Howell v. Spokane & Inland Empire Blood Bank, 117 Wn.2d 619, 818 P.2d 1056 (1991), does not alter this conclusion. (Op. Brf. 38-40)

There, the plaintiff received a blood transfusion and sued his anonymous donor after contracting HIV. *Howell*, 117 Wn.2d at 629. The anonymous donor, who appeared in the action, resisted disclosure of his true identity. The trial court fashioned a unique order allowing the plaintiff to depose the donor with protections in place to conceal the donor's identity. *Id.* In so doing, the trial court "foresaw a 'fishing expedition' and protected the donor by requiring a greater showing of entitlement before allowing discovery of the donor's name." *Id.*

The plaintiff appealed summary judgment in favor of the donor, claiming his inability to uncover the donor's identity prejudiced his case. The Washington Supreme Court disagreed, noting that the plaintiff had conducted "extensive discovery" against the defendant but "was unable to uncover a scintilla of evidence indicating that John Doe X donated blood at a time when he should have known not to" and failed to explain "what relevant evidence he expects to discover if allowed access to John Doe X's name." *Id.* at 628.

Kazakhstan's subpoena is decidedly not a "fishing expedition." The domain name registrant's identity is an important piece of the puzzle and can help confirm who hacked into Kazakhstan's computers and stole privileged documents. In particular, if the IP address for any domain name registrant matches the IP address for the computer connected to the

hacking incident, then Kazakhstan will be able to focus its search on that IP address and the person who used it. (Tr. 15) If anything, *Howell* shows that a carefully crafted protective order—one that balances the need for discovery against any potential side effects of that discovery will be upheld. As discussed above, that is exactly what the trial court’s order has done here.

State v. Rinaldo, 36 Wn. App. at 86, is similarly inapt. There, a newspaper reporter wrote several articles about Rinaldo’s farm, promising to keep his sources confidential in the process. *Id.* at 88. After Rinaldo was charged with serious criminal offenses, including witness intimidation, he served a document subpoena on the newspaper requesting all written and recorded material related to his farm. *Id.* Pointing to Washington cases finding a journalist’s privilege in the civil context, the Court of Appeal extended that privilege to the criminal context and held that the newspaper was not required to divulge its confidential sources. *Id.*

LMC seizes on the witness intimidation charges in *Rinaldo*, arguing that Kazakhstan will similarly use information gleaned from its document subpoena to intimidate the domain name registrant, Respublika’s journalists, and its confidential sources. But again, the subpoena here does not seek the identity of journalists or their sources, and LMC fails to explain how disclosing the identity of a domain name

registrant will lead to such disclosure. Moreover, the trial court took considered steps to narrow the subpoena and prevent Kazakhstan's attorneys from conveying to their client any information received from the subpoena. *Rinaldo* changes none of this.

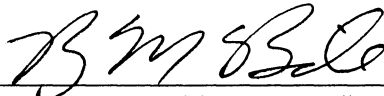
LMC's arguments regarding burden and oppression—while unfounded—were nevertheless appropriately addressed through the trial court's narrowing of the subpoena and its restrictions on disclosure. No abuse of discretion occurred here.

V. CONCLUSION

For the foregoing reasons, the trial court's discovery order should be affirmed in full.

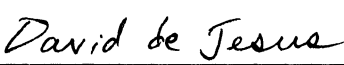
RESPECTFULLY SUBMITTED this 10th day of May, 2015.

LANE POWELL PC

By 

Ryan P. McBride, WSBA # 33280
Abraham K. Lorber, WSBA # 40668

REED SMITH LLP

By  (^{per e-mail} consent)

Robert N. Phillips, *Pro Hac Vice*
David J. de Jesus, *Pro Hac Vice*

*Attorneys for Respondent
The Republic of Kazakhstan*

CERTIFICATE OF SERVICE

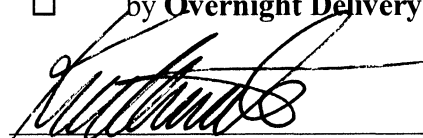
I hereby certify that on August 10, 2015, I caused to be served a copy of the foregoing Brief of Respondent on the following person(s) in the manner indicated below at the following address(es):

Robert N. Phillips
David J. de Jesus
Reed Smith, LLP
101 Second Street, 1800
San Francisco, CA 94105
robphillips@reedsmith.com
ddejesus@reedsmith.com

- by **CM/ECF**
- by **Electronic Mail**
- by **Facsimile Transmission**
- by **First Class Mail**
- by **Hand Delivery**
- by **Overnight Delivery**

Andrew J. Kinstler
Helsell Fetterman LLP
1001 Fourth Avenue, Suite 4200
Seattle, WA 98154-1154
akinstler@helsell.com

- by **CM/ECF**
- by **Electronic Mail**
- by **Facsimile Transmission**
- by **First Class Mail**
- by **Hand Delivery**
- by **Overnight Delivery**



Kree Arvanitas

~~FILED~~
COURT OF APPEALS DIV 1
STATE OF WASHINGTON
2015 AUG 10 PM 2:42