

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.

RECEIVED
COURT OF APPEALS
DIVISION ONE
MAR 23 2016

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

RESPONDENT'S PETITION FOR REVIEW

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 197914, *Pro Hac Vice*
REED SMITH LLP
101 Second Street, Suite 1800
San Francisco, CA 94105
Tel: 415.543.8700
Fax: 415.391.8269

Attorneys for Plaintiff/Respondent The Republic of Kazakhstan

TABLE OF CONTENTS

	<u>Page</u>
I . Identity Of Petitioner And Introduction	1
II . Court Of Appeals Decision.....	4
III . Statement Of Issues Presented For Review	5
IV . Nature Of The Case And Decision Below.....	5
A. Email Accounts Of High-Level Kazakh Government Officials Are Hacked, And Attorney-Client Privileged Materials Are Stolen And Publicly Disseminated; Kazakhstan Issues A Subpoena Duces Tecum As Part Of Its Investigation	5
B. The Trial Court Denies LMC’s Motion To Quash The Subpoena Under Washington’s Shield Laws Finding That The Subpoena Did Not Seek Journalists’ Confidential Sources.....	8
C. The Court Of Appeals Reverses, Holding That The Shield Law Applies.....	9
V . Why Review Should Be Accepted	11
A. Review Is Warranted To Define A Confidential “Source” For Purposes Of The Shield Law	11
B. Review Is Warranted To Establish The Evidentiary Showing Needed To Invoke The Shield Law	17
VI . Conclusion	20

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Cont'l Cablevision, Inc. v. Storer Broad. Co.</i> , 583 F. Supp. 427 (D.C. Mo. 1984)	18
<i>Davis v. Cox</i> , 180 Wn. App. 514, 325 P.3d 255 (2014)	13
<i>Eugster v. City of Spokane</i> , 121 Wn.App. 799, 91 P.3d 117 (2004)	17
<i>In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)</i> , 830 F. Supp. 2d 114 (E.D. Va. 2011)	15
<i>In re Indiana Newspapers Inc.</i> , 963 N.E.2d 534 (Ind. Ct. App. 2012).....	13
<i>Smith v. Maryland</i> , 442 U.S. 735, 99 S. Ct. 2577, 61 L.Ed. 2d 220 (1979).....	16
<i>Snedigar v. Hoddersen</i> , 53 Wn. App. 476, 768 P.2d 1 (1989) (<i>aff'd in part</i> , <i>rev'd in part on other grounds</i> , 114 Wn.2d 153, 786 P.2d 781 (1990))	17
<i>State v. Nw. Magnesite Co.</i> , 28 Wn.2d 1, 182 P.2d 643 (1947) (en banc).....	14
<i>United States v. Sterling</i> , 724 F.3d 482 (4th Cir. 2013)	12
<i>United States v. Hively</i> , 202 F. Supp. 2d 886 (E.D. Ark. 2002).....	18
<i>United States v. Miller</i> , 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976).....	16

**Table of Authorities
(Continued)**

Page(s)

Statutes and Rules

735 Ill. Comp. Stat. § 8-902(c)	13
Del. Code Ann. Tit. 10, § 4320(5)	13
Mich. Comp. Laws Ann. § 767.5a	14
RAP 9.11	9
RAP 13.4(b)(4)	11
RCW 5.51.020	6
RCW 5.68.010	passim

Other Authorities

<i>Confidential Source</i> , Black's Law Dictionary (10th ed. 2014)	13
Laws of 2007, ch. 196, H.B. 1366, Final Bill Report, eff. July 22, 2007	11
<i>The Wall Street Journal Glossary of Terms: Journalism</i> at http://info.wsj.com/college/glossary/journalism.pdf	13

I. Identity Of Petitioner And Introduction

Respondent The Republic of Kazakhstan respectfully petitions this Court for review and reversal of the Court of Appeals' published decision in this matter. The decision raises novel issues of public importance regarding the journalist's privilege under Washington law.

The Shield Law, RCW 5.68.010, codifies a common law journalist's privilege that protects journalists from revealing their confidential sources of information. The statutory scheme protects not only journalists, but also third parties who might have information leading to the identification of a journalist's confidential source. Although the statute does not expressly define "source," that word is a term of art in journalism that connotes the person who provides information to the journalist for a story. Other states with similar statutory protections for journalists' confidential sources have endorsed this definition. And many other courts have recognized that parties must present detailed supporting evidence showing they are entitled to these protections.

In the proceedings below, Kazakhstan is investigating a serious computer security breach: someone hacked into email accounts belonging to Kazakhstan's high-ranking officials, stole thousands of confidential emails and documents containing sensitive matters of State and attorney-client privileged information, and posted them on third-party websites. As

part of its investigation, Kazakhstan issued a document subpoena to a Washington-based domain name registrar named eNom, seeking information regarding (1) the person who registered the domain name for one of the websites posting the stolen, privileged materials, and (2) the computer used to register that domain name. A company named LLC-Media Consult (“LMC”) operates that website.

LMC invoked the Shield Law to quash the subpoena on the grounds that its website was an online news organization. Kazakhstan contended that the Shield Law did not apply because (1) its subpoena did not seek confidential journalist sources, and (2) LMC failed to present any evidence that the person who registered the website had provided journalists with the stolen documents—i.e., that this person was a confidential source. This was particularly true because the online news organization *admitted* during the course of the appeal that it did *not* receive the stolen documents from any confidential source, but instead had retrieved them from one of the other publicly available third-party websites that posted the documents.

Rejecting Kazakhstan’s arguments, the Court of Appeals held that the Shield Law broadly prevented the disclosure of “any information that would tend to identify a source.” According to the court, because the subpoena was part of an effort to establish the *hackers’* identities, the

Shield Law applied and protected against the requested discovery regarding the domain name registrant. This is the first published decision tackling the Shield Law and it warrants this Court's review.

First, although the Court of Appeals did not define the word "source," its holding effectively means that the *hackers* were a journalistic "source" within the meaning of the statute. But it was undisputed that the online news organization retrieved the stolen materials from a public, third party-website and did *not* receive them from the hackers. Thus, the court's interpretation of the word "source" strayed well beyond how journalists use that phrase—that is, a person who provides materials directly to journalists for a story. Importantly, it departed from how other states define "source" for purposes of their journalist privilege statutes. And it disregarded the statutory requirement that the "source" must have a reasonable expectation of confidentiality to qualify for protection.

Second, the Court of Appeals applied the Shield Law without any discussion of the evidentiary showing necessary to invoke the privilege. This shortcoming was problematic because LMC did not present any evidence connecting the news organization to the hackers or explaining how revealing the identity of whoever registered the domain name of the website posting the stolen materials or of the computer used for that purpose would lead to the disclosure of confidential news sources.

Caselaw from other jurisdictions makes clear that a party invoking the journalist privilege must do more than simply assert that media considerations are in play—the party must support its request with specific evidence showing that the privilege applies. The Court of Appeals departed from this rule and turned the burden of proof on its head.

The potential consequences of the Court of Appeals' decision loom large. Under the court's holding, the Shield Law would prevent a party from discovering a thief's identity, so long as a reporter happened upon the stolen materials and wrote an article about them. There would be no need, moreover, for a party resisting disclosure to explain how the journalist's privilege arises, other than to say that a reporter possesses the stolen materials. That construct is not the rule elsewhere and it should not be the rule in Washington. Kazakhstan respectfully requests that the Court grant this petition.

II. Court Of Appeals Decision

Kazakhstan petitions this Court to review the February 22, 2016, published opinion issued by Division 1 of the Court of Appeals. The Court of Appeals reversed the trial court's order denying LMC's motion to quash Kazakhstan's subpoena duces tecum and held that the subpoena was prohibited under Washington's Shield Law. A copy of the opinion is attached as Appendix A.

III. Statement Of Issues Presented For Review

(1) What is the definition of a journalist’s confidential “source” for purposes of invoking the journalist’s privilege under Washington’s Shield Law, RCW 5.68.010?

(2) What evidentiary showing is necessary to meet the moving party’s burden of proof under the Shield Law?

IV. Nature Of The Case And Decision Below

A. Email Accounts Of High-Level Kazakh Government Officials Are Hacked, And Attorney-Client Privileged Materials Are Stolen And Publicly Disseminated; Kazakhstan Issues A Subpoena Duces Tecum As Part Of Its Investigation

In January 2015, Kazakhstan discovered that unidentified hackers had broken into the email accounts of high-ranking officials in the Kazakhstan government and stolen 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) 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)

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, alleging violations of state and federal computer privacy laws. (CP 50-57; Tr. 13) 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 federal computer privacy laws. (CP 192-201)

In connection with the California action, Kazakhstan issued several subpoenas duces tecum to different entities in an effort to gather documents identifying the hackers. One of these entities was eNom, a Kirkland company and the domain name registrar for www.respublika-kaz.info.¹ (CP 1-16) The eNom subpoena was issued pursuant to Washington's interstate discovery act [RCW 5.51.020] and sought, among other things: (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

¹ A domain name registrar is an accredited organization that manages and controls the reservation of internet domain names. (CP 34-35 ¶¶6-8) A domain name registrant is the person or entity who reserves the internet domain name.

corresponding IP Addresses and/or Mac Addresses from which the domain name was registered, created or modified.

Kazakhstan suspected that a Kazakh national named Mukhtar Ablyazov and his supporters were responsible for the hacking and theft. (CP 210) An English court previously had entered two judgments against Ablyazov, finding that he defrauded a Kazakh bank of billions of dollars. (CP 206 ¶¶20; CP 223-26) Ablyazov has maintained close ties with Irina Petrushova, who is the editor-in-chief of an online Russian-language newspaper named Respublika and co-owner of LMC. (CP 78 ¶4; CP 204-05 ¶¶12-19; CP 207 ¶¶26-29, 31-32) LMC, in turn, operates the online version of Respublika, which has published articles asserting that the pursuit of Ablyazov and his conviction in the English High Court for the bank fraud scheme are politically motivated. (CP 209 ¶¶40-44)

Respublika's main website is none other than www.respublika-kaz.info—the very same website posting the stolen documents. (CP 77 ¶3) Many of the stolen, privileged documents related to the fraud proceedings against Ablyazov. (CP 210 ¶55) Consequently, Kazakhstan has reason to believe that the hacking and public dissemination of privileged documents were part of a broader attempt to sway public opinion in Ablyazov's favor and minimize the fact that a court has found

Ablyazov to have committed multi-billion dollar fraud against a Kazakh bank. (CP 206 ¶23; CP 209-11 ¶¶40-44, 55-56)

B. The Trial Court Denies LMC's Motion To Quash The Subpoena Under Washington's Shield Laws Finding That The Subpoena Did Not Seek Journalists' Confidential Sources

LMC—not eNom—appeared and moved to quash the subpoena, contending among other things that the subpoena was improper under Washington's Shield Law. (CP 21-31) LMC proffered a declaration from Petrushova, most of which set forth Petrushova's belief that Kazakhstan had persecuted her and other journalists and that Kazakhstan was seeking the domain registrant's identity because it intended to pursue unfounded criminal charges against him or her. (CP 77-90) Petrushova 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.*) Kazakhstan denied that it targeted opposition journalists. (CP 205 ¶16)

The trial court agreed with Kazakhstan that its subpoena did not seek information regarding a confidential source and therefore was not precluded under the Shield Law. (Tr. 26) It denied LMC's motion to quash and directed eNom to produce documents, except that: (1) eNom was not required to produce "billing information," and (2) the produced documents were for attorneys' eyes only. (CP 412) The trial court retained jurisdiction over the matter "if there's any violation of that order." (Tr. 31)

C. The Court Of Appeals Reverses, Holding That The Shield Law Applies

LMC appealed. During the appeal, Respublika revealed in the New York action that its journalists found the stolen "documents the same way the rest of the world did—after 69 gigabytes of documents were anonymously posted to kazaword.wordpress.com." (The Court of Appeals received this statement into evidence pursuant to Rule of Appellate

Procedure 9.11). (Opn. at 13 nn.21, 22) In other words, despite LMC telling a Washington state court that Kazakhstan's subpoena improperly sought the identity of Respublika's confidential source of the stolen materials, Respublika was telling a New York federal court that it did not obtain them from a confidential source at all.

The Court of Appeals nevertheless reversed. According to the court, "[t]he heart of the dispute is whether this subpoena seeks these records and information 'for the purpose of discovering the identity of a source'" or information that "would tend to identify the source where such source has a reasonable expectation of confidentiality." (Opn. at 11 (quoting RCW 5.68.010(1)(a))) The court further explained that Kazakhstan sought "to establish either that the registrants are the hackers, or that they have information that can lead to the hackers." (Opn. at 12) However, the court held that "[b]y seeking to establish that the registrants are the hackers, Kazakhstan's purpose is to identify 'a source of any news or information'" in violation of the Shield Law. (Opn. at 12) Similarly, the court held that "[b]y seeking to establish a link to the hackers, Kazakhstan's purpose is to obtain information 'that would tend to identify' a source of news or information." (Opn. at 12)

The Court of Appeals rejected Kazakhstan's argument that the word "source" had a special meaning in the journalism context that

referred to the person who gave the stolen materials directly to the journalist for a story. (Opn. at 12-13) Although the Court recognized that “several cases and technical definitions” supported that view, it nevertheless held that the Shield Law’s plain language was “very broad” and protected against disclosure of the identity of “a source” or information that “*would tend to identify a source.*” (Opn. at 12-13) (emph. orig.)

V. Why Review Should Be Accepted

The Court of Appeals’ erroneous holding raises novel issues of substantial public importance [RAP 13.4(b)(4)], the resolution of which will determine the scope of the journalist’s privilege under Washington’s Shield Law and the evidentiary showing required to invoke the privilege. Unless review is accepted and the decision reversed, the Court of Appeals’ overly broad interpretation of the Shield Law exceeds the First Amendment and public policy principles that underlie the privilege, and unnecessarily inhibits legitimate discovery and criminal investigations.

A. Review Is Warranted To Define A Confidential “Source” For Purposes Of The Shield Law

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. The Shield Law also protects 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.*

As to nonnews media entities, 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).

No cases discuss the Shield Law in a manner that illuminates these provisions.² In particular, neither the statute nor its legislative history defines a “source” or “confidential source.”

² Only two other cases cite the Shield Law, and neither discussed it in any detail. See *United States v. Sterling*, 724 F.3d 482, 532 (4th Cir.

[Footnote continued on next page]

In journalist parlance, the word “source” is a “term of art[.]” *In re Indiana Newspapers Inc.*, 963 N.E.2d 534, 537 (Ind. Ct. 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.”) (last visited March 20, 2016).

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).

Plus, at least three states whose statutes define “source” embrace this view. *See, e.g.*, Del. Code Ann. Tit. 10, § 4320(5) (defining source as “a person from whom a reporter obtained information by means of written or spoken communication or the transfer of physical objects”); 735 Ill.

[Footnote continued from previous page]
2013) (noting thirty-nine states plus the District of Columbia have statutory journalist’s privileges); *Davis v. Cox*, 180 Wn. App. 514, 546 n.11, 325 P.3d 255 (2014) (explaining that the Shield Law permits disclosure of journalist work *product* where there is a clear and convincing showing of need).

Comp. Stat. § 8-902(c) (defining “source” to mean “the person or means from or through which the news or information was obtained”; Mich. Comp. Laws Ann. § 767.5a (using the word “informant” to refer to the confidential source)).

Here, Kazakhstan’s subpoena sought information regarding the identity of current and past domain name registrants. Although the Court of Appeals held that the subpoena was susceptible to the Shield Law, it did not point to any evidence that the domain name registrant provided journalists with the stolen documents or was connected to the stolen documents in any way. That is because, as the Court of Appeals recognized, Republika did not receive the stolen materials from any person, but retrieved them from a publicly available third-party website.

The Court of Appeal overlooked these facts and nevertheless held that the Shield Law applied because the subpoena was issued in the course of Kazakhstan’s investigation into the identities of *the hackers*. In other words, in the Court of Appeals’ view, the Shield Law protected the *hackers’* identities because the *hackers* were a journalistic “source” within the meaning of the statute.

That was error. The Washington Supreme Court recognized nearly sixty years ago that where a statutory term is undefined, “the information relative to the meaning of undefined words in a statute must be obtained

from experts in the business or work under consideration.” *State v. Nw. Magnesite Co.*, 28 Wn.2d 1, 57, 182 P.2d 643 (1947) (en banc). “Technical words, or terms of art relating to trade, when used in the statute dealing with the subject matter of such trade, are to be taken in their technical sense.” *Id.* (citation omitted).

Although the Shield Law was intended to protect the identity of journalists’ confidential sources, the word “source” itself is undefined. The Court of Appeals provided no definition of its own, but its treatment of the word source to include the *hackers* in this case is wholly inconsistent with how journalists themselves define a “source” and thus violates a core tenet of statutory construction that technical terms must be understood in their technical sense. It is also inconsistent with how other states have construed the journalists’ privilege, aligning the word “source” with its technical usage.

Moreover, the Court of Appeals disregarded the requirement that the “source” be confidential. *See* RCW 5.68.010(1)(a) (source must have “a reasonable expectation of confidentiality”). The whole point of the statute is to protect journalists’ sources who do not want their identities disclosed and who provide information on the condition that they remain unidentified. At the same time, nobody has a “legitimate expectation of privacy in information he voluntarily turns over to third parties.” *See In re*

Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 131 (E.D. Va. 2011) (citation omitted); *see also Smith v. Maryland*, 442 U.S. 735, 743–44, 99 S. Ct. 2577, 61 L.Ed. 2d 220 (1979) (telephone numbers); *United States v. Miller*, 425 U.S. 435, 442-43, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976) (bank records). But the Court of Appeals did not discuss confidentiality at all, holding instead that the Shield Law applied even though the materials were retrieved *not* from the hackers, but from a public, third party website.

The ramifications of the Court of Appeals’ statutory construction are startling. In the court’s view, a party is broadly prohibited from discovering a criminal’s identity simply because a journalist—who did not even receive any materials from the criminal—found the stolen materials and wrote an article about them. It does not matter how far removed the criminals are from the journalists or whether the criminals had a reasonable expectation of confidentiality. The logical consequence of the Court of Appeals’ construction is that the Shield Law would prohibit *any* attempt to investigate the identity of one who committed criminal theft, so long as a reporter obtained the materials from somewhere and wrote a story about it. That view stretches the Shield Law beyond absurdity.

The Shield Law was intended to protect journalists’ confidential sources and it should not apply where confidential sources did not provide

journalists with the materials for their reporting. The Court of Appeals' contrary construction should not be the rule. This Court should accept review and clarify that a "source" under the statute means a person who has a reasonable expectation of confidentiality and provides materials to a journalist for a story.

B. Review Is Warranted To Establish The Evidentiary Showing Needed To Invoke The Shield Law

The party asserting a First Amendment privilege has the prima facie burden of proof. *See Eugster v. City of Spokane*, 121 Wn.App. 799, 807, 91 P.3d 117 (2004) (party asserting 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) (*aff'd in part, rev'd in part on other grounds*, 114 Wn.2d 153, 170, 786 P.2d 781 (1990)). "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.”

No case has discussed the specifics of the moving party’s evidentiary showing under the Shield Law. Cases from other jurisdictions, however, make clear that the moving party may not invoke the journalists’ privilege merely through the “bare assertion that certain testimony may implicate confidential sources or information....” *United States v. Hively*, 202 F. Supp. 2d 886, 889 (E.D. Ark. 2002) (“Vague allegations of potential indication of confidential sources will not suffice to support a claimed qualified reporter’s privilege.” (citation omitted)). Rather, the moving party “must provide the court with particularized allegations or facts to support a privilege claim.” *Id.*; *see also Cont’l Cablevision, Inc. v. Storer Broad. 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”).

The Court of Appeals here applied the Shield Law without discussing LMC’s evidentiary burden. That void was particularly troubling because LMC did not attempt to draw any link between Kazakhstan’s subpoena for information regarding the domain name registrant’s identity and Respublika’s confidential source. 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 how the stolen materials were provided to Respublika's journalists in exchange for confidentiality. She *never* explained whether or how the domain name registrant provided the stolen materials to Respublika's journalists, much less that the domain name registrants ever possessed those stolen materials. (*Id.*) She *never* explained how disclosing the domain name registrant's identity would tend to identify the person who supposedly provided Respublika's journalists with the stolen materials. (*Id.*) Nor *could* she draw that link, because, as Respublika later admitted during the appeal, it retrieved the stolen materials from a public, third-party website.

The Court of Appeals overlooked these gaps, instead pointing to portions of Petrushova's declaration stating that (1) the domain "owner" was an individual and thus more vulnerable to purported reprisals than a media company would be, and (2) disclosure may place domain name registrants generally at risk. (Opn. at 5) But accusations of reprisals—which Kazakhstan denies—against the domain name registrant do not explain how disclosure of that person's identity would, in turn, tend to identify Respublika's confidential sources.

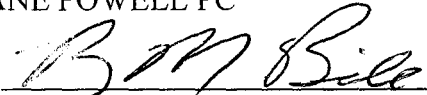
Ultimately, the Court of Appeals was satisfied that the Shield Law applied *not* because of any evidence LMC had proffered, but because Kazakhstan admitted that its subpoena was part of an investigation into the hackers' identities. Putting aside whether the hackers qualify as a "source" under the circumstances, the court's holding turned the burden of proof on its head. It relieved LMC from its burden of presenting evidence in support of its motion. Again, that should not be the law. This Court should accept review for this independent reason as well, and hold that any party seeking to invoke the Shield Law must come forward with a particularized showing demonstrating that the subpoena seeks to identify a journalist's confidential sources.

VI. Conclusion


For the foregoing reasons, this Court should grant review.

RESPECTFULLY SUBMITTED this 23rd day of March, 2016.

LANE POWELL PC

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

REED SMITH LLP

By  (per consent)
Robert N. Phillips, *Pro Hac Vice*
David J. de Jesus, *Pro Hac Vice*

*Attorneys for Plaintiff/Respondent
The Republic of Kazakhstan*

CERTIFICATE OF SERVICE

I hereby certify that on March 23, 2016, I caused to be served a copy of the foregoing **RESPONDENT'S PETITION FOR REVIEW** on the following person(s) in the manner indicated below at the following address(es):

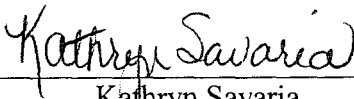
RECEIVED
COURT OF APPEALS
DIVISION ONE
MAR 23 2016

Robert N. Phillips
David J. de Jesus
Reed Smith LLP
101 Second Street, Suite 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**



Kathryn Savaria

APPENDIX A

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON

THE REPUBLIC OF KAZAKHSTAN,)
)
 Respondent,) No. 73391-5-1
)
 v.) DIVISION ONE
)
 DOES 1-100, inclusive,) PUBLISHED OPINION
)
 Defendants,)
)
 LLC MEDIA-CONSULT,)
)
 Appellant.) FILED: February 22, 2016

2016 FEB 22 AM 9:47
STATE OF WASHINGTON
COURT OF APPEALS

TRICKEY, J. — The Republic of Kazakhstan initiated a California state court lawsuit against 100 unnamed “John Doe” defendants.¹ Kazakhstan alleged that these defendants hacked into Kazakhstan’s government computer network and stole and published hundreds of privileged and confidential e-mails from high-ranking Kazakh officials in violation of California and United States law.

In connection with that lawsuit, Kazakhstan requested that the King County Superior Court issue a subpoena duces tecum to eNom, Inc., an Internet domain name registration company located in Kirkland, Washington. The subpoena seeks domain name registrant information and Internet Protocol (IP) and/or Mac addresses for a website operated by “Respublika,” an opposition newspaper based in Kazakhstan that published several of the stolen e-mails.

On appeal, we must interpret Washington’s news media shield law, RCW 5.68.010, and determine whether it protects the information sought by this

¹ Clerk’s Papers (CP) at 50-57.

subpoena. The trial court concluded that the news media shield law did not apply, and it denied third-party LLC Media-Consult's (LMC) motion to quash subject to certain modifications. We disagree and therefore reverse.

FACTS

Appellant LMC is a Russian limited liability company that operates the online publication of Respublika. Irina Petrushova, Respublika's founder and editor-in-chief, owns LMC with her brother. Petrushova founded Respublika in 2000, and the newspaper has been published online since September 2008. Its main website is "www.respublika-kaz.info."²

Published weekly, Respublika principally covers business and politics in Kazakhstan, a country in central Asia. According to Petrushova, Respublika is "a forum for expressing opposition to the political regime in Kazakhstan."³ It has consistently published articles critical of Kazakhstan's President Nursultan Nazarbayev. As a result, Petrushova asserts, Respublika's journalists have become targets of an aggressive intimidation campaign. In 2002, Petrushova left Kazakhstan in fear for her life.

Petrushova continues to run Respublika's editorial board and report on government corruption in Kazakhstan. Petrushova claims that the editorial team established various newspapers over the years, but the government shut down all of them. Printing houses in Kazakhstan refused to publish Respublika's newspapers, and the editorial team was forced to publish them on home printers and in Russia.

² CP at 77.

³ CP at 78.

According to Petrushova, in 2010, the Kazakh government blocked access to Respublika's online portal. As a result, in order to access Respublika's news from Kazakhstan, Respublika's readers have to use proxy servers and other programs that can work around domestic blocking. In 2013, a Kazakh court closed websites associated with Respublika. In 2014, pressure on Respublika mounted in Russia when Russian authorities seized a server that hosted Respublika's website.

In early 2015, Kazakhstan claimed that it had discovered a major breach of its computer systems. According to Marat Beketayev, the Executive Secretary of the Ministry of Justice of the Republic of Kazakhstan, e-mail accounts of several high-ranking government officials were hacked and thousands of e-mails and documents were stolen and posted to various websites. Kazakhstan claims that these e-mails and documents contain confidential and privileged material, including communications between Kazakhstan and its legal advisers who were advising the government on various sensitive matters. A website hosted by WordPress, "<https://kazaword.wordpress.com>," published several of these stolen e-mails.⁴ Respublika also published several of these e-mails, along with an article critical of the government.

Following these events, Kazakhstan commenced an action in Santa Clara, California superior court against 100 "John Doe" defendants, alleging violations of California and federal law.⁵ Kazakhstan also commenced an action against the

⁴ CP at 203; Report of Proceedings (RP) (Apr. 30, 2015) at 7, 12-13.

⁵ CP at 50-57.

unnamed Does in the United States District Court for the Southern District of New York, seeking injunctive relief and damages.⁶

On March 4, 2015, Kazakhstan initiated this limited action in King County Superior Court. Pursuant to RCW 5.51.020, the uniform interstate depositions and discovery act, Kazakhstan sought to serve a subpoena duces tecum on eNom, Inc., a domain name registration company located in Kirkland, Washington. For several years, eNom, Inc. has registered the domain name for Respublika's main website: "www.respublika-kaz.info."⁷ eNom, Inc. offers a domain privacy service called "ID Protect," which shields a domain name registrant's personal, identifying information.⁸ Respublika uses eNom's privacy service to shield its current and former registrants' information.

The subpoena duces tecum requested certain information associated with Respublika's domain name. Defining "domain name" as "www.respublika-kaz.info," it requested that eNom produce the following two⁹ categories of information:

1. Documents sufficient to show all details of all current and former registrants, including any underlying registrant using a privacy or proxy service, of the Domain Name including, but not limited to, his or her email address, physical address, phone number, and billing information, including any updated or revised details since registration.
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.^[10]

⁶ Br. of Appellant (LLC Media-Consult) at App. B.

⁷ CP at 86, 88.

⁸ CP at 34.

⁹ Initially, Kazakhstan requested three additional categories of documents but it later withdrew these requests.

¹⁰ CP at 10.

LMC, a nonparty, moved to quash the subpoena. LMC argued that the subpoena was oppressive and burdensome, violated Washington's news media shield law, and ran contrary to "core constitutional values."¹¹ It asserted that a protective order would be ineffective and unworkable and that the court could grant no effective relief short of quashing the subpoena.

LMC supported its motion with a declaration from Petrushova. Petrushova detailed threats against Respublika's members. For example, she asserted that one of Respublika's printers quit after finding a human skull on his doorstep. In other examples, Petrushova asserted that she received a funeral wreath that marked her for death, found a dog's headless body hung from one of Respublika's window grates with a threatening note, and found a dog's head outside her apartment door. She also asserted that Respublika's editorial board's office had been set on fire and that Respublika's newsroom had been firebombed.

In her declaration, Petrushova also stated several concerns about the consequences of disclosing information about Respublika's current and former domain name registrants. She declared that the current owner of the domain is an individual, not a company. She feared that the Kazakhstan government would bring unfounded civil and criminal claims against the domain name registrants and that the registrants would be at risk of physical danger, such as beating, kidnapping, and unlawful detention. She also worried that the financiers of the domain name would be persecuted and that the accounts would be frozen. And

¹¹ CP at 24.

she expressed concern about the effect of this disclosure on other opposition journalists:

Disclosure of domain registration and hosting details, both current and former, would undoubtedly lead to enormous pressures on Respublika's current and past registrars and hosting providers. The disclosure would lead to requests to Respublika's registrars and hosting providers to cancel its domains and shut down its websites. If our main domain were cancelled or shut down, Respublika would lose a large part of the audience that has been visiting that domain since September 15, 2008. The precedent would also have a tremendous chilling effect on the freedom of the press for any remaining opposition journalists who are risking their lives to report on Kazakhstan.^[12]

Along with her declaration, Petrushova included copies of newspaper articles detailing the political climate and media crackdown in Kazakhstan. She also included reports from human rights organizations that described Kazakhstan's restrictions on freedom of expression and classified Kazakhstan as one of the world's most repressive states.

Kazakhstan opposed the motion to quash. It argued that the news media shield law was inapplicable and that the subpoena was not burdensome or oppressive. In support of its position, Kazakhstan provided a declaration from Secretary Beketayev. He denied Petrushova's accusations that Kazakhstan targeted opposition journalists. He asserted that Petrushova and her husband were working for Mukhtar Ablyazov, a Kazakh national who has been found by an English court to have defrauded a Kazakh bank of \$4.6 billion. Secretary Beketayev asserted that Petrushova and her husband were working on behalf of Ablyazov to propagate the distribution of the hacked e-mails and documents.

¹² CP at 89.

A hearing on LMC's motion to quash occurred on April 30, 2015. After hearing argument from the parties, the trial court concluded that the news media shield law was inapplicable. But the court decided to limit discovery in two ways. First, the court ruled that Kazakhstan could not obtain billing information, and it struck this category from the subpoena. Second, the court limited the produced records to "Attorneys' Eyes Only."¹³ The trial court denied LMC's motion to quash the subpoena subject to these modifications. It entered an order stating as follows:

[e]Nom shall produce the documents in categories 1 and 2 of the subpoena, with the exception of "billing information," by Monday, May 4, 2015. Categories 3, 4, [and] 5 are withdrawn by [Kazakhstan]. The produced records shall be for attorneys' eyes only.¹⁴

LMC appealed to this court. A commissioner of this court granted LMC's motion for an emergency stay of the trial court's order.

ANALYSIS

We review a trial court's order granting or denying a motion to quash a subpoena for abuse of discretion. Eugster v. City of Spokane, 121 Wn. App. 799, 807, 91 P.3d 117 (2004). We also review 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). A court abuses its discretion if its decision is manifestly unreasonable or exercised on untenable grounds or reasons. Eugster, 121 Wn. App. at 807.

A court shall quash a subpoena if it requires disclosure of privileged or other protected information and no exception or waiver applies. CR 45(c)(3)(A)(iii).

¹³ RP (Apr. 30, 2015) at 30-31.

¹⁴ CP at 412.

Washington News Media Shield Law

LMC argues that the trial court erred in its interpretation of Washington's news media shield law. It contends that this shield law applies to the parties and records sought in this case, because the purpose of the subpoena is to identify a confidential source. We agree.

In general, “[t]he burden of showing that a privilege applies in any given situation rests entirely upon the entity asserting the privilege.” Guillen v. Pierce County, 144 Wn.2d 696, 716, 31 P.3d 628 (2001), reversed in part, Pierce County v. Guillen, 537 U.S. 129, 123 S. Ct. 720, 154 L. Ed. 2d 610 (2003). Accordingly, LMC has the burden of showing that the news media shield law applies.

No court has interpreted Washington's news media shield law. In determining the meaning and scope of a statute, we apply general principles of statutory construction. State v. Chester, 133 Wn.2d 15, 21, 940 P.2d 1374 (1997). Our primary purpose is to ascertain and effectuate the legislature's intent. Anderson v. Dussault, 181 Wn.2d 360, 368, 333 P.3d 395 (2014). We first examine the plain meaning of the statute. “When determining a statute's plain meaning, we consider ‘the ordinary meaning of words, the basic rules of grammar, and the statutory context to conclude what the legislature has provided for in the statute and related statutes.’” Darkenwald v. Emp't Sec. Dep't, 183 Wn.2d 237, 245, 350 P.3d 647 (2015) (quoting In re Forfeiture of One 1970 Chevrolet Chevelle, 166 Wn.2d 834, 838-39, 215 P.3d 166 (2009)). If the meaning is plain on its face, we give effect to that plain meaning. If the statute is ambiguous, we may look to other aids of statutory construction, such as the legislative history, to determine

the legislature's intent. State v. A.G.S., 182 Wn.2d 273, 277-78, 340 P.3d 830 (2014). Statutory construction is an issue of law that we review de novo.

Washington's news media shield law has its origins in common law. The United States Supreme Court left it to individual states to determine how broadly to recognize a reporter's privilege. Branzburg v. Hayes, 408 U.S. 665, 706, 92 S. Ct. 2646, 33 L. Ed. 2d 626 (1972). In Washington, our courts first recognized the privilege in Senear v. Daily Journal-American, 97 Wn.2d 148, 641 P.2d 1180 (1982). There, the Supreme Court held that journalists have a qualified common law privilege with respect to their sources of information, but it confined the privilege to civil cases. Senear, 97 Wn.2d at 151, 155. Two years later, in State v. Rinaldo, 102 Wn.2d 749, 755, 689 P.2d 392 (1984), the Supreme Court extended the qualified common law privilege for journalists to criminal cases.

In 2007, the legislature codified this privilege in RCW 5.68.010. In doing so, it extended the privilege both to members of the news media and to nonnews media parties.

RCW 5.68.010(1) applies to the "news media."¹⁵ Under subsection (1), no judicial, legislative, administrative, or other body may compel the news media to testify, produce, or otherwise disclose:

¹⁵ The term "news media" is defined by the statute as follows:

"(a) Any newspaper, magazine or other periodical, book publisher, news agency, wire service, radio or television station or network, cable or satellite station or network, or audio or audiovisual production company, or any entity that is in the regular business of news gathering and disseminating news or information to the public by any means, including, but not limited to, print, broadcast, photographic, mechanical, internet, or electronic distribution;

(b) Any person who is or has been an employee, agent, or independent contractor of any entity listed in (a) of this subsection, who is or has been

(a) The identity of a source of any news or information or any information that would tend to identify the source where such source has a reasonable expectation of confidentiality; or

(b) Any 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, including, but not limited to, any notes, outtakes, photographs, video or sound tapes, film, or other data of whatever sort in any medium now known or hereafter devised. This does not include physical evidence of a crime.

RCW 5.68.010(2) provides that a court may compel disclosure of the news or information described in subsection (1)(b) under certain circumstances. Thus, as the legislature explained in its final bill report, the news media has an absolute privilege with respect to the information contained in subsection (1)(a), and it has a qualified privilege with respect to the information contained in subsection (1)(b). FINAL B. REP. on H.B. 1366, 60th Leg., Reg. Sess. (Wash. 2007).

Washington's news media shield law also contains a provision for nonnews media parties. That subsection is RCW 5.68.010(3). In relevant part, it states:

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. . . .

engaged in bona fide news gathering for such entity, and who obtained or prepared the news or information that is sought while serving in that capacity; or

(c) Any parent, subsidiary, or affiliate of the entities listed in (a) or (b) of this subsection to the extent that the subpoena or other compulsory process seeks news or information described in subsection (1) of this section." RCW 5.68.010(5)(a),(b),(c).

Here, Kazakhstan's subpoena seeks information from eNom, Inc., an Internet domain name registration company. The parties do not dispute that eNom is a nonnews media party, and thus, the relevant statutory provision is RCW 5.68.010(3).

The parties also do not dispute that the information and records sought in this case fall within the scope of RCW 5.68.010(3), that is, they are "records, information, or other communications relating to business transactions between such nonnews media party and the news media." Kazakhstan seeks:

1. Documents sufficient to show all details of all current and former registrants, including any underlying registrant using a privacy or proxy service, of the Domain Name including, but not limited to, his or her email address, physical address, phone number, and billing information,^[16] including any updated or revised details since registration.
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.^[17]

The heart of the dispute is whether this subpoena seeks these records and information "for the purpose of discovering the identity of a source or obtaining news or information described in subsection (1) of this section." RCW 5.68.010(3). Again, subsection (1) protects against disclosure of, among other things, "The identity of a source of any news or information 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).

¹⁶ The trial court struck "billing information" from the subpoena. RP (Apr. 30, 2015) at 29.

¹⁷ CP at 3.

As Kazakhstan stated in the trial court and on appeal, it seeks the documents in this subpoena for the purpose of identifying the individual who illegally hacked into the e-mail accounts and stole the confidential materials. Specifically, it seeks the IP and Mac addresses to cross-reference against IP addresses that accessed Kazakh government servers at the time of the alleged hacking. And it seeks the domain name registrants' identities because they "can help confirm who hacked into Kazakhstan's computers and stole privileged documents."¹⁸

Kazakhstan seeks to establish either that the registrants are the hackers, or that they have information that can lead to the hackers. Both purposes are prohibited by the shield law. By seeking to establish that the registrants are the hackers, Kazakhstan's purpose is to identify "a source of any news or information." RCW 5.68.010(1)(a). By seeking to establish a link to the hackers, Kazakhstan's purpose is to obtain information "that would tend to identify" a source of news or information. RCW 5.68.010(1)(a). Accordingly, this subpoena falls within the plain language of the statute.

Kazakhstan argues that in journalist parlance the word "source" is a term of art.¹⁹ It cites several cases and technical definitions to support this argument, including one authority that defines "source" as a "[p]erson, record, document or event that provides the information for the story."²⁰ Relying on these definitions, Kazakhstan contends that for the news media shield law to apply, LMC must

¹⁸ Br. of Resp't at 43.

¹⁹ Br. of Resp't at 27.

²⁰ Br. of Resp't at 28 (citing *The Wall Street Journal Glossary of Terms: Journalism*, <http://www.info.wsj.com/college/glossary.journalism.pdf>).

establish that the registrant is the source that provided the stolen materials directly to Respublika's journalist, or that the registrant would tend to identify the source that provided the stolen materials directly to Respublika's journalist.

Kazakhstan further claims that LMC is unable to do this, given its statements that it obtained the e-mails from a public source—the WordPress website. In New York federal court, LMC filed a letter²¹ stating that “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.”²² LMC's attorney made similar representations to this court at oral argument for this appeal.

We decline to read the statute so narrowly. The plain language of RCW 5.68.010(1)(a) is very broad. It protects against disclosure of the identity of a source of *any* news or information. It also protects against the disclosure of any information that *would tend to identify* a source. By requesting registrant information and IP addresses for the purpose of discovering the identity of the hackers, Kazakhstan impermissibly seeks information that falls within the plain language of RCW 5.68.010(1)(a). Accordingly, LMC's statement that it obtained the stolen materials from a third-party website does not prevent it from invoking the news media shield law.

CONCLUSION

We hold that the Washington news media shield law prevents disclosure of the information sought by this subpoena. The trial court abused its discretion when

²¹ We previously granted Kazakhstan's motion to supplement the record with this additional evidence.

²² Republic of Kazakhstan's Motion to Permit Additional Evidence on Review at Ex. A.

it denied LMC's motion to quash. In light of this conclusion, we need not address LMC's arguments that the discovery order should be reversed because Kazakhstan is engaging in improper claim splitting or because the subpoena violates the Washington Constitution. We also need not address LMC's arguments that the discovery order is burdensome and oppressive.

We reverse the denial of the motion to quash the subpoena and remand to the trial court to dismiss the action.

Trickey, J.

WE CONCUR:

Schivelder, J.

Becker, J.