Cause No. 19-0845

In the Supreme Court of Texas

In re Toyota Motor Sales, U.S.A., Inc. and Toyota Motor Corporation,

Relators,

Original Proceeding from Cause No. DC-16-15296,
134th District Court, Dallas County, Texas

Brief of Amici Curiae Lawyers for Civil Justice and Chamber of Commerce of the United States of America in Support of Petition for Writ of Mandamus

Stephanie Dooley Nelson
State Bar No. 24002006
stephanie.nelson@tklaw.com

Thompson & Knight LLP
One Arts Plaza
1722 Routh Street, Suite 1500
Dallas, Texas 75201
Phone: (214) 969-1700
Fax: (214) 969-1751

Jennifer Henry
State Bar No. 15859500
jennifer.henry@tklaw.com

Thompson & Knight LLP
777 Main Street, Suite 3300
Fort Worth, Texas 76102
Telephone: (817) 347-1733
Facsimile: (214) 999-1616

Counsel for Amici Curiae
Lawyers for Civil Justice and
Chamber of Commerce of the United States of America

Identity of Parties and Counsel

Relators	Counsel for Relators
Toyota Motor Sales, USA, Inc.	Allyson N. Ho
Toyota Motor Corporation	Bradley G. Hubbard
	Gibson, Dunn & Crutcher LLO
	2100 McKinney Avenue, Suite 1100
	Dallas, Texas 75201
	Anne M. Johnson
	Nina Cortell
	Jason N. Jordan
	Haynes and Boone, LLP
	2323 Victory Avenue, Suite 700
	Dallas, Texas 75219
	Victor Vital
	Benjamin T. Pendroff
	Barnes & Thornburg LLP
	2121 North Pearl Street, Suite 700
	Dallas, Texas 75201
	James W. Halbrooks, Jr.
	Suzanne H. Waner
	Bowman and Brooke LLP
	5830 Granite Park, Suite 1000
	Plano, Texas 75024
	Winstol D. "Winn" Carter, Jr.
	Claire Swift Kugler
	John M. Deck
	Morgan, Lewis & Bockius LLP
	1000 Louisiana, Suite 4000
	Houston, Texas 77002

Respondent
Honorable Dale Tillery
Judge, 134th District Court
Dallas County, Texas
600 Commerce Street, Box 650
6th Floor West
Dallas, Texas 75202

Real Parties in Interest
Benjamin Thomas Reavis, and
Kristie Carol Reavis,
Individually and as Next Friends
of E.R. and O.R., Minor
Children

Counsel for Real Parties in Interest
Frank L. Branson
Frank L. Branson, P.C.
4514 Cole Avenue, Suite 1800
Dallas, Texas 75205

Eric T. Stahl
Law Offices of Eric T. Stahl
3212 Drexel Drive
Dallas, Texas 75205

Eugene A. "Chip" Brooker
Brooker Law, PLLC
750 North Saint Paul Street, Suite 600
Dallas, Texas 75201

Harry M. Reasoner
Marie R. Yeates
Benjamin H. Moss
Vinson & Elkins, LLP
1001 Fannin Street, Suite 2500
Houston, Texas 77002

Michael A. Heidler
Vinson & Elkins, LLP
2801 Via Fortuna, Suite 100
Austin, Texas 78746

Amicus Curiae	Counsel for Amicus Curiae
Lawyers for Civil Justice and Chamber of Commerce of the United States of America	Jennifer Henry Thompson & Knight LLP 777 Main Street, Suite 3300 Fort Worth, Texas 76102 Stephanie Dooley Nelson Thompson & Knight LLP One Arts Plaza 1722 Routh Street, Suite 1500 Dallas, Texas 75201

Table of Contents

Index of Authorities

CASES

RULES

OTHER AUTHORITIES

Identity and Interest of Amicus Curiae

This brief is tendered on behalf of Lawyers for Civil Justice ("LCJ") and the Chamber of Commerce of the United States of America ("Chamber"), which are paying a stipend for the preparation of this brief. LCJ is a national coalition of corporations, law firms, and defense trial lawyer organizations that advocates for procedural rule reforms in to order to: (1) promote balance and fairness in the civil justice system; (2) reduce costs and burdens associated with litigation; and (3) advance predictability and efficiency in litigation. LCJ supports procedural rules that are fair and efficient for all litigants, regardless of the litigants' positions in any particular lawsuit.

The Chamber is the world's largest business federation. The Chamber directly represents 300,000 members and indirectly represents more than three million businesses and professional organizations of every size, in every sector, and from every geographic region of the country. An important function of the Chamber is to represent its members' interests in matters before the courts, Congress, and the Executive Branch.

Cybersecurity and the preservation of the confidential nature of an organization's information-technology systems are of central concern to amici's membership. As frequent litigants, amici's members routinely produce—subject to protective orders—confidential commercial and proprietary information.

Amici's members rely on protective orders to preserve the confidentiality of their information. The trial court's refusal to treat information about the framework and security of a company's information-technology systems as "confidential information" under the court's protective order establishes a dangerous precedent. As cybercrimes have escalated from hypothetical to commonplace and "discovery about discovery" becomes more accepted, data privacy protection is an increasingly important priority for litigants. Against this backdrop, amici urge the Court to consider the importance of courts protecting the confidentiality of discovery materials that could subject parties to cybersecurity intrusions as it reviews Relators' request for mandamus relief.

Introduction

This Court recently recognized that "[e]lectronic discovery plays an increasingly significant role in litigation" and "discovery disputes involving electronically stored information (ESI) are a growing litigation concern." *In re State Farm Lloyds*, 520 S.W.3d 595, 598-99 (Tex. 2017). To obtain ESI, litigants often conduct "discovery about discovery"—i.e., "discovery about an opponent's e-discovery processes and the manner in which a party preserves, identifies, collects, searches, and produces ESI." Craig B. Shaffer, *Deconstructing "Discovery About Discovery"*, 19 SEDONA CONF. J. 215, 215 (2018). Also known as "process-directed" discovery, the requested information has nothing to do with

the merits of the case. *See id.* at 216. Instead, it deals with the manner and efficacy of the production process itself and often delves deep into the ways an entity has set up its information-technology infrastructure to manage, store, and access data about its business and its customers. *See id.* While such information may provide a "roadmap" for litigants in conducting e-discovery, that "roadmap" can also place the infrastructure and data contained within it at risk if it is publicly disclosed. *See Sheridan v. U.S. Office of Pers. Mgmt.*, 278 F. Supp. 3d 11, 23 (D.D.C. 2017) (noting that disclosure of database information could increase the risk that a malicious actor might hack into the system and access confidential data housed in the system). Moreover, if a company derives a competitive advantage due to its investment in its own proprietary information-technology architecture, public disclosure of that information can harm the company by allowing competitors to see what it has done. *See, e.g.*, *How Information Gives You Competitive Advantage*, HARVARD BUSINESS REV., https://hbr.org/1985/07/how-information-gives-you-competitive-advantage (last visited October 30, 2019).

Whether courts should permit process-directed discovery is beyond the scope of this brief; however, if courts permit it, courts should support the responding party's efforts to protect the confidentiality of discovery regarding its information-technology infrastructure. Not only is there no independent relevance of process-directed discovery, there is no public interest in disclosure of such information in any circumstance. The failure to uniformly enforce

protective orders to secure IT-system discovery will have substantial, negative consequences and expose litigants to unwarranted risk. This concern is particularly acute given the rampant nature of cybersecurity attacks that can cripple businesses, government entities, and critical infrastructure sectors.

As in *In re State Farm*, the Court now has the opportunity to "enter the fray" and provide "further clarity regarding ESI"—this time regarding the importance of maintaining the confidentiality of process-directed discovery about the responding party's ESI systems. The Court should request briefing on the merits and, ultimately, grant Relators' petition for writ of mandamus.

Argument

I. The threat of cyberattacks is real, and the burden of those attacks on the economy is substantial.

Now more than ever, data holders must guard against cyberattacks by vigilantly protecting the information-technology systems that house their data because such attacks and data breaches are becoming more and more prevalent. For example:

- In October 2019, Florida-based Trial Works, a software company that manages electronic records for thousands of law firms nationwide, had digital legal documents held hostage under a ransomware threat. *See* Jay Weaver, *Ransomware Incident Blocked Some Law Firms from Countless Records*, MIAMI HERALD, October 30, 2019, https://www.miamiherald.com/news/local/article236645058.html.

- American Medical Collection Agency announced in June 2019 that a data security breach of its systems reportedly compromised patient data that various medical diagnostic testing companies had provided to AMCA for billing and collection purposes, including Quest Diagnostics, Inc., Laboratory Corporation of America Holdings, Bio-Reference Laboratories, Inc., and others. *See In re Am. Med. Collection Agency, Inc.*, MDL 2904, 2019 WL 4010740, at *1 (U.S. Jud. Pan. Mult. Lit. July 31, 2019).

- In 2017, Equifax Inc. announced that criminal hackers breached Equifax's computer network and obtained a vast amount of personally identifiable information in the company's custody affecting more than 148 million Americans. *See In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1205 (N.D. Ga. 2019).

- In 2016, Yahoo! announced that a data security breach of its network occurred in late 2014 in which the personal account information of at least 500 million Yahoo! users was stolen. *See In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 223 F. Supp. 3d 1353, 1354 (U.S. Jud. Pan. Mult. Lit. 2016).

- In 2015, Premera disclosed that its computer network had been breached, compromising the confidential information of approximately 11 million current and former members, affiliated members, and employees of Premera, including the names, dates of birth, social security numbers, member identification numbers, mailing addresses, telephone numbers, email addresses, medical claims information, financial information, and other protected health information. *See In re Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2019 WL 3410382, at *1 (D. Or. July 29, 2019).

- During the 2013 holiday shopping season, computer hackers stole credit- and debit-card information and other personal information for approximately 110 million customers of Target's retail stores, resulting in one of the "largest breaches of payment-card security in United States retail history." *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014).

In short, the risk of a malicious attack is not an imagined threat. It is a reality that data holders face daily. As the Director of the Federal Bureau of Investigation succinctly explained in a 2018 speech:

> We're seeing these diverse threats in every company, at every level. . . . The days of wondering if you're going to be the next victim are gone. Now it's a matter of how often you'll get hit, and how bad it'll be. And we're not talking just about defense contractors or critical infrastructure. Every company is a target. Every single bit of information, every system, and every network is a target. Every link in the chain is a potential vulnerability.

Christopher Wray, Director of the FBI, The FBI and Corporate Directors: Working Together to Keep Companies Safe from Cyber Crime, Address Before the National Association of Corporate Directors Global Board Leaders Summit (October 1, 2018), *available at* https://www.fbi.gov/news/speeches/the-fbi-and-corporate-directors-working-together-to-keep-companies-safe-from-cyber-crime (last visited October 30, 2019).

The impact of cybercrimes is immense, including exposure of personal information, identity theft, denials of service, data and property destruction, business disruption, ransoms, and theft of proprietary data, intellectual property, and financial and strategic information. The resulting financial impact is devastating. In a February 2018 report, the Council of Economic Advisors estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 alone.

Moreover, a litigant's security measures could be compromised if litigants disclose confidential information about their IT-system architecture as part of process-directed discovery and courts decline to safeguard that information through valid protective orders. That is precisely what happened here.

II. Information about Toyota's information-technology infrastructure is confidential "commercial information," and its disclosure could expose Toyota to an increased risk of cyberattacks.

In the trial court, Toyota sought to protect its sensitive information disclosed in depositions that focused on the company's ESI systems. Toyota apparently did not seek to limit the use of the data in the litigation below and did not challenge the plaintiffs' ability to share the data with attorneys in other cases (subject to protective orders). Toyota, however, did seek to limit disclosure of its sensitive information outside the parameters of the litigation process.

By its terms, the trial court's protective order allowed the parties to designate "Confidential Information," which the order defines as "information that constitutes a trade secret or reveals confidential research, development, or commercial information." (MR.022) Toyota maintains that testimony about the structure, contents, use, access policies, business purposes, and locations of its information-technology databases is confidential and commercially valuable. This type of information has unique qualities, is proprietary, and companies have a protectable interest in it. Indeed, companies generally treat this type of information as confidential, carefully guard it, and would be alarmed by a court's

refusal to protect its confidentiality—particularly when the information is not relevant to the merits of the litigation. Thus, at a minimum, that information would plainly fall within the scope of "commercial information" the protective order was designed to keep confidential. The trial court and court of appeals erred in construing "Confidential Information" to exclude Toyota's confidential database information.

The trial court's error warrants this Court's intervention through mandamus relief because the discovery at issue is precisely the type of information that can give malicious actors a "head start" and thereby render a company more vulnerable to cyberattacks. Allowing the disclosure of a company's information-technology infrastructure is akin to disclosing the blueprint of a house, showing where valuables are kept and describing the home's security system. *See* Nat'l Institute of Standards & Technology Rick Management Guide for Information Technology (2002) at § 4.1.1 (IT-system architecture is a basic technical security control needed to secure data).

Moreover, the information at issue also reportedly includes the identity of the persons who have access to Toyota's various databases. Failing to keep their identity confidential increases the likelihood that those individuals will be targets of spear-phishing attacks. In short, the more information cybercriminals have about Toyota's information-technology systems, the easier it will be for them to access the information in those systems. *See Sheridan*, 278 F. Supp. 3d at 23

(noting that disclosure of database information could increase the risk that a malicious actor might hack into the system and access confidential data housed in the system).

III. Public policy favors maintaining the confidentiality of information-technology discovery.

A litigant's interest in protecting from disclosure confidential information about its information-technology infrastructure greatly outweighs any competing interest in the public disclosure of that information, and those competing interests should inform the trial court's case management. As discussed above, litigants have a significant interest in protecting from disclosure their confidential discovery materials pertaining to information technology. Maintaining the confidentiality of this type of information lessens the risk of cyberattacks and hacking.

In contrast, there is no public interest in the disclosure of this type of information-technology discovery. Once the requesting party utilizes the process-directed discovery to create the framework for conducting its *merits* discovery, the process-directed discovery serves no purpose. It has no connection to the merits of the case, and thus it plays no role in the trial or summary disposition of the case. *See* Deconstructing "Discovery About Discovery," 19 SEDONA CONF. J. at 217 (opining that reasonable case

management should "distinguish between 'merits-directed discovery' and 'process-directed discovery.'").

According to Toyota's petition for writ of mandamus, that is the case here: the deposition testimony at issue was not relevant to the merits of the case and was not introduced at trial. Thus, the public disclosure of deposition testimony about Toyota's information-technology databases would serve no interest, particularly given that the protective order would allow the disclosure of that information to counsel in other actions arising out of the same or similar facts (MR.023). Trial courts should consider the parties' competing interests in evaluating whether process-directed discovery should be subject to protection. *See generally In re State Farm Lloyds*, 520 S.W.3d at 595 (holding that when electronic data in a reasonably usable form is readily available, trial courts must balance the burdens against the benefits in ordering production in a different form).

Further, the trial court's error in ruling that the challenged information-technology discovery is not "confidential information" under the protective order could have a chilling effect on other litigants. Here, Toyota (like many litigants) produced witnesses for deposition to provide the requested process-directed discovery, reasonably believing that the requested information would remain confidential by virtue of the protective order. If courts do not enforce protective orders to prohibit the public disclosure of information-technology systems, parties will be less willing to agree to open and broad discovery

(including process-directed discovery). The result will be more discovery disputes, a less efficient discovery process, and increased litigation costs—all of which are contrary to the objectives of the rules of civil procedure. *See* TEX. R. CIV. P. 1 (objective of the rules is for litigants to achieve a "just, fair, equitable and impartial adjudication ... with as great expedition and dispatch and at the least expense ... as may be practicable").

Conclusion

For these reasons, amici respectfully urge the Court to request briefing on the merits and ultimately grant Relators' request for mandamus relief.

Respectfully submitted,

By: */s/ Jennifer Henry*
Jennifer Henry
State Bar No. 15859500
jennifer.henry@tklaw.com
Thompson & Knight LLP
777 Main Street, Suite 3300
Fort Worth, TX 76102
Telephone: (817) 347-1733
Facsimile: (214) 999-1616

Stephanie Dooley Nelson
State Bar No. 24002006
Stephanie.nelson@tklaw.com
Thompson & Knight LLP
One Arts Plaza
1722 Routh Street, Suite 1500
Dallas, Texas 75201
Phone: (214) 969-1700
Fax: (214) 969-1751

Counsel for Amici Curiae Lawyers for Civil Justice and the Chamber of Commerce of the United States of America

Certificate of Compliance

The undersigned counsel certifies that this petition complies with the typeface requirements of TEX. R. APP. P. 9.4(e), because it has been printed in a conventional typeface no smaller than 14-point except for footnotes, which are no smaller than 12-point. This document also complies with the word-count limitations of TEX. R. APP. P. 9.4(i), because it contains less than 4,500 words, excluding any parts exempted by TEX. R. APP. P. 9.4(i)(1).

/s/ Jennifer Henry
Jennifer Henry

Certificate of Service

On October 30, 2019 I electronically filed this Amicus Brief in Support of Petition for Writ of Mandamus with the Clerk of Court using the eFile.TXCourts.gov electronic filing system which will send notification of such filing to the following:

Allyson N. Ho
Bradley G. Hubbard
Gibson, Dunn & Crutcher LLO
2100 McKinney Avenue, Suite 1100
Dallas, Texas 75201

Anne M. Johnson
Nina Cortell
Jason N. Jordan
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219

Frank L. Branson
Frank L. Branson, P.C.
4514 Cole Avenue, Suite 1800
Dallas, Texas 75205

Eric T. Stahl
Law Offices of Eric T. Stahl
3212 Drexel Drive
Dallas, Texas 75205

Eugene A. "Chip" Brooker
Brooker Law, PLLC
750 North Saint Paul Street, Ste 600
Dallas, Texas 75201

Harry M. Reasoner
Marie R. Yeates
Benjamin H. Moss
Vinson & Elkins, LLP
1001 Fannin Street, Suite 2500
Houston, Texas 77002

Michael A. Heidler
Vinson & Elkins, LLP
2801 Via Fortuna, Suite 100
Austin, Texas 78746

Jonathan Manning
Law Offices of Gallerson & Yates
2110 Walnut Hill Lane, Suite 200
Irving, Texas 75038

/s/ Jennifer Henry
Jennifer Henry