Cause No. 348-362718-25

KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY,	§	IN THE DISTRICT COURT OF
Plaintiff,	§	TARRANT COUNTY, TEXAS
v.	§	
GRAPEVINE–COLLEYVILLE INDEPENDENT SCHOOL DISTRICT	§	348th JUDICIAL DISTRICT
Defendant.		

PLAINTIFF KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY'S REPLY IN SUPPORT OF PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT

Thomas S. Leatherbury
State Bar No. 12095275
THOMAS S. LEATHERBURY LAW, PLLC
1901 N. Akard St.
Dallas, TX 75201
Tel.: (214) 213-5004
Email: tom@tsleatherbury.com

Peter Steffensen
State Bar No. 24106464
SMU DEDMAN SCHOOL OF LAW FIRST AMENDMENT CLINIC
3315 Daniel Avenue (75205)
P.O. Box 750116
Dallas, Texas 75275-0116
Tel.: (214) 768-4077
Email: psteffensen@mail.smu.edu

Jennifer Jones*
Katherine Fallow*
Kiran Wattamwar*
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
Email: jennifer.jones@knightcolumbia.org

**Pro Hac Vice*

Attorneys for Plaintiff

TABLE OF CONTENTS

TABLE OF CONTENTS i

TABLE OF AUTHORITIES ii

INTRODUCTION 1

RESPONSE 2

I. The District's broad interpretation of Section 552.139 in this litigation improperly advances a new theory of withholding not raised before the Attorney General. 2

II. Consistent with the Attorney General's review, the Court should interpret Sections 552.139(a) and (b) together. 4

III. To the extent the Court interprets the phrase "relates to . . . the design, operation, or defense of a computer network" in Section 552.139(a) in isolation, the court should consider legislative intent because the phrase is ambiguous 6

CONCLUSION AND PRAYER FOR RELIEF 8

TABLE OF AUTHORITIES

Cases

Arlington Indep. Sch. Dist. v. Tex. Att'y Gen.,
37 S.W.3d 152 (Tex. App.—Austin 2001, no pet.) 7

City of Dallas v. Paxton,
721 S.W.3d 60 (Tex. App.—15th Dist. 2025, no pet.) 2, 4

City of Fort Worth v. Cornyn,
86 S.W.3d 320 (Tex. App.—Austin 2002, no pet.) 7, 8

City of Garland v. Dall. Morning News,
22 S.W.3d 351 (Tex. 2000) 8

Colorado County v. Staff,
510 S.W.3d 435 (Tex. 2017) 7

Greater Hou. P'ship v. Paxton,
468 S.W.3d 51 (Tex. 2015) 8

King v. Paxton,
576 S.W.3d 881 (Tex. App.—Austin 2019, pet. denied) 2, 4, 7

Molinet v. Kimbrell,
356 S.W.3d 407 (Tex. 2011) 7

Paxton v. Escamilla,
590 S.W.3d 617 (Tex. App.—Austin 2019, pet. denied) 7

Tex. Comm'n on Envtl. Quality v. Sierra Club,
712 S.W.3d 630 (Tex. App.—Austin 2022, pet. granted), order withdrawn (June 21, 2024) 2

Uvalde Consol. Indep. Sch. Dist. v. Tex. Trib.,
720 S.W.3d 466 (Tex. App.—San Antonio 2025, no pet.) 5

Statutes

Tex. Gov't Code § 552.139 5

Tex. Gov't Code § 552.301 2

Tex. Gov't Code § 552.326 2

Other Authorities

AppsEDU, *Lightspeed 'Filter' and 'Alert' Demo*, YouTube (Feb. 8, 2024), https://www.youtube.com/watch?v=RsHMEBJmOxc 6

Gaggle.net, *Student Safety Net: How to Build One*, YouTube (Feb. 21, 2023), https://www.youtube.com/watch?v=suR9yyECEoI&t=708s 6

Gaggle.net, *What's New at Gaggle*, YouTube (Aug. 19, 2025), https://youtu.be/BU1yBjWmrIQ?t=1374 6

TO THE HONORABLE JUDGE OF SAID COURT:

COMES NOW, Plaintiff Knight First Amendment Institute at Columbia University (the "Knight Institute" or "Institute"), and files this response to Defendant Grapevine-Colleyville Independent School District's (the "District") response to Plaintiff's Motion for Summary Judgment, and respectfully offers the following for consideration by the court:

INTRODUCTION

The Knight Institute brought this request under the Texas Public Information Act ("TPIA") to determine the scope of the District's use of surveillance systems to monitor student activity on school-issued digital devices. As demonstrated in the Institute's motion for summary judgment, the District fails to meet its burden of establishing that the information sought here—the keywords and websites that the District monitors or blocks—are exempt from disclosure under the TPIA, because it has not shown that the requested information would facilitate unauthorized access to the District's computer network.

In response, the District argues that it should be able to withhold any information that "relates to" its computer network, urging the court to adopt its "plain meaning" interpretation of the computer network security exception that would shield from disclosure *any* information related to computer network activity. *Defendant's Response to Plaintiff's Motion for Summary Judgment* at 7–8 [hereinafter *Def.'s Resp. Mot.*]. This interpretation would not only violate the TPIA's strong public policy favoring disclosure, but is based on a new theory of withholding that was not raised before the Attorney General, and therefore not properly before this Court. The court should reject the District's last-ditch effort to expand the scope of the computer network security exception to justify its improper withholding of information.

Further, as the Institute has already explained in its summary judgment motion and opposition to the District's summary judgment motion, the Attorney General's finding that there

was a compelling reason to withhold the 824 emails was incorrect; the Institute does not challenge the District's FERPA-based redactions; the Institute is entitled to a fee waiver for the costs of the District's processing of its TPIA request; and the Institute is entitled to attorneys' fees if this court determines that any information was improperly withheld by the District. The Institute incorporates those arguments here. Accordingly, this Court should deny Defendant's motion for summary judgment in all respects and grant Plaintiff's cross-motion for summary judgment.

RESPONSE

I. The District's broad interpretation of Section 552.139 in this litigation improperly advances a new theory of withholding not raised before the Attorney General.

The District's broad interpretation of Section 552.139 in this litigation improperly advances a new theory of withholding that was not raised before or considered by the Attorney General. The TPIA mandates that government bodies must "state the *specific exceptions* that apply" when requesting an Attorney General decision. Tex. Gov't Code § 552.301(b) (emphasis added). Moreover, courts have made clear that advancing a new theory of withholding during TPIA litigation is improper. *City of Dallas v. Paxton*, 721 S.W.3d 60, 75–76 (Tex. App.—15th Dist. 2025, no pet.) (a government body cannot assert a new basis for withholding in a public information suit that it did not raise and argue before the Attorney General in its initial request); *see also Tex. Comm'n on Envtl. Quality v. Sierra Club*, 712 S.W.3d 630, 643 n.3 (Tex. App.—Austin 2022, pet. granted), order withdrawn (June 21, 2024) (TPIA suits are "limited to review of the attorney general's decision" based solely on what the "'governmental body properly raised before the attorney general in connection with its request for a decision.'") (quoting Tex. Gov't Code § 552.326). This is true even where the government body raises an exception *under a different subsection of the same statute* for the first time during litigation. *King v. Paxton*, 576 S.W.3d 881, 890 (Tex. App.—Austin 2019, pet. denied) (courts generally cannot consider

alternative theory of withholding based on other subsections for the first time during judicial review, even when the government body relies on the same statutory exception). But that is precisely what the District attempts to do here. In all three of its submissions to the Attorney General requesting an opinion pursuant to Texas Government Code Section 552.301(e), the District explained its position that the requested information was exempt under Section 552.139 because "certain words and website addresses which the District has chosen to block or filter have been chosen because of their propensity to expose the District's computers and network to malicious sites and other risks." *Plaintiff's Motion for Summary Judgment*, Ex. B at 2 [hereinafter *Pl.'s Mot.*]. "In other words," the District specified, "the requested information is 'information directly arising from the [District's] routine efforts to prevent . . . a computer security incident.' Tex. Gov't Code § 552.139(b)(4)." *Id.* The District's submissions left no doubt that it was specifically relying on Section 552.139(b)(4) in its assertion that Section 552.139 applies to the requested information, and that it believed the Institute's request implicated information that, if disclosed, would expose its computer systems, networks, and data to threats from cyberattacks and unauthorized access.

Now, the District has changed course, claiming that Section 552.139(a)'s use of the disjunctive term "or" in the phrase "relates to . . . the design, operation, or defense of a computer network" means that the exception can be employed without reference to computer network security. *Def.'s Resp. Mot.* at 9, 11. In other words, the District has amended its theory to posit that even information that relates only to the design or operation of a computer network is exempt from disclosure, irrespective of whether its release would expose the District to security threats. But whether the requested information merely relates to the *design or operation* of a computer network is not the basis for withholding that the Attorney General reviewed. In its opinions, the

Attorney General specified that the District's argument that the release of the requested information "may expose the [d]istrict to unnecessary security threats" informed its conclusion that the information relates to computer network security, and the design, operation, or defense of the district's computer network within the meaning of Section 552.139. *See Pl.'s Mot.*, Ex. F at 2. The District cannot now rely on the Attorney General's opinions to advance the new theory that information detailing the design or operation of a government's computer network—even if its release wouldn't raise security concerns—is exempt. *City of Dallas*, 721 S.W.3d at 75–76; *King*, 576 S.W.3d at 890. Accordingly, because the District fails to meet its burden of showing that Section 552.139(b)(4) applies to the requested information, it necessarily fails to show that Section 552.139 applies to the Institute's request.

II. Consistent with the Attorney General's review, the Court should interpret Sections 552.139(a) and (b) together.

In determining whether the information requested by the Institute is excepted from disclosure under the TPIA, the Court should interpret the relevant parts of the exception in conjunction with each other. Interpreting Sections 552.139(a) and (b) together, rather than in isolation, is appropriate here both because Section 552.139(b) clarifies the scope of Section 552.139(a), and because the Attorney General's interpretation of Section 552.139(b) provided the basis for its decisions. Thus, while the District is correct that courts must "take statutes as they find them," and "must give effect to every word and phrase if it reasonable to do so because we presume the Legislature used every word or phrase intentionally, with a meaning and a purpose," this canon of construction is fatal to the District's own arguments because it then completely ignores Section 552.139(b). *Def.'s Resp. Mot.* at 5, citing *Holmes v. Morales*, 924 S.W.2d 920, 925 (Tex. 1996) (quoting *Simmons v. Arnim*, 220 S.W. 66, 70 (Tex. 1920)); *Lippincott v. Whisenhunt*, 462 S.W.3d

507, 509 (Tex. 2015); *N.P. v. Methodist Hosp*., 190 S.W.3d 217, 223 (Tex. App.—Houston [1st Dist.] 2006, pet. denied).

Section 552.139(a) provides that information is excepted from disclosure if it "relates to computer network security, to restricted information under Section 2059.055, or to the design, operation, or defense of a computer network." Section 552.139(b) goes on to clarify certain types of information that are made confidential under Section 552.139(a):

> (b) The following information is confidential:
>
> (1) a computer network vulnerability report;
>
> (2) any other assessment of the extent to which data processing operations, a computer, a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is vulnerable to unauthorized access or harm, including an assessment of the extent to which the governmental body's or contractor's electronically stored information containing sensitive or critical information is vulnerable to alteration, damage, erasure, or inappropriate use;
>
> (3) a photocopy or other copy of an identification badge issued to an official or employee of a governmental body; and
>
> (4) information directly arising from a governmental body's routine efforts to prevent, detect, investigate, or mitigate a computer security incident, including information contained in or derived from an information security log.

Tex. Gov't Code § 552.139. In other words, Section 552.139(a) supplies a starting point to understand the meaning of the computer network security exception, while Section 552.139(b) precisely defines the categories of confidential information contemplated by Section 552.139(a). *Uvalde Consol. Indep. Sch. Dist. v. Tex. Trib.*, 720 S.W.3d 466, 481–82 (Tex. App.—San Antonio 2025, no pet.) (finding that language added by amendment to TPIA exception clarified the scope of the exception's broad language).

As discussed above, the District explicitly endorsed this reading of the statute in its requests for Attorney General opinions, explaining its position that the requested information is exempt under Section 552.139 generally because it is "information directly arising from the [District's]

routine efforts to prevent . . . a computer security incident" under Section 552.139(b)(4) specifically. *Pl.'s Mot.*, Ex. B, *supra* at 3.The Attorney General subsequently relied on this reading in its determination that the requested information "relates to computer network security, and the design, operation, or defense of the district's computer network." *Pl.'s Mot.*, Ex. F, *supra* at 4. Although the Attorney General erred in finding that the requested information is in fact exempt under Section 552.139, its review of the information under Sections 552.139(a) and 552.139(b)(4)—taken together—was consistent with the rules of statutory interpretation requiring that every word and phrase, including clarifying language, must be given their intended effect. Because the information requested is not exempt under Section 552.139(b)(4) or any other subsection of 552.139(b), it is not information that "relates to computer network security . . . or to the design, operation, or defense of a computer network" within the meaning of Section 552.139(a).[1]

III. To the extent the Court interprets the phrase "relates to . . . the design, operation, or defense of a computer network" in Section 552.139(a) in isolation, the court should consider legislative intent because the phrase is ambiguous.

Should the Court elect to interpret the phrase "relates to . . . the design, operation, or defense of a computer network" in Section 552.139(a) without reference to 552.139(b)—and for the reasons explained above, it should not—the Court should consider the Legislature's intent because the phrase is ambiguous. Although ordinarily "the plain meaning of the text is the best expression

[1] To the extent the District maintains that the requested information is related to computer network security within the meaning of (b)(4) as it initially claimed, the Institute responds that the District's vendors—Gaggle.net and Lightspeed Systems—clearly bifurcate their security functions from other content filtering functions in their products. *See* Gaggle.net, *What's New at Gaggle*, YouTube, at 22:54 (Aug. 19, 2025), https://youtu.be/BU1yBjWmrIQ?t=1374; *See* Gaggle.net, *Student Safety Net: How to Build One*, YouTube, at 11:48 (Feb. 21, 2023), https://www.youtube.com/watch?v=suR9yyECEoI&t=708s (separating "adult" and "high risk" filters from other custom filters); *See* AppsEDU, *Lightspeed 'Filter' and 'Alert' Demo*, YouTube, at 14:49 (Feb. 8, 2024), https://www.youtube.com/watch?v=RsHMEBJmOxc (a product demo of Lightspeed Filter co-hosted by Colin McCabe, the General Manager of Lightspeed's International Market). The Institute's request seeks information related to the systems' content filtering functions, and to the extent there is overlap with the products' security functions, that may provide a basis for redactions as determined by in camera review—not categorical withholding of records.

of legislative intent," that is not the case when "a different meaning is apparent from the context or the plain meaning leads to absurd or nonsensical results." *Paxton v. Escamilla*, 590 S.W.3d 617, 621 (Tex. App.—Austin 2019, pet. denied) (quoting *Molinet v. Kimbrell*, 356 S.W.3d 407, 411 (Tex. 2011)). When the statutory text is "susceptible to more than one reasonable interpretation," courts may look to other extrinsic aides for assistance to determine the legislative intent. *Id.* (citing *Colorado County v. Staff*, 510 S.W.3d 435, 444 (Tex. 2017)). Here, it is appropriate for the court to look to legislative intent because the phrase is susceptible to more than one reasonable interpretation, and applying its plain meaning devoid of context would lead to absurd or nonsensical results.

Despite the District's claims that Texas courts consistently interpret the phrase "relates to" very broadly, courts have actually reached varying conclusions on the phrase's meaning and scope, narrowing it as appropriate to favor disclosure under the TPIA. *City of Fort Worth v. Cornyn*, 86 S.W.3d 320, 327 (Tex. App.—Austin 2002, no pet.) (adopting a narrow definition of "relates to" in interpreting the law enforcement exception); *Arlington Indep. Sch. Dist. v. Tex. Att'y Gen.*, 37 S.W.3d 152, 158 (Tex. App.—Austin 2001, no pet.) (applying similar reasoning to Section 552.111, which incorporates the deliberative process privilege); *King v. Paxton*, 576 S.W.3d 881, 890–92 (Tex. App.—Austin 2019, pet. denied) (rejecting argument that information about welfare checks relates to law enforcement because their distribution by officers is "totally divorced" from their law enforcement functions).

A narrower interpretation of "relates to" than the one proffered by the District is appropriate in this case, because the District's interpretation would lead to nonsensical results. Under the District's view, anything transmitted over Texas government computer networks—whether that is text, audio, video, images, or software files—would be shielded from public scrutiny. Moreover,

even information that "relates to" the design or operation of the District's computer network and has already been publicly disclosed would be exempt, including the District's acceptable technology use policy or the names of the vendors it uses to monitor students' online activities. But this information is already public, as it should be. To avoid the risk of the computer network security exception "swallow[ing] the rule," the court should interpret it narrowly. *Cornyn*, 86 S.W.3d at 327 (citing *City of Garland v. Dall. Morning News*, 22 S.W.3d 351, 364 (Tex. 2000)) (rejecting broad reading of "relates to" that would result in "none of a police department records . . . be[ing] subject to disclosure"); *Greater Hou. P'ship v. Paxton*, 468 S.W.3d 51, 60 (Tex. 2015) (rejecting a broad reading of the word "supported" in the TPIA as "untenable" because it "risks sweeping any private entity that received any public funds within the definition of a 'governmental body'").

As explained in the Institute's summary judgment motion, the legislative history of Section 552.139 demonstrates that the exception was intended to protect sensitive information that would expose government computer networks to unauthorized access and malicious attacks. *See Pl.'s Mot.* at 19. Because the Institute only seeks information related to categories of student expression the District blocks or monitors on its networks, it is not the type of information the Legislature sought to exempt and must be disclosed.

CONCLUSION AND PRAYER FOR RELIEF

Plaintiff Knight Institute prays that the Court deny Defendant's motion for summary judgment in all respects and grant Plaintiff's cross-motion for summary judgment.

March 9, 2026

Respectfully submitted,

/s/ *Thomas S. Leatherbury*
Thomas S. Leatherbury
State Bar No. 12095275

THOMAS S. LEATHERBURY LAW, PLLC
1901 N. Akard St.
Dallas, TX 75201
Tel.: (214) 213-5004
Email: tom@tsleatherbury.com

/s/ *Peter Steffensen*
Peter Steffensen
State Bar No. 24106464
SMU DEDMAN SCHOOL OF LAW
FIRST AMENDMENT CLINIC
3315 Daniel Avenue (75205)
P.O. Box 750116
Dallas, Texas 75275-0116
Tel.: (214) 768-4077
Email: psteffensen@mail.smu.edu

/s/ *Jennifer Jones*
Jennifer Jones*
Katherine Fallow*
Kiran Wattamwar*
KNIGHT FIRST AMENDMENT INSTITUTE
AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
Email: jennifer.jones@knightcolumbia.org

**Pro Hac Vice*

Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I, Peter Steffensen, Attorney for the Knight First Amendment Institute at Columbia University, hereby certify that a true and correct copy of this document was served via the Court's electronic filing system on all parties of record in this proceeding on this 9th day of March 2026.

/s/ *Peter Steffensen*
Peter Steffensen