FILED
TARRANT COUNTY
2/27/2026 6:37 PM
THOMAS A. WILDER
DISTRICT CLERK

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 OPPOSITION TO DEFENDANT'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 iii

SUMMARY OF DEFENDANT'S MOTION 1

RESPONSIVE ARGUMENT AND RECORD FACTS 1

I. The District has failed to carry its burden of demonstrating that the information sought by the Knight Institute should be withheld from public disclosure under TPIA Section 552.139. 2

A. The Court should not defer to the Attorney General's application of TPIA's computer network security exception because it ignores the legislative intent behind the exception and because its broad reading of the exception contravenes the purposes behind the TPIA. 2

B. The District's argument that information need only "relate to" "the design, operation, or defense of a computer network" to be exempt from disclosure is contrary to the legislative intent behind the computer network security exception, and undermines the strong presumption of disclosure under the TPIA. 4

C. Disclosing the information sought by the Institute will not threaten network security. 6

II. The District's obligations under the federal Children's Internet Protection Act do not relate to computer network security and do not justify withholding the requested information under Section 552.139. 7

III. The District has failed to demonstrate a compelling reason to excuse its failure to timely seek a letter ruling for the 824 emails responsive to the Institute's clarified request. 9

IV. Although the Institute does not challenge the District's redaction of personally identifiable information protected by the Family Educational Rights and Privacy Act, that does not justify wholesale withholding of responsive documents. 10

V. The Knight Institute is entitled to a fee waiver, and this Court has the authority to reduce or waive the fees charged by a government body. 11

VI. The Knight Institute is entitled to attorneys' fees. 12

CONCLUSION AND PRAYER FOR RELIEF 13

TABLE OF AUTHORITIES

Cases

Abbott v. Tex. State Bd. of Pharmacy,
391 S.W.3d 253 (Tex. App.—Austin 2012, no pet.) 3

Amedisys, Inc. v. Kingwood Home Health Care, LLC,
437 S.W.3d 507 (Tex. 2014)..... 1

Arlington Indep. Sch. Dist. v. Tex. Att'y Gen.,
37 S.W.3d 152 (Tex. App.—Austin 2001, no pet.) 5

Austin Bulldog v. Leffingwell,
490 S.W.3d 240 (Tex. App.—Austin 2016, no pet.) 3

Austin Chron. Corp. v. City of Austin,
No. 03–08–00596–CV, 2009 WL 483232 (Tex. App.—Austin Feb. 24, 2009, no pet.) 12

City of Dallas v. Abbott,
304 S.W.3d 380 (Tex. 2010)..... 2, 3

City of Fort Worth v. Cornyn,
86 S.W.3d 320 (Tex. App.—Austin 2002, no pet.) 5, 6, 7

City of Garland v. Dall. Morning News,
22 S.W.3d 351 (Tex. 2000)..... 5

City of San Antonio v. San Antonio Express-News,
47 S.W.3d 556 (Tex. App.—San Antonio 2000, pet. denied)..... 6

Dep't of Air Force v. Rose,
425 U.S. 352 (1976)..... 5

Hancock v. State Bd. of Ins.,
797 S.W.2d 379 (Tex. App.—Austin 1990, no writ), *rev'd on other grounds*, 711 S.W.3d 655 (Tex. 2024)..... 10

Harris Cnty. Appraisal Dist. v. Integrity Title Co., LLC,
483 S.W.3d 62 (Tex. App.—Houston [1st Dist.] 2015, pet. denied)..... 2

King v. Paxton,
576 S.W.3d 881 (Tex. App.—Austin 2019, pet. denied) 6

Kirwan v. The Diamondback,
352 Md. 74 (1998) 11

Paxton v. City of Dallas,
509 S.W.3d 247 (Tex. 2017)..... 10

Tex. Comptroller of Pub. Accounts v. Att'y Gen. of Tex.,
354 S.W.3d 336 (Tex. 2010)..... 12

United States v. Am. Libr. Ass'n, Inc.,
539 U.S. 194 (2003)..... 9

Univ. of Tex. at Austin v. Gatehouse Media Tex. Holdings, II, Inc.,

656 S.W.3d 791 (Tex. App.—El Paso 2022) 10

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

Statutes

5 U.S.C. § 552 12

20 U.S.C. § 1232g 10

47 U.S.C. § 254 ..... 7, 8, 9

Minn. Stat. § 13.37.1 9

Minn. Stat. § 13.37.2 9

Tex. Gov't Code § 552.001 ..... 4, 5

Tex. Gov't Code § 552.139 ..... 2, 4

Tex. Gov't Code § 552.323 12

Tex. Gov't Code § 620.006 7

Other Authorities

146 CONG. REC. S5836 (daily ed. June 27, 2000) (statement of Sen. McCain),
https://perma.cc/X59V-6QMN 9

CIPA Compliance and Content Filtering, Lightspeed Systems (last visited Feb. 11, 2026),
https://perma.cc/PCL6-RSEA 8

Covered Applications and Prohibited Technologies, Texas Department of Information Resources (last visited Feb. 5, 2026), https://perma.cc/SLX6-4HQX 7

Grapevine Colleyville Independent School District, *Director of Network Operations,* Glassdoor (Mar. 8, 2022), https://perma.cc/DVR5-C3HR 4

Mark Keierleber, *Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning — and Now Won't Leave,* The 74 (Sep. 14, 2021), https://perma.cc/9HK3-LWYC 9

Mark Keierleber, *Minneapolis School District Addresses Parent Outrage Over New Digital Surveillance Tool as Students Learn Remotely*, The 74 (Oct. 28, 2020),
https://perma.cc/D53H-ZYLY 9

Rules

Tex. R. Civ. P. 166a 1

Regulations

34 C.F.R. § 99.31 10

TO THE HONORABLE JUDGE OF SAID COURT:

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

SUMMARY OF DEFENDANT'S MOTION

The District moves for summary judgment on the Institute's Mandamus Petition on the following grounds: (1) the Attorney General's opinions in this case, which found that the information the Institute requested is exempt from disclosure under Texas Government Code Section 552.139, are entitled to great weight; (2) the requested information is exempt from disclosure under Section 552.139(a) because it "relates to" the "design and/or operation" of the District's computer network; (3) the District's obligations under the Children's Internet Protection Act ("CIPA"), 47 U.S.C. § 254 (2001), foreclose disclosure of the requested information; (4) the Institute lacks standing to challenge the withholding of information under the Family Educational Rights and Privacy Act of 1974 ("FERPA"), 20 U.S.C. § 1232g(a)(2) (1974); and (5) the court is not authorized to review the District's denial of the Institute's fee waiver.

RESPONSIVE ARGUMENT AND RECORD FACTS

The court should deny the District's motion for summary judgment because the District has not met its "burden of establishing each element of the claim or defense on which it seeks summary judgment." Tex. R. Civ. P. 166a(c); *Amedisys, Inc. v. Kingwood Home Health Care, LLC*, 437 S.W.3d 507, 511 (Tex. 2014). Contrary to the District's arguments, the Attorney General's decisions in this case are not entitled to deference; the information requested does not "relate[] to computer network security . . . or to the design, operation, or defense of a computer network" of the District's computer network within the meaning of the Texas Public Information

Act ("TPIA"), Tex. Gov't Code § 552.139(a); CIPA does not require the District to withhold the information requested; there is no compelling reason that excuses the District's failure to timely seek an Attorney General opinion for a subset of the requested information; the Institute does not challenge the District's FERPA determinations; and the court can exercise its discretion to assess the District's denial of the Institute's fee waiver.

I. The District has failed to carry its burden of demonstrating that the information sought by the Knight Institute should be withheld from public disclosure under TPIA Section 552.139.

As the Knight Institute's cross-motion for summary judgment demonstrates, the exception from disclosure found in Section 552.139 does not apply here, as it covers only information that would expose the District's computer network to threats from cyberattacks or unauthorized access, and the information sought by the Institute poses no such threat. None of the District's arguments in support of its cross-motion refute that conclusion.

A. The Court should not defer to the Attorney General's application of TPIA's computer network security exception because it ignores the legislative intent behind the exception and because its broad reading of the exception contravenes the purposes behind the TPIA.

The Attorney General's interpretation of the computer network security exception is not entitled to deference because it contradicts the exception's purpose of protecting only information that, if disclosed, would threaten the security of a government body's computer network. Courts have repeatedly emphasized that the Attorney General's interpretation of the TPIA "*may* be persuasive, [but] *it is not controlling*." *City of Dallas v. Abbott*, 304 S.W.3d 380, 384 (Tex. 2010) (emphasis added); *see also Harris Cnty. Appraisal Dist. v. Integrity Title Co., LLC*, 483 S.W.3d 62, 66 (Tex. App.—Houston [1st Dist.] 2015, pet. denied). Judicial deference to the Attorney General's TPIA decisions is particularly improper where the agency's interpretation contradicts the meaning of the statute or is otherwise inconsistent with the meaning of the Act. *See Austin*

Bulldog v. Leffingwell, 490 S.W.3d 240, 249–50 (Tex. App.—Austin 2016, no pet.) (refusing to defer to the Attorney General's interpretation of TPIA exception because it contradicted "the exception's plain language"); *Abbott v. Tex. State Bd. of Pharmacy*, 391 S.W.3d 253, 259 (Tex. App.—Austin 2012, no pet.) (declining to follow Attorney General construction of TPIA because it was not supported by the plain text of the statute); *see also City of Dallas*, 304 S.W.3d at 384 (rejecting the Attorney General's interpretation of TPIA provision because it was "inconsistent with other provisions of the Act").

Here, the Attorney General's interpretation of the computer network security exception is not entitled to "great weight," *see Defendant's Motion for Summary Judgment*, 12 [hereinafter *Def.'s Mot.*], or indeed any deference because it contradicts both the plain meaning and legislative purpose of the exception, and because it is inconsistent with the overriding purpose of the TPIA. As the Institute explained in its summary judgment motion and reiterates below, the plain and technical meaning of Section 552.139 's operative language makes clear that the exception applies only to information that could facilitate unauthorized access to the District's computer network, an interpretation that is corroborated by the statute's legislative history and the context of its enactment. *Plaintiff's Motion for Summary Judgment*, 18–21 [hereinafter *Pl.'s Mot*.]. None of the Attorney General opinions in this case consider the plain and technical meaning of Section 552.139's terms or address the legislative intent behind the exception. Nor do the opinions explain the basis for the Attorney General's conclusion that the requested information would expose the District's computer systems to cyberattacks or unauthorized access—aside from noting without analysis the District's conclusory claim that its release would pose "security threats." *See Pl.'s Mot.* at 6 (describing Letter Ruling No. OR2023-20568). The Attorney General's broad interpretation permitting withholding of the requested information would also conflict directly

with other provisions of the TPIA that strongly favor disclosure of information related to the work of government. *See* Tex. Gov't Code § 552.001(a)–(b). Deference to the Attorney General's opinions is therefore not warranted.

B. The District's argument that information need only "relate to" "the design, operation, or defense of a computer network" to be exempt from disclosure is contrary to the legislative intent behind the computer network security exception, and undermines the strong presumption of disclosure under the TPIA.

The District's motion rests on an interpretation of the computer network security exception that is so broad that it would exempt from disclosure anything deemed to be "related" to a government entity's computer network—in contravention of the legislative intent behind the exemption and the policy underlying the TPIA. According to the District, information that bears any connection to the District's network—including the data that travels over the network—"relates to" the computer network security and is therefore categorically exempt from disclosure. *See Def*.'s *Mot.* at 13 (citing Berger Declaration ¶ 5) (suggesting that any information routed over the network is "part of GCISD's computer network"); § 552.139(a). This seems to mean that *any* information on the Internet—so long as it can be routed over the District's network—would fall within the scope of Section 552.139. Under this reasoning, any policy the District creates that relates to the online lives of students could be shielded from public scrutiny under the guise of network security.[1]

Texas law rejects this premise. First, the District's reading of the exception to encompass anything that is "related" to a computer network ignores the plain and technical meaning of, and

[1] Consider, for instance, that the District's job posting for a Director of Network Operations lists several technologies and responsibilities a qualified director should be familiar with. *See* Grapevine Colleyville Independent School District, *Director of Network Operations,* Glassdoor (Mar. 8, 2022), https://perma.cc/DVR5-C3HR. If this information is "confidential" because it "relates to network security" then under the District's theory, it must be shielded from disclosure, which would be an absurd outcome.

the legislative intent behind, the computer network security exception. The language, structure, and legislative history of the exception demonstrate that the Legislature intended to shield from public disclosure only information that would expose a government entity's computer systems, networks, and data to cyberattacks and unauthorized access. *See Pl.'s Mot.* at 19. Second, the District's overbroad reading of the computer network security exception is incompatible with the Legislature's explicit command that the TPIA "shall be liberally construed in favor of granting a request for information," Tex. Gov't Code § 552.001(b), with its exceptions being "narrowly construed." *Uvalde Consol. Indep. Sch. Dist. v. Tex. Trib.*, 720 S.W.3d 466, 477 (Tex. App.—San Antonio 2025, no pet.) (citing *Dep't of Air Force v. Rose*, 425 U.S. 352, 360–61 (1976)); *see* Tex. Gov't Code § 552.001(b).

In analogous cases involving other statutory exceptions to the TPIA, Texas courts have rejected the type of expansive definition of "relates to" advanced by the District here. In *City of Fort Worth v. Cornyn*, 86 S.W.3d 320, 327 (Tex. App.—Austin 2002, no pet.), for example, the court rejected a police department's argument that information about an applicant's fitness for being a police officer "related to" law enforcement under the law enforcement exception found in Section 552.108. As that court explained:

> If, instead of limiting the scope of the law enforcement exception as we do, we accepted the City's argument that any activity engaged in by a police department is exempt from disclosure under section 552.108, we would allow the exception to swallow the rule. Because everything a police department does arguably involves law enforcement, were we to adopt the City's interpretation, none of a police department records would be subject to disclosure.

Cornyn, 86 S.W.3d at 327 (citing *City of Garland v. Dall. Morning News*, 22 S.W.3d 351, 364 (Tex. 2000)); *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). The court in *Cornyn* went on to explain that "the more reasoned

approach, and the one we adopt" is to limit the exception to only "that type of information which, if released, would permit private citizens to anticipate weaknesses in a police department, avoid detection, jeopardize officer safety, and generally undermine police efforts to effectuate the laws of this State." *Cornyn*, 86 S.W.3d at 327.

Likewise, here, Section 552.139 "evidences an intent by the Legislature" to exempt only those documents that would expose government computer networks to hacking and other forms of cyberattacks. *Cornyn*, 86 S.W.3d at 327. And even broadly worded exceptions demand proof that disclosure would implicate the protected interest, not merely that the information concerns the same general topic. *See id.* at 326 (concluding that a background check of an applicant for a police role did not "relate[] to law enforcement" because to recognize so "would be ignoring the special purpose behind the [] exception"); *see also King v. Paxton*, 576 S.W.3d 881, 890–92 (Tex. App.—Austin 2019, pet. denied) (finding that because "[w]elfare checks are considered to be within an officer's 'community caretaking functions,'" which are "totally divorced" from enforcing the law, they did not "relate[] to" law enforcement); *City of San Antonio v. San Antonio Express-News*, 47 S.W.3d 556, 563 (Tex. App.—San Antonio 2000, pet. denied) (finding that use of force reports do not "reasonably relate[] to a police officer's employment relationship" merely because they are listed in an officer's employee file, and are subject to disclosure). Accordingly, the District is required to demonstrate how disclosure would expose an actual network security vulnerability. It has not done so.

C. Disclosing the information sought by the Institute will not threaten network security.

Put plainly, Section 552.139 allows government entities to withhold information that would reveal technical weaknesses in computer systems—such as passwords, API keys and secrets, maps of the network's critical infrastructure, and assessments of its architectural

vulnerabilities. *See Pl.'s Mot.*, Exhibit T, at 6. But it does not shield information about general policies governing user behavior or administrative monitoring. *Cf. Cornyn*, 86 S.W.3d at 327 (agencies may withhold tactical details that would compromise their operations but not general policies or practices).

The records at issue—race and gender-related keyword lists and categories the District monitors and blocks—describe categories of student expression. Disclosing these keywords will not prevent the District from continuing to monitor and block these terms. At most, the keywords would inform students and parents about what categories of speech trigger review under District policy.[2]

II. The District's obligations under the federal Children's Internet Protection Act do not relate to computer network security and do not justify withholding the requested information under Section 552.139.

Citing its expert's report, the District asserts that it is justified in withholding the information sought by the Institute based on the District's obligations under the Children's Internet Protection Act, 47 U.S.C. § 254. *See Def.'s Mot.* at 13–14. The District's argument mixes apples with oranges. Unlike Section 552.139 of the TPIA, CIPA is not intended to prevent hacking or unauthorized access to a computer network. Instead, it requires schools to block students from seeing sexually explicit images. CIPA does not justify shielding the requested records from disclosure.

[2] Texas Government Code Chapter 620, which prohibits certain social media applications and services from being accessed on government devices, demonstrates this principle. The Texas Department of Information Resources publicly lists and updates an extensive set of applications and hardware vendors that Texas prohibits from state-managed networks. *Covered Applications and Prohibited Technologies*, Texas Department of Information Resources (last visited Feb. 5, 2026), https://perma.cc/SLX6-4HQX. The District must block these services from being accessed on its network. Listing these prohibited websites publicly does not threaten the State's or the District's network security, even though these applications have been identified to "pose[] a threat to the State's sensitive information." *Id.* In fact, the public posting of this list of blocked applications is statutorily *required*. *See* Tex. Gov't Code § 620.006(b)(2).

In exchange for federal subsidies for internet access, CIPA requires schools to use technological protection measures to block students from accessing visual depictions of obscenity, child pornography, and materials deemed "harmful to minors," which are defined as sexually explicit depictions that are lawful for adults but not for minors (in other words, pornography). *See* 47 U.S.C. § 254 (h)(5)(B), (h)(7)(G), (l)(1). CIPA also requires that participating schools maintain Internet safety policies that provide for "educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response." 47 U.S.C. § 254 (h)(5)(B)(iii). Finally, school policies must address and enforce the issues of "access by minors to inappropriate matter on the Internet," "the safety and security of minors" in "electronic mail" and "chat rooms," hacking and unauthorized access by minors, and the unauthorized disclosure and use of minor's personal information. 47 U.S.C. § 254 (l)(1)(A).

Nothing about the District's obligations under CIPA justifies withholding the information sought by the Institute under the TPIA's computer network security exception or CIPA's own terms. First, disclosing information about keywords requested by the Institute will not enable students to circumvent the District's filtering of the specific type of content that CIPA targets—sexually explicit images. What is blocked now will still remain blocked, even if the District discloses keywords that it uses to flag internet activity that it otherwise disfavors.[3] Second, nothing in CIPA requires a participating school to hide its content filtering criteria from students or the

[3] Notably, companies like Gaggle and Lightspeed, in their own words, purport to further "student safety *beyond CIPA filtering compliance*." *CIPA Compliance and Content Filtering*, Lightspeed Systems (last visited Feb. 11, 2026), https://perma.cc/PCL6-RSEA (emphasis added). The District's use of their services to monitor online activity generally is a concrete example of student safety measures that go beyond—rather than merely comply with—CIPA's requirements.

broader public.[4] Finally, because CIPA is not a cybersecurity statute targeting unauthorized access to a computer network, information about the District's efforts to comply with it should not be construed as the type of information covered by Section 552.139.[5]

III. The District has failed to demonstrate a compelling reason to excuse its failure to timely seek a letter ruling for the 824 emails responsive to the Institute's clarified request.

The 824 emails responsive to the second part of the Institute's Clarified Request II remain presumptively public because the District has not provided a compelling reason excusing its failure to seek an Attorney General ruling. The District concedes that its nearly two-year delay in requesting an Attorney General opinion requires it to show a "compelling reason" to overcome the presumption of disclosure triggered by its untimeliness, but it does not even attempt to make that showing. *Def.'s Mot.* at 16. Instead, the District merely reiterates its claim that Section 552.139 alone provides a compelling reason to overcome the presumption. It does not. The computer network security exception on its own has never been held to constitute a compelling reason to withhold records to which a presumption of disclosure has attached. Nor does the exception protect the kind of "significant" or "special" interests which would justify a *per se* rule. *See Paxton v. City*

[4] Indeed, other school districts bound by CIPA have previously disclosed records similar to those sought here. For example, similar records about Gaggle incidents were disclosed by the Minneapolis School District, despite the fact that the district was subject to CIPA and despite Minnesota statutes designating "security information" as nonpublic. Minn. Stat. §§ 13.37.1(a), 13.37.2(a); Mark Keierleber, *Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning — and Now Won't Leave,* The 74 (Sep. 14, 2021), https://perma.cc/9HK3-LWYC (referencing 1300 incidents collected by Gaggle that the outlet accessed via public records requests); Mark Keierleber, *Minneapolis School District Addresses Parent Outrage Over New Digital Surveillance Tool as Students Learn Remotely*, The 74 (Oct. 28, 2020), https://perma.cc/D53H-ZYLY (confirming the school district that disclosed the records were bound by CIPA).

[5] CIPA is not a cybersecurity policy. Its stated purpose is to "protect America's children from exposure to obscene material," not to protect school networks. 146 CONG. REC. S5836 (daily ed. June 27, 2000) (statement of Sen. McCain), https://perma.cc/X59V-6QMN; s*ee also United States v. Am. Libr. Ass'n, Inc.*, 539 U.S. 194, 198–99 (2003) ("To address the problems associated with the availability of Internet pornography in public libraries, Congress enacted the Children's Internet Protection Act."). CIPA only references "hacking" and network security in a provision that requires schools to educate students about "unlawful activities by minors online." 47 U.S.C. § 254 (l)(1)(A)(iii).

of Dallas, 509 S.W.3d 247, 259–62 (Tex. 2017) (protection of attorney-client privilege provides "compelling" reason to withhold records).

The TPIA requires more than what the District has offered. Once the presumption of openness due to a governmental entity's failure to timely request an Attorney General opinion attaches, the entity must make a "'compelling demonstration' above and beyond" producing evidence that the information falls within an exception's protections. *Univ. of Tex. at Austin v. Gatehouse Media Tex. Holdings, II, Inc*., 656 S.W.3d 791, 801 (Tex. App.—El Paso 2022) (citing *Hancock v. State Bd. of Ins*., 797 S.W.2d 379, 381 (Tex. App.—Austin 1990, no writ), *rev'd on other grounds*, 711 S.W.3d 655 (Tex. 2024). In other words, even if the Court finds that the information falls within the computer network security exception, the District must provide additional, compelling reasons that justify withholding this specific subset of responsive information. Because it has not, the 824 emails must be disclosed.

IV. Although the Institute does not challenge the District's redaction of personally identifiable information protected by the Family Educational Rights and Privacy Act, that does not justify wholesale withholding of responsive documents.

The Institute is not seeking personally identifiable information within the meaning of the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(a)(2) (1974) ("FERPA"). FERPA protects personally identifiable information within "education records" that are directly connected to students and which are "maintained by" the school from disclosure. 20 U.S.C. §§ 1232g(a)(4)(A), (b)(1). "[E]ducation records" can include "appropriate information . . . concerning disciplinary action taken against [the] student for conduct that posed a significant risk to the safety or well-being of that student, other students, or other members of the school community." *Id*. § 1232g(h)(1).

Under FERPA, records may be released if all personally identifiable information has been removed and the student's identity is not reasonably identifiable. 34 C.F.R. § 99.31(b)(1). The

District can therefore redact student names, student ID numbers or identifying device information from records of students' browsing activity produced by the District's use of Gaggle and Lightspeed Systems. But the District cannot justify withholding all records entirely. *See, e.g., Kirwan v. The Diamondback*, 352 Md. 74, 91 (1998) ("The legislative history of [FERPA] indicates that the statute was not intended to preclude the release of any record simply because the record contained the name of a student. . . . [I]n addition to protecting the privacy of students, Congress intended to prevent educational institutions from operating in secrecy. Prohibiting disclosure of any document containing a student's name would allow [schools] to operate in secret, which would be contrary to one of the policies behind the [] Act."). Removing student names, emails, and device identifiers would be sufficient to keep these records reasonably anonymized. But FERPA does not justify the District's wholesale refusal to disclose the requested records.

V. The Knight Institute is entitled to a fee waiver, and this Court has the authority to reduce or waive the fees charged by a government body.

As the Institute explained in its summary judgment motion, it is entitled to a fee waiver for the cost of processing information responsive to its request under TPIA Section 552.267(a), which allows fees to be waived or reduced if disclosure would primarily benefit the general public. The Institute has shown that disclosure of the information sought here would primarily benefit the public interest and would not further the Knight Institute's commercial interest, and therefore the District wrongfully denied the Institute's fee waiver request. *Pl.'s Mot.* at 27.

Although the TPIA permits a governmental entity to grant a waiver or reduction of fees at its discretion, the discretion of the government body does not prohibit a court from exercising its own discretion to reduce or waive the fees charged to a requestor. Because the TPIA is modeled after the Freedom of Information Act, federal precedent is persuasive on the question of how Texas courts should approach requests for fee waivers. *Tex. Comptroller of Pub. Accounts v. Att'y Gen.*

of Tex., 354 S.W.3d 336, 342 (Tex. 2010) (noting that precedent in FOIA litigation is particularly persuasive where the statutory provisions mirror one another). Like the TPIA, FOIA permits fee waivers for requestors if disclosure of responsive records is likely to contribute significantly to public understanding of the operations or activities of the government. 5 U.S.C. § 552(a)(4)(A)(iii). Here, too, the Court should exercise its discretion to review the District's denial of the Institute's fee waiver and order the District to reimburse the Institute for the cost of processing its request.

VI. The Knight Institute is entitled to attorneys' fees.

Under Section 552.323, "the court shall assess costs of litigation and reasonable attorney fees incurred by a plaintiff who substantially prevails" unless the governmental body acted in reasonable reliance on a prior judgment applicable to the governmental body, a pre-existing appellate opinion, or an Attorney General opinion. Tex. Gov't Code § 552.323(a). But a government body should not be entitled to rely on an Attorney General opinion that contradicts the plain meaning and legislative purpose of a statutory exception, or is otherwise inconsistent with the meaning of the Act. Such reliance is particularly improper where, as here, the Attorney General did not consider legal authority supporting the requestor's position, and there is uncertainty regarding the scope of representative records it reviewed. *Austin Chron. Corp. v. City of Austin*, No. 03–08–00596–CV, 2009 WL 483232, at *7 (Tex. App.—Austin Feb. 24, 2009, no pet.) (mem. op.) (explaining that Attorney General's review of facts and legal authority provided by *both* the requestor and government body supported "reasonable reliance"). At minimum, the Institute is entitled to attorneys' fees if the Court's in camera review establishes that information responsive to its request—yet clearly not exempt under the Attorney General's interpretation of Section 552.139—was improperly withheld by the District.

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.

February 27, 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 27th day of February 2026.

/s/ *Peter Steffensen*
Peter Steffensen

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Peter Steffensen on behalf of Peter Steffensen
Bar No. 24106464
psteffensen@smu.edu
Envelope ID: 111839535
Filing Code Description: Answer/Response
Filing Description: Plaintiff's Opposition to Defendant's Motion for Summary Judgment
Status as of 3/2/2026 8:34 AM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Lucas ChristopherHenry		lhenry@abernathy-law.com	2/27/2026 6:37:20 PM	SENT
Charles J.Crawford		ccrawford@abernathy-law.com	2/27/2026 6:37:20 PM	SENT
Kimberly Escamilla		kescamilla@abernathy-law.com	2/27/2026 6:37:20 PM	SENT
Laura Ball		lball@abernathy-law.com	2/27/2026 6:37:20 PM	SENT
Peter Steffensen		psteffensen@smu.edu	2/27/2026 6:37:20 PM	SENT
Jennifer Jones		jennifer.jones@knightcolumbia.org	2/27/2026 6:37:20 PM	SENT
Katie Fallow		katie.fallow@knightcolumbia.org	2/27/2026 6:37:20 PM	SENT
Thomas Leatherbury		tom@tsleatherburylaw.com	2/27/2026 6:37:20 PM	SENT
Kiran Wattamwar		Kiran.Wattamwar@knightcolumbia.org	2/27/2026 6:37:20 PM	SENT