FILED
TARRANT COUNTY
1/30/2026 6:50 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 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

INTRODUCTION 1

SUMMARY JUDGMENT EVIDENCE 2

FACTS AND PROCEDURAL HISTORY 3

I. Factual background 3

II. The Knight Institute's request under the Texas Public Information Act 5

A. The Original Request 5

B. The Attorney General's Letter Ruling on parts (a) and (b) of the Original Request 6

C. Clarified requests and second Attorney General Letter Ruling 6

D. The District's untimely request for a third Attorney General ruling 9

E. The Institute's petition 10

SUMMARY JUDGMENT GROUNDS 11

SUMMARY JUDGMENT STANDARD 11

ARGUMENT 12

I. Texas's strong public policy favoring disclosure of government information compels the disclosure of the requested information, which is of significant public interest. 13

II. TPIA section 552.139's exception to disclosure does not apply because the information sought by the Institute would not compromise "computer network security." 15

A. The District carries the burden of overcoming the TPIA's presumption of disclosure. 16

B. The language, history, and context of section 552.139 demonstrate that the exception is intended to apply to information that would expose a government entity's computer systems, networks, and data to threats from cyberattacks and unauthorized access. 17

C. The information sought by the Institute would not expose the District's computer networks to cyberattacks or unauthorized access. 21

D. The 824 emails identified by the District as responsive to the second part of the Institute's Clarified Request II must be disclosed because the District has not provided a "compelling reason" to excuse its failure to timely seek a letter ruling for these materials. 25

III. The Institute is entitled to a fee waiver. 27

CONCLUSION AND PRAYER FOR RELIEF..... 27

TABLE OF AUTHORITIES

Cases

A & T Consultants, Inc. v. Sharp,
904 S.W.2d 668 (Tex. 1995) 12

Abu v. Dickson,
107 F.4th 508 (6th Cir. 2024) 22

Amedisys, Inc. v. Kingwood Home Health Care, LLC,
437 S.W.3d 507 (Tex. 2014) 11

Arlington Indep. Sch. Dist. v. Tex. Att'y Gen.,
37 S.W.3d 152 (Tex. App.—Austin 2001, no pet.) 16

Austin Bulldog v. Leffingwell,
490 S.W.3d 240 (Tex. App.—Austin 2016, no pet.) 17, 21

City of Dallas v. Paxton,
721 S.W.3d 60 (Tex. App.—15th Dist. 2025, no pet.) 17

City of Garland v. Dall. Morning News,
22 S.W.3d 351 (Tex. 2000) 12, 13, 16

City of Rockwall v. Hughes,
246 S.W.3d 621 (Tex. 2008) 17

City of San Antonio v. Tex. Att'y Gen.,
851 S.W.2d 946 (Tex. App.—Austin 1993, writ denied) 14

Dall. Area Rapid Transit v. Dall. Morning News,
4 S.W.3d 469 (Tex. App.—Dallas 1999, no pet.) 26

Doe v. Tarrant Cnty. Dist. Att'y's Off.,
269 S.W.3d 147 (Tex. App.—Fort Worth 2008, no pet.) 26

Paxton v. City of Dallas,
509 S.W.3d 247 (Tex. 2017). 26

Simmons v. Kuzmich,
166 S.W.3d 342 (Tex. App.—Fort Worth 2005, no pet.) 26

State v. Shumake,
199 S.W.3d 279 (Tex. 2006) 17

Tex. Comm'n on Env't Quality v. Sierra Club,
712 S.W.3d 630 (Tex. App.—Austin 2022, pet. granted), order withdrawn (June 21, 2024)... 26

Tex. Dep't of Transp. v. City of Sunset Valley,
146 S.W.3d 637 (Tex. 2004) 17

TGS–NOPEC Geophysical Co. v. Combs,
340 S.W.3d 432 (Tex.2011) 17, 21

Thomas v. Cornyn,
71 S.W.3d 473 (Tex. App.—Austin 2002, no pet.) 16

UnitedHealthcare Ins. Co. v. Paxton,
691 S.W.3d 209 (Tex. App.—Austin 2024, no pet.) 14

Uvalde Consol. Indep. Sch. Dist. v. Tex. Trib.,
720 S.W.3d 466 (Tex. App.—San Antonio 2025, no pet.) 24

Van Buren v. United States,
593 U.S. 374 (2021) 22

Statutes

18 U.S.C. § 1030 ..... 19, 20

Acts 2017, 85th Leg., R.S., Ch. 555 (S.B. 532), Sec. 1, eff. Sept. 1, 2017 20

Tex. Gov't Code § 552.001 ..... 13, 14, 16

Tex. Gov't Code § 552.139 ..... passim

Tex. Gov't Code § 552.301(b) 8

Tex. Gov't Code. § 552.0222 14

Other Authorities

CDT Report, *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI*, Ctr. for Democracy & Tech. (Sept. 2023), https://perma.cc/3QNP-6EVR. 4, 14

Dave Maass, Daly Barnett & Jason Kelley, *GoGuardian: A Red Flag Machine By Design*, Electronic Frontier Foundation (last visited Mar. 7, 2025), https://perma.cc/Q966-5LU8. . 4, 24

Digital Learning, Grapevine-Colleyville Independent School District (accessed January 28, 2026), https://perma.cc/2TLS-8ESR 24

Ellen Barry, *Spying on Student Devices, Schools Aim to Intercept Self-Harm Before It Happens*, N.Y. Times (Dec. 11, 2024), https://perma.cc/ZDD7-GTSL. 3, 14

Jackie Benton, *Public Data Systems, Infrastructure under Attack*, Comptroller (March 2019), https://perma.cc/5DY7-8UA9. 20

Lightspeed Relay Parent Portal (accessed Jan. 30, 2026), https://perma.cc/E79T-H9VP 24

Mark Keierleber, *Gaggle Surveils Millions of Kids in the Name of Safety. Targeted Families Argue it's 'Not That Smart'*, The 74 (Oct. 12, 2021), https://perma.cc/Q94H-T6TG. 4, 14

NICCS, *Glossar*y, https://perma.cc/8DAM-XJVR. 18

S.B. 532 Bill Analysis, Senate Research Center (June 5, 2017), https://perma.cc/GVN9-Y59T. . 20

Rules

Tex. R. Civ. P. 166a 11

Regulations

1 Tex. Admin. Code § 70.11 23

47 CFR § 54.520 25

TO THE HONORABLE JUDGE OF SAID COURT:

COMES NOW, Plaintiff Knight First Amendment Institute at Columbia University ("Knight Institute" or "Institute"), and files this Motion for Summary Judgment pursuant to Texas Government Code section 552.321 against Defendant Grapevine-Colleyville Independent School District ("GCISD" or "District"), and in support thereof respectfully shows the Court the following:

INTRODUCTION

This case involves access to information about how the District uses surveillance software to monitor its students' speech and internet use. Like the District, schools nationwide are increasingly turning to automated surveillance tools to screen and filter what students communicate and access while online. These surveillance systems, developed by a handful of private technology companies, monitor students' private chats and emails, internet searches, and files in search of keywords, phrases, or website addresses that school administrators deem objectionable.

How school districts use this software, including whether they use it not just to achieve their stated safety concerns, but also to impermissibly surveil students' private speech and viewpoints, is of great public interest. Accordingly, the Knight Institute, a nonprofit organization dedicated to protecting and strengthening free speech in the digital age, filed requests under the Texas Public Information Act (TPIA), seeking information about the District's use of school surveillance software to monitor student activity on school-issued laptops and tablets.

Under the public policy favoring disclosure of information under the TPIA, the Institute is entitled to the information it requested from the District because of the public interest in knowing whether the District is using school surveillance software to monitor the speech and online searches of its students. 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. Moreover, a subset of the information sought by the Institute is presumptively public because the District failed to request an Attorney General ruling within the required time period. Finally, the Institute is entitled to a fee waiver, because disclosure of the information it requested would primarily benefit the general public.

SUMMARY JUDGMENT EVIDENCE

The Institute presents evidence contained in the following agreed-upon exhibit list in support of this Motion:

- Exhibit A: Original Request from Knight Institute to GCISD under the TPIA (March 29, 2023)
- Exhibit B: 15-day request from GCISD to Attorney General (April 20, 2023)
- Exhibit C: Clarified Request I from Knight Institute to GCISD with narrowed scope (June 2, 2023)
- Exhibit D: Search terms provided by Knight Institute to GCISD to assist with Clarified Request I (June 2, 2023)
- Exhibit E: Email from Knight Institute to GCISD memorializing Clarified Request II terms (June 14, 2023)
- Exhibit F: Attorney General Informal Letter Ruling on Original Request, parts (a) and (b) (June 16, 2023)
- Exhibit G: Email from GCISD to Knight Institute on search volume, fee waiver denial, and estimated charges for search (June 21, 2023)
- Exhibit H: Letter from GCISD to Attorney General requesting ruling on part of Clarified Request II (June 28, 2023)
- Exhibit I: Email from Knight Institute to GCISD regarding fee waiver request (June 30, 2023)
- Exhibit J: Attorney General Letter Ruling No. OR2023-30020 regarding part of Clarified Request II (August 31, 2023)

- Exhibit K: Email from GCISD to Knight Institute confirming receipt of the Institute's payment and download of 824 responsive emails (October 23, 2023)
- Exhibit L: Letter from Knight Institute to GCISD requesting processing and disclosure of the 824 responsive emails (November 7, 2023)
- Exhibit M: Email from GCISD to Knight Institute regarding redactions and claiming exceptions (November 14, 2023)
- Exhibit N: Email from Knight Institute objecting to GCISD's claim to withholdings, noting untimely Attorney General request (November 16, 2023)
- Exhibit O: Correspondence from GCISD sharing redacted responsive emails (November 17, 2023)
- Exhibit P: Letter from GCISD to Attorney General seeking retroactive authorization to withhold information from emails (April 17, 2025)
- Exhibit Q: Response Letter from Knight Institute regarding Attorney General request (May 27, 2025)
- Exhibit R: Attorney General Letter Ruling No. OR2025-022099 regarding April 17 request (June 26, 2025)
- Exhibit S: Declaration of Jennifer Jones (January 30, 2026)
- Exhibit T: Expert Report of Bruce Schneier (January 30, 2026)
- Exhibit U: Expert Report of Kyle Berger (November 19, 2025)

FACTS AND PROCEDURAL HISTORY

I. Factual background

Schools in Texas and across the country are using A.I.-powered software to monitor student activity on school-issued devices and networks. Created by companies including GoGuardian, Gaggle, and Lightspeed Systems, these systems use artificial intelligence to scan student files, emails, searches, chats, and network activity to detect a list of flagged categories of content, keywords, or phrases, while their filtering technology blocks access to certain websites. Ellen Barry, *Spying on Student Devices, Schools Aim to Intercept Self-Harm Before It Happens*, N.Y. Times (Dec. 11, 2024), https://perma.cc/ZDD7-GTSL. When the software detects that a student

has typed or viewed a word or phrase that is on the list of flagged terms, it sends an alert to school administrators. Depending on the type of alert, the school may initiate disciplinary action against the student and notify parents or law enforcement. *Id*. When a school district contracts to use this surveillance software, the vendors typically implement their monitoring using their own standardized lists of flagged keywords, phrases, and prohibited websites. However, school districts can also, at their discretion, customize the list of flagged keywords, phrases, and blocked websites. Mark Keierleber, *Gaggle Surveils Millions of Kids in the Name of Safety. Targeted Families Argue it's 'Not That Smart'*, The 74 (Oct. 12, 2021), https://perma.cc/Q94H-T6TG.

The ostensible purpose of school surveillance software is to protect students at risk of causing physical harm to themselves or others, and to prevent students from accessing sexually explicit material while using school-provided devices. But there is nothing in the technology itself that limits the surveillance to such content, and public reporting suggests that school districts have used it to track and even restrict students' constitutionally protected—but apparently disfavored—speech. A recent report found that the technology routinely flags benign content as harmful, stifling student learning and impeding access to information necessary to complete school assignments. CDT Report, *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI*, Ctr. for Democracy & Tech. (Sept. 2023), https://perma.cc/3QNP-6EVR. Students have been flagged for reading the text of Genesis on Bible.com and blocked from classic literature like *Romeo and Juliet*. Dave Maass, Daly Barnett & Jason Kelley, *GoGuardian: A Red Flag Machine By Design*, Electronic Frontier Foundation (last visited Mar. 7, 2025), https://perma.cc/Q966-5LU8. One service, GoGuardian, blocked a Texas student from visiting the online Texas Driver Handbook, because the website uses the term "cocaine" in warning about the risk of driving while using the drug. *Id*. The same service blocked the website of the Texas House of Representatives, because of

references to "cannabis" in legislation regulating medical marijuana, and because of the use of the term "sexual" in legislation relating to sexual assault. *Id*.

The risk that school districts will abuse or misuse surveillance and filtering software is exacerbated by the fact that schools generally keep their lists of flagged content hidden from public scrutiny. This secrecy has emboldened some schools to block, filter, or monitor content deemed to be controversial, including constitutionally protected content related to sexuality, gender, and race. *Id.*

II. The Knight Institute's request under the Texas Public Information Act

A. The Original Request

The Knight Institute is a not-for-profit organization that defends the freedoms of speech and the press in the digital age through strategic litigation, research, policy advocacy, and public education. Promoting the public's right to access information is a core part of the Institute's mission. The Institute regularly relies on public records laws and the First Amendment to obtain information about government activity and disseminates that information to the press and public.

As part of its ongoing work on free speech and surveillance, the Knight Institute is exploring whether school districts are using surveillance software in a manner that undermines or infringes their students' rights to privacy, speech, and association. To that end, on March 29, 2023, the Institute submitted a request under the TPIA, section 552.003(6) for information related to the District's use of surveillance systems to monitor students' activity on school-issued devices and software, including:

> (a) Any information identifying the words or phrases the District has included, or plans to include, in its list(s) of blocked or monitored words;
> (b) Any information identifying the websites the District has included, or plans to include, in its list(s) of blocked or filtered websites;
> (c) Any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications

> between District employees, and communications between the District and the company supplying the District's digital surveillance system.

Exhibit A [hereinafter "Original Request"].

B. The Attorney General's Letter Ruling on parts (a) and (b) of the Original Request

With respect to parts (a) and (b) of the Original Request, the District asked that the Texas Attorney General provide an opinion ruling that responsive information was excepted from disclosure under section 552.139 of the TPIA. *See* Tex. Gov't Code § 552.139; **Exhibit B** [hereinafter "April 20 15-day AG Request"]. Under this provision, 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." Tex. Gov't Code § 552.139(a).

On June 16, 2023, the Attorney General issued a Letter Ruling No. OR2023-20568. *See* **Exhibit F** [hereinafter "AG Letter Ruling I"]. The opinion found that all but two of the requested records[1] were exempt from disclosure under section 552.139. The opinion did not explain the basis for concluding that the information fell under the exception, aside from noting the District's claim that it would pose "security threats." *Id.* The opinion noted that the ruling was "limited to the particular information at issue in this request" and "must not be relied upon as a previous determination regarding any other information or any other circumstances." *Id*.

C. Clarified requests and second Attorney General Letter Ruling

With respect to part (c) of the Original Request, the District asked the Institute to clarify the scope of the information sought and to provide search terms to aid in the retrieval of responsive materials. On June 2, 2023, the Institute provided a list of search terms for the District to use to

[1] The Attorney General determined that two letters, from representatives at Gaggle and Lightspeed Systems, who both asserted that their keyword lists were proprietary, must still be disclosed.

search employee email correspondence since January 1, 2020. **Exhibit C** [hereinafter "Clarified Request I"]. The Institute also narrowed the scope of the entire Original Request, inclusive of parts (a)–(c), to information related to the monitoring and filtering of LGBTQ+ and race-related content, and asked the District to confirm the name(s) of the vendors it had contracted with for its online filtering and monitoring. **Exhibit D** [hereinafter "Search Terms"].

In response to the Institute's Clarified Request I, the District disclosed that it uses Lightspeed Systems and Gaggle to monitor students' digital activities. The District also conducted a search for materials responsive to part (c) of the Original Request using the search terms provided by the Institute. Counsel for both parties then met to discuss how to narrow part (c) even further in light of the high volume of responsive documents. The parties agreed to narrow the request by (1) prioritizing the production of analytics concerning types of content that the monitoring software has flagged; and (2) searching only email correspondence originating from Lightspeed and Gaggle domains or containing their names. *See* **Exhibit E** [hereinafter "Clarified Request II"].

On June 21, 2023, the District's counsel informed the Institute that its search of email correspondence related to Lightspeed and Gaggle yielded 824 emails that were potentially responsive to part (2) of Clarified Request II, and indicated its intent to seek a ruling on exceptions for part (1) of Clarified Request II. *See* **Exhibit G** [hereinafter "June 21 District Response"].

On June 28, 2023, the District sought an Attorney General ruling regarding part (1) of Clarified Request II—the portion of the request seeking analytics concerning the type of content that the monitoring software has flagged.[2] *See* **Exhibit H** [hereinafter "June 28 10-Day Request"].

[2] The District's request characterizes the first part of Clarified Request II as only requesting reports from Gaggle and Lightspeed Systems. *See* June 28 AG request. The Knight Institute, however, merely requested that the District *prioritize* this information in its search—not limit its search to these records. The Knight Institute is still entitled to all requested records.

Notably, the District did not at the time seek a ruling with respect to part (2) of Clarified Request II. *See* id., fn. 4.

On August 31, 2023, the Attorney General responded by issuing Letter Ruling No. OR2023-30020. *See* **Exhibit J** [hereinafter "AG Letter Ruling II"]. The ruling held that the requested information from Clarified Request II, part (1) was exempt from disclosure under the computer network security exception. *See* Tex. Gov't Code § 552.139.

On July 13, 2023, the Knight Institute confirmed its intent to move forward with part (2) of Clarified Request II and agreed to pay the estimated fees, conditional on its right to seek judicial review of the denial of its request for a fee waiver.[3] The District confirmed receipt of the Institute's payment on October 23, 2023, and began processing the 824 responsive emails, but claimed that "almost all [of the] emails contain the very information the Texas Attorney General agreed must be withheld." *See* **Exhibit K**.

On November 7, 2023, the Institute sent a letter to the District requesting that it continue to process the responsive emails. *See* **Exhibit L**. In addition, the letter notified the District that a request for an Attorney General opinion regarding the information would be untimely, because it was not initiated within ten business days of the Institute confirming its intent to move forward with the request. *See id*., Tex. Gov't Code § 552.301(b). On November 14, 2023, the District agreed to continue processing the emails but insisted it would still redact them pursuant to "the Attorney General's [previous] ruling that certain information should be withheld as it relates to computer network security, and the design, operation, or defense of the District's computer

[3] GCISD shared its estimated of a $741.60 cost to process the responsive emails with the Knight Institute on June 21, 2023. *See* **Exhibit G.** There, GCISD also denied the Knight Institute's initial request for a fee waiver. *Id.* GCISD indicated it was waiting for the Knight Institute to confirm the estimated charges before proceeding. *Id.* In parallel, the Knight Institute asked GCISD to reconsider its decision to deny its request for a fee waiver on June 30, 2023 given that the requested information would serve the public interest. *Id.* GCISD responded one week later that it would continue to deny the request. *See* **Exhibit I**.

network." **Exhibit M**. The District did not indicate which prior Attorney General ruling it purported to rely on, or why it believed it did not need to seek a new Attorney General opinion.

On November 16, 2023, the Knight Institute objected to the District's reliance on the previous Attorney General opinion(s) to redact the responsive emails. *See* **Exhibit N**. Neither previous ruling applied to part two of the Clarified Request, and neither could be "relied upon as a previous determination." *See* **Exhibit F, Exhibit R**. The District's counsel never responded to this objection.

On November 17, 2023, the District disclosed the 824 responsive emails via its online public records portal, redacting virtually all information relevant to the request, including keywords and phrases that the District monitors.[4] *See* **Exhibit O** [hereinafter "GCISD Responsive Emails"].

D. The District's untimely request for a third Attorney General ruling

On April 17, 2025—twenty-two months after receiving Clarified Request II, and after the Institute filed this lawsuit—the District sought an Attorney General opinion as to the second part of Clarified Request II. *See* **Exhibit P**. Acknowledging that its request was untimely, the District claimed that the computer network security exception provides a "compelling reason" to rebut the presumption of public disclosure triggered by its procedural violation *See id* (citing Tex. Gov't Code § 552.139(b)(4)). The Knight Institute objected to the District's request on the grounds that it was untimely, and asserted that the 824 emails that the District had identified as responsive to part two of Clarified Request II should thus be considered presumptively public under the TPIA. *See* **Exhibit Q**.

[4] In some of the responsive emails disclosed by GCISD, the relevant information was not fully redacted by the District. On information and belief, those emails were disclosed inadvertently. *See, e.g.*, **Exhibit O**, 1, 3.

On June 26, 2025, the Attorney General issued Letter Ruling No. OR2025-022099, determining that the information was exempt under section 552.139, and concluding that the fact that it was exempt provided a compelling reason to overcome the presumption of public disclosure. *See* **Exhibit R** [hereinafter "AG Letter Ruling III"].

E. The Institute's petition

The Knight Institute filed this action on March 12, 2025. The District filed its Answer on April 14, 2025. The parties agreed to exchange expert reports on the meaning of the statutory exception in section 552.139(b)(4). On October 31, 2025, Plaintiff submitted the expert report of Bruce Schneier, one of the nation's leading experts on cybersecurity. *See* **Exhibit T** [hereinafter "Expert Report of Bruce Schneier"]. Schneier testified to the technical meaning of computer network security as understood by the cybersecurity industry, emphasizing that the term generally refers to the protection of computer networks from external unauthorized access. Schneier further testified that the public release of the requested information would not undermine the District's efforts to secure its network from external attacks, because the information sought relates to the monitoring of the expression—e.g., the web searches and viewing histories—of those already authorized to access the network. *Id*.

Defendant submitted its expert report of Kyle Berger, the District's IT specialist, on November 26, 2025. Berger's report claimed that the information sought by the Institute would undermine the District's computer network security by providing students with a roadmap to evade monitoring and bypass website filters, allowing them to engage in cyberbullying, access harmful content, and coordinate violence and self-harm. *See* **Exhibit U** [hereinafter "Expert Report of Kyle Berger"]. Accordingly, he opined, information about keywords, phrases and websites the District monitors necessarily "relates to the design, operation, or defense of a computer network" because improper use by authorized users (*i.e.*, students) is also a question of computer network security.

On September 23, 2025, the Knight Institute filed an amended Mandamus Request to include additional allegations regarding the District's late-filed request for an AG opinion. *See Plaintiff's Amended Mandamus Petition* (September 23, 2025).

SUMMARY JUDGMENT GROUNDS

As a matter of law, the Institute is entitled to summary judgment against the District on the following grounds:

1. The information the Institute requested is public and must be disclosed.
2. The information the Institute requested is not excepted under Tex. Gov't Code section 552.139 or any other exception of the TPIA and must be disclosed.
3. The District failed to timely request an Attorney General Opinion for the information sought by the Institute in part two of Clarified Request II, and because there is no "compelling reason" under section 552.139 to withhold the information responsive to that part of the request, it must be disclosed. *See* Tex. Gov't Code § 552.302.
4. The Institute is entitled to a fee waiver for the cost of processing its request for information because it has demonstrated that the information sought "is in the public interest" and will "primarily benefit[] the general public" under section 552.267(a).

SUMMARY JUDGMENT STANDARD

Under Tex. R. Civ. P. 166a, a court must grant a moving party summary judgment when the movant shows that there is no genuine issue of material fact, and that the movant is entitled to judgment as a matter of law. Tex. R. Civ. P. 166a(c); *Amedisys, Inc. v. Kingwood Home Health Care, LLC*, 437 S.W.3d 507, 511 (Tex. 2014). When a moving party has met its "burden of establishing each element of the claim or defense on which it seeks summary judgment, the burden then shifts to the non-movant to disprove or raise an issue of fact as to at least one of those

elements." *Amedisys*, 437 S.W.3d at 511. In TPIA matters, "[t]he questions for each category of information [the requestor] seeks . . . are questions of law." *A & T Consultants, Inc. v. Sharp*, 904 S.W.2d 668, 674 (Tex. 1995); *see also City of Garland v. Dall. Morning News*, 22 S.W.3d 351, 357 (Tex. 2000) ("[W]hether information is subject to the [TPIA] and whether an exception to disclosure applies to the information are questions of law.").

In this case, no questions of fact exist. The Institute has met its summary judgment burden, and the District cannot disprove or raise a fact issue as to any of the claim's elements. Accordingly, this Court should grant summary judgment in favor of the Institute.

ARGUMENT

Under the TPIA, the Institute is entitled to the information it requested from the District. Therefore, this Court should grant summary judgment in favor of the Institute for three reasons: (1) Texas public policy as reflected in the TPIA compels the disclosure of the requested information, which is of significant public interest; (2) the information the Institute requested is not excepted under section 552.139 of the TPIA ("the computer network security exception") because disclosure of the information would not expose the District's computer network to malicious or unauthorized access; and (3) subsets of the information the Institute requested are presumptively public under sections 552.302 and 552.0222(a), meaning the District cannot simply assert that the computer network security exception applies, but meet the higher burden that a "compelling reason" prevents disclosure. Given these facts, the Court should grant the Institute's Motion for Summary Judgment and require the District to disclose the information sought in the Institute's request.

I. Texas's strong public policy favoring disclosure of government information compels the disclosure of the requested information, which is of significant public interest.

The information requested by the Institute is of significant public interest because it will provide insight into how the District uses school surveillance software to monitor students' speech and internet searches. Importantly, disclosure of the requested information will promote government transparency and accountability.

The TPIA embodies a strong state policy favoring disclosure of information related to the work of government. "[I]t is the policy of this state that each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees." Tex. Gov't Code § 552.001(a). Modeled after the federal Freedom of Information Act, the TPIA emphasizes that access to public information is a fundamental tenet of government accountability and effective self-government. *See id.* ("The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may retain control over the instruments they have created."). Notably, the TPIA's policy favoring public access to information is even stronger than its federal counterpart. *City of Garland*, 22 S.W.3d at 364 ("Unlike the FOIA, [the TPIA] contains a strong statement of public policy favoring public access to governmental information and a statutory mandate to construe the Act to implement that policy and to construe it in favor of granting a request for information."). Accordingly, the provisions of the TPIA "shall be liberally construed" "in favor of granting a request for information." Tex. Gov't Code § 552.001(a)–(b).

Here, the information requested by the Institute fits squarely within the TPIA's mandate favoring disclosure. The Institute's request seeks information about how the District uses surveillance software to monitor all student activity—from private chat and email communications

to internet searches and written assignments—on school-issued laptops and other digital devices. There is strong public interest in understanding how such technology is used, in part to determine whether the purported benefits of the technology are outweighed by well-documented harms caused to students' privacy and expressive interests. *See* Barry, *supra*, at 3; CDT Report, *supra*, at 4; Keierleber, *supra*, at 4. Bringing these surveillance practices to light is precisely what the TPIA was designed to promote, particularly when such information will foster government transparency and accountability. *See* Tex. Gov't Code § 552.001(a); *City of San Antonio v. Tex. Att'y Gen*., 851 S.W.2d 946, 950 (Tex. App.—Austin 1993, writ denied) (noting that "[t]he legitimacy of the public interest is not in doubt" where information would reveal how a public officer performs his duties and promote public accountability). Students, parents, and the broader public not only have a right to know how children are being monitored by school administrators and private surveillance companies, but also to decide what the parameters of such surveillance should be. Given this significant public interest, this Court should require the District to disclose the information sought in the Institute's request.[5]

[5] The information sought by the Institute should be disclosed for the additional reason that it includes "[c]ontracting information" between the District and the software companies that is deemed presumptively public. Tex. Gov't Code. § 552.0222(a). "Contracting information is public and must be released," unless it is "excepted from disclosure" under some other identifiable provision of the Act. *Id.* Relevant here, the Act defines "[c]ontracting information" to include "communications and other information sent between a governmental body and a vendor or contractor related to the performance of a final contract with the governmental body or work performed on behalf of the governmental body." *Id*.; *Id.* § 552.003(1-a)(E).

Because Lightspeed and Gaggle perform their services for the District on an ongoing, contractual basis, the information sought by the Institute constitutes "contracting information" that is subject to the Act's presumptive disclosure rules under that provision. That only underscores the need for the District to rigorously meet their "burden of establishing that the exception applies." *UnitedHealthcare Ins. Co. v. Paxton*, 691 S.W.3d 209, 215 (Tex. App.—Austin 2024, no pet.). It also necessitates a careful review of the responsive records which reveal how the District's contracts with Lightspeed and Gaggle are being performed, so that they are not subjected to an overly capacious reading of the computer network security exception. To the contrary, not only must the Act's terms be narrowly construed, but also "[c]lose judgment calls are to be resolved in favor of the stated purpose of the legislation[,]" *id.*—that is, "in favor of granting a request for information." Tex. Gov't Code. § 552.001(b).

The Institute acknowledges that the District has a legitimate interest in protecting its computer network from attacks, but, as explained below, the information it seeks would not undermine the District's cybersecurity. Instead, it would allow the public to understand which constitutionally protected ideas and viewpoints the District has determined are off-limits for its students. For example, information responsive to the Institute's request could reveal whether the District is scanning students' communications for any mention of terms related to race or gender, or scanning its students' web searches for terms like "Second Amendment" or "The Bible." There is no conceivable way that this information would subvert the security of the District's networks, but it would unquestionably shed light on the surveillance and suppression of constitutionally protected inquiry.

II. TPIA section 552.139's exception to disclosure does not apply because the information sought by the Institute would not compromise "computer network security."

The District claims, and the Attorney General has agreed, that the information requested by the Institute is excepted from disclosure under section 552.139, but that view rests on a fundamental misapprehension of the meaning of that statutory exception. As explained below, the statutory language, history, and context of section 552.139 demonstrates that the exception is intended to shield from public disclosure only that information that would expose a government entity's computer systems, networks, and data to threats from cyberattacks and unauthorized access. It does not, as the District and its expert claim, apply to the kind of keywords and phrases used in surveillance and filtering software because disclosure of those terms will not enable cyberattacks or unauthorized access of that software; disclosure would expose only the kinds of ideas and viewpoints the District deems suspicious and off-limits for its students.

A. The District carries the burden of overcoming the TPIA's presumption of disclosure.

Section 552.139 of the TPIA ("the computer network security exception") provides, in relevant part:

> (a) Information is excepted from [required public disclosure] if it is information that relates to computer network security, to restricted information under Section 2059.055 [of the Government Code], or to the design, operation, or defense of a computer network.
>
> (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;
>
> . . .
>
> (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.

To defeat the Institute's motion for summary judgment and overcome the TPIA's presumption in favor of disclosure, the District must "prove that an exception to disclosure applies." *Thomas v. Cornyn*, 71 S.W.3d 473, 488 (Tex. App.—Austin 2002, no pet.); Tex. Gov't Code § 552.001(a)–(b) (TPIA must "be liberally construed…in favor of granting a request for information"); *City of Garland*, 22 S.W.3d at 364 (emphasizing that courts should ensure that a claimed "exception [does not] swallow the Act"); *Thomas*, 71 S.W.3d at 480–81 ("[e]xceptions to the [TPIA] are [to be] narrowly construed"); *Arlington Indep. Sch. Dist. v. Tex. Att'y Gen.*, 37 S.W.3d 152, 157–58 (Tex. App.—Austin 2001, no pet.) (observing that the Texas Supreme Court has declined to interpret exceptions under the TPIA as broadly as its federal counterpart, FOIA). Thus, while courts balance a government entity's legally recognized interests with the public's

right to the disclosure of public information, that balancing strongly favors disclosure of public information to the requestor. *See City of Dallas v. Paxton*, 721 S.W.3d 60, 64 (Tex. App.—15th Dist. 2025, no pet.); Tex. Gov't Code §§ 552.101–163.

As established below, the District cannot meet its burden of proving that the exception applies to the information requested by the Institute.

B. The language, history, and context of section 552.139 demonstrate that the exception is intended to apply to information that would expose a government entity's computer systems, networks, and data to threats from cyberattacks and unauthorized access.

With no court having interpreted section 552.139 to date, and with no statutory definition of "computer network security," traditional methods of statutory interpretation help to discern the intent of the Legislature in enacting the exception. In construing statutes, courts "ascertain and give effect to the Legislature's intent as expressed by the language of the statute…and [] use definitions prescribed by the Legislature and any technical or particular meaning the words have acquired." *Austin Bulldog v. Leffingwell*, 490 S.W.3d 240, 245 n.24 (Tex. App.—Austin 2016, no pet.); *City of Rockwall v. Hughes*, 246 S.W.3d 621, 625 (Tex. 2008) (Willett, J., dissenting) (internal citations omitted) (citing Tex. Gov't Code § 311.011(a) ("Words and phrases [shall] be read 'in context and construed according to the rules of grammar and common usage.'"); *State v. Shumake*, 199 S.W.3d 279, 284 (Tex. 2006); *Tex. Dep't of Transp. v. City of Sunset Valley*, 146 S.W.3d 637, 642 (Tex. 2004). Where—as here—the Legislature has not prescribed definitions for certain statutory language, courts "construe the statute's words according to their plain and common meaning," and consider the specific context in which a statute was passed. *Austin Bulldog*, 490 S.W.3d at 245 n.24, 246 & n.28 (citing *TGS–NOPEC Geophysical Co. v. Combs*, 340 S.W.3d 432, 441 (Tex.2011) ("Language cannot be interpreted apart from context.")).

Here, the plain and technical meaning of the provision's operative language, and the context of the exception's enactment, make clear that TPIA section 552.139 applies only to information that could facilitate unauthorized access to the District's computer network. It does not apply to, and the interests that motivated its enactment would not be served by applying it to, lists of keywords that would reveal only the kinds of ideas and viewpoints the District is monitoring in its students' internet usage.

To begin, the technical meaning of the phrase "information that relates to computer network security . . . or to the design, operation, or defense of a computer network," TPIA section 552.139(a), means information that that would expose a government entity's computer systems, networks, and data to threats from cyberattacks and unauthorized access. To illustrate why this is the proper definition, the Knight Institute submitted the expert report of Bruce Schneier, an internationally-renowned computer security technologist who has worked in the area of computer network security for decades. As Schneier explained in his report, "computer network security" is often used interchangeably with the term "cybersecurity," which the Merriam Webster Dictionary defines as "measures taken to protect a computer or computer system against unauthorized access or attack." Expert Report of Bruce Schneier at 3–4 (quoting Merriam-Webster, cybersecurity, https://perma.cc/5T36-N5EN). In the cybersecurity industry, the technical meaning of "computer network security" similarly refers to "defenses of computers, servers, and other networked devices against unauthorized access." *Id.* Relatedly, the term "computer security incident" generally refers to incidents in which an unauthorized individual succeeds in gaining access to servers and other networked computers; such unauthorized access is often called a "hack" or a "breach." *Id.*; NICCS, *Glossar*y, https://perma.cc/8DAM-XJVR. Cybersecurity professionals "typically work to keep an organization's internal computer network safe and secure from threats such as cyber-attacks,

viruses, malware, phishing, password attacks, denial of service attacks, ransomware, and other *intrusions by external actors*…by preventing these attacks before they occur, or detecting them as quickly as possible as they are occurring." Expert Report of Bruce Schneier at 4 (emphasis added).

The legislative history of section 552.139 confirms that the Legislature intended the exception to prevent the disclosure of information that could facilitate unauthorized access to government computer networks. The provision was originally enacted in 2001, alongside an amendment to Penal Code chapter 33, which is Texas's 1985 analog to the federal anti-hacking statute, the Computer Fraud and Abuse Act ("CFAA"). *See* 18 U.S.C. § 1030(a)(4). Subsection (a) of TPIA section 552.139 allows for withholding of "information that relates to computer network security . . . or to the design, operation, or defense of a computer network." The meaning of subsection (a) is illuminated by the specific examples provided in subsection (b), which originally provided two types of information that should be considered confidential: (1) network vulnerability reports and (2) "any other assessment" which identified the extent to which government systems would be "vulnerable to unauthorized access or harm" including the "alteration, damage, or erasure" of electronically stored data. Tex. Gov. Code § 552.139 (2004).

Taken together, sections (a) and (b) express the Legislature's intent to shield from disclosure information that would pose a threat to computer network security from malicious actors or unauthorized users. This understanding of the meaning of section 552.139's exception was confirmed by a subsequent amendment to the statute. In 2017, the Legislature amended section 552.139 to also designate as confidential "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(b)(4) (2018). The context surrounding the passage of this amendment is notable. In the

preceding year, government agencies in Texas were the targets of dozens of computer security breaches. Jackie Benton, *Public Data Systems, Infrastructure under Attack*, Comptroller (March 2019), https://perma.cc/5DY7-8UA9. To combat cybercrimes against government agencies, the Legislature passed SB 532 to "promote[] cybersecurity and cost saving within state agencies by requiring an assessment of information technology risks and encouraging agencies to explore cloud computing innovations." Acts 2017, 85th Leg., R.S., Ch. 555 (S.B. 532), Sec. 1, eff. Sept. 1, 2017; *S.B. 532 Bill Analysis*, Senate Research Center (June 5, 2017), https://perma.cc/GVN9-Y59T. The information technology assessment requirement was codified with an amendment to Tex. Gov't Code section 2054.068, which mandates that government agencies monitor their computer networks for security risks and disclose those audits to the State Department of Information Resources. Presumably recognizing that these sensitive audits might be subject to disclosure under the TPIA, SB 532 included an amendment to section 552.139 to designate "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" as confidential. Acts 2017, 85th Leg., R.S., Ch. 555 (S.B. 532), Sec. 1, eff. Sept. 1, 2017; *see* Tex. Gov't Code § 552.139(b)(4).

Finally, the context within which section 552.139 was enacted provides additional support for the understanding that the exception is intended to protect information that, if disclosed, would pose a threat to government entities' computer network security. The exception was originally enacted in 2001 alongside an amendment to Penal Code chapter 33, Texas's corollary to the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(4). Like the CFAA, chapter 33 was passed in the mid-1980s to combat security threats posed by the increasingly widespread use of computers and the advent of the internet. Expert Report of Bruce Schneier at 5. These laws

generally prohibit an individual from intentionally accessing a computer without authorization. *Id*.; 18 U.S.C. § 1030. The language of TPIA section 552.139 "cannot be interpreted apart from context" of other laws that drove its passage, and "as the supreme court has emphasized on numerous occasions, [that] context matters." *Austin Bulldog*, 490 S.W.3d at 246 & n.28 (citing *TGS–NOPEC Geophysical Co.*, 340 S.W.3d at 441). Given this context, this Court should interpret the exception as only permitting the withholding of information that, if disclosed, would expose the District's computer networks to cyberattacks or unauthorized access.

C. The information sought by the Institute would not expose the District's computer networks to cyberattacks or unauthorized access.

The District incorrectly claims that the requested information is excepted from disclosure under section 552.139. The District's arguments and the claims of its expert Kyle Berger ignore the meaning of the section 552.139, and rest on an overly broad reading of the exception that runs contrary to the Act's mandate favoring disclosure and requiring its exceptions to be construed narrowly.

Public disclosure of the information the Institute seeks—such as the keywords and websites that the District monitors or blocks on account of the ideas and viewpoints they contain—would not undermine the District's efforts to prevent unauthorized access to the District's computer networks. At most, the requested information might reveal the categories of content that the District (and Gaggle and Lightspeed) deems objectionable or unsafe for its students to access, share, or communicate. But content that a government body has determined is objectionable or unsafe for students is categorically different from the type of information that section 552.139 excepts from disclosure—sensitive information about computer network security. As the Institute's expert Bruce Schneier explained: "None of the information that [the Institute] has requested, if disclosed to the public, would facilitate the harm or destruction of the District's computers and

digital devices. Nor would disclosure of the information enable phishing and password attacks that can deceive people into giving out their login information, or prevent legitimate users from accessing information systems, devices, and other network resources." Expert Report of Bruce Schneier at 6. By contrast, if the Institute had requested information about the specific network services the District uses, the configurations of the specific security products they use, or assessments of vulnerabilities in the District's computer network, that would potentially implicate the exception. *Id*. But the Institute has not requested any of that information here.

The District's expert makes the unpersuasive claim that releasing information about monitored words and blocked websites would provide a "guaranteed roadmap for circumvention." Expert Report of Kyle Berger at 7. Mr. Berger contends that by having access to information about the specific content the District monitors and filters, students and external malicious actors could bypass filters to engage in cyberbullying, access harmful content, and coordinate violence and self-harm. While the potential for students and hackers to bypass filters is an inherent risk when operating any computer network, the hypothetical consequences of circumvention that Berger points to here relate to improper use and student safety, not computer network security.

The federal caselaw interpreting the CFAA—which is analogous to Texas's laws relating to network security—is probative on this point. As the U.S. Supreme Court and other federal courts have reaffirmed in recent years, the purpose of the CFAA is to prevent unauthorized access to computers or computer networks, and it cannot be used to enforce limitations on how or why an individual uses a computer. *See, e.g*., *Van Buren v. United States*, 593 U.S. 374, 396 (2021) (holding that "exceeds authorized access" is limited to access of information in different areas of a computer without authorization, and does not encompass misusing authorized access for improper purposes); *Abu v. Dickson*, 107 F.4th 508, 514 (6th Cir. 2024) (clarifying that the CFAA prevents two forms

of hacking—access without authorization (i.e., "outside hackers") and access that exceeds authorization (i.e., "inside hackers"), and emphasizing that access does not "exceed authorization" merely because it is motivated by an improper purpose); *see also* Expert Report of Bruce Schneier at 5. Here, too, TPIA section 552.139 was enacted alongside Texas's anti-hacking statute with the specific objective of ensuring that disclosure of information under the Act would not enable unauthorized access to government computer networks. While the District might very well have concerns about the ideas and viewpoints that students use their computers to express or explore, those concerns are not related to computer network security and thus not covered by section 552.139. *See* Expert Report of Bruce Schneier at 6.

Moreover, this argument ignores the fact that some of this information is routinely disclosed, and that the public availability of this information has not resulted in any "catastrophic failure" of the District's ability to protect student safety. [6] As explained in the Institute's Amended Mandamus Petition, the District's staff are notified when certain content is flagged by Gaggle or Lightspeed technology, and these notifications include the specific words or websites that triggered the flag. *See* GCISD Responsive Emails. That information is then shared with parents via the "Lightspeed Parent Portal," which allows parents to view content their children sought that was blocked by Lightspeed. Parents are therefore made aware of the specific content that the District monitors and filters through at least one vendor. *See* Lightspeed Relay Parent Portal (accessed Jan.

[6] The District's expert seeks to collapse this clear distinction by positing that the Lightspeed product it utilizes has both content monitoring and network security functions. Expert Report of Kyle Berger at 4, 10. More specifically, Berger notes that Lightspeed's filtering system protects against malware and online threats by blocking high-risk traffic before such exposure occurs, thereby reducing the likelihood that exploit delivery, phishing, or ransomware reaches students' digital devices. But this argument fails to make a case for categorically withholding information about content monitoring from public disclosure. Assuming it is true that its surveillance software functions as both a content monitoring system and network security system, the court's in camera review can determine whether information about their dual functions can be segregated for purposes of producing responsive information. *See* 1 Tex. Admin. Code § 70.11(d)(3)(G) ("[a]ll governmental bodies responding to information requests have the responsibility to . . . [s]egregate public information from information that may be withheld and provide that public information promptly").

30, 2026), https://perma.cc/E79T-H9VP; *see also Digital Learning*, Grapevine-Colleyville Independent School District (accessed January 28, 2026), https://perma.cc/2TLS-8ESR (The page, maintained by the District, suggests that as a parent, you can "[l]og into your parent portal to view your child's online activity").[7] Notably, Berger's report omits any mention of instances where a school district's disclosure of information about monitored or blocked content led to a "catastrophic failure" to protect student safety, because no such failure has been documented.

The District's expert concludes that the requested information is excepted from disclosure because it "relates to the design, operation, or defense of a computer network," and notes that the phrase "relates to" as contemplated by the TPIA has been interpreted very broadly. Expert Report of Kyle Berger at 8–9 (quoting Tex. Gov't Code § 552.139(a)). Setting aside the fact that Berger is not qualified to opine on conclusions of law, this interpretation is simply incorrect. The information that the Institute seeks—information about the District's monitoring of ideas and viewpoints—does *not* "relate[] to" the District's computer network. It relates, instead, to the District's policy decisions about the speech its students may engage with. Moreover, the District's theory ignores the clarification of the scope of TPIA section 552.139(a) that is written into sections 552.139(b)(1)–(4). Courts' interpretations of other clarifying subsections to TPIA exceptions, including amendments, are instructive for evaluating their effect on the scope of the broader exception. For example, in *Uvalde Consolidated Independent School District v. Texas Tribune*, 720 S.W.3d 466, 481–82 (Tex. App.—San Antonio 2025, no pet.) the court reviewed the effect of a

[7] What's more, many school districts nationwide have disclosed information about the content that their monitoring and filtering systems flag, including schools in the state of Texas. *See, e.g.,* Dave Maass, Daly Barnett and Jason Kelley, *GoGuardian: A Red Flag Machine By Design*, Electronic Frontier Foundation (October 2023), https://perma.cc/G49Y-H6HB (discussing how a Texas student was flagged by a content monitoring system for visiting the online Texas Driver Handbook, which warns about cocaine's impact on concentration, due to the word "cocaine" generating an alert); Caroline Haskins, *Gaggle Knows Everything About Teens And Kids In School*, Buzzfeed News (November 1, 2019), https://perma.cc/JPY2-K26F (noting that Gaggle-produced student incident reports were obtained from 17 school district via public records requests).

1997 amendment on the broad language of the original exception— "information . . . that deals with the detection, investigation, or prosecution of crime" —finding that the additional language clarifying that such information "would interfere with the detection, investigation, or prosecution of crime" limited the scope of the exception's application, and explaining that a government body must show "interference" to justify its withholding of records. Here, too, the District must specifically explain how the information it seeks to withhold falls within section 552.139(b)(1)–(4). Yet the District's expert makes generalized claims that information about the monitoring and filtering of content "relates to the design, operation, or defense of a computer network," without explaining how that information is excepted by section 552.139(b)(1)–(4). Berger's broad interpretation of section 552.139(b) is inconsistent with both the rule of interpretation laid out in *Uvalde*, and the TPIA's general mandate in favor of disclosure.[8]

D. The 824 emails identified by the District as responsive to the second part of the Institute's Clarified Request II must be disclosed because the District has not provided a "compelling reason" to excuse its failure to timely seek a letter ruling for these materials.

Even if the District could establish that some of the information sought by the Institute falls within the "computer network security" exception—and for the reasons explained above, it cannot—the 824 emails that the District has identified as responsive to part (2) of the Institute's Clarified Request II must be disclosed because the District failed to seek a ruling from the Attorney General as to those materials within the required period of time, and now must meet the higher burden of showing that a "compelling reason" warrants withholding of the information under the

[8] Expert Kyle Berger makes an additional argument that the federal Children's Internet Protection Act ("CIPA"), 47 CFR § 54.520, bars disclosure of the requested information because CIPA requires blocking or filtering measures on school computer networks, and disclosure of information about such filtering "would likely result in nullification of CIPA compliance." *See* Expert Report of Kyle Berger at 7. While it is true that CIPA requires that participating schools monitor and block student access to visual depictions of obscene content on school networks, it does not require the full range of features and filtering that GCISD uses Gaggle and Lightspeed to enable, nor does it require withholding of public records detailing the type of content that is filtered. 47 CFR § 54.520(c)(1)(i).

exception. *Doe v. Tarrant Cnty. Dist. Att'y's Off.*, 269 S.W.3d 147, 153 (Tex. App.—Fort Worth 2008, no pet.) ("governmental entity attempting to overcome the presumption cannot simply assert an exception to disclosure; rather, the entity must present evidence of a compelling reason to prevent disclosure under that exception."). Despite the Institute's insistence that the District seek an AG ruling, the District did not do so until nearly two years after receiving the Institute's clarification and after this lawsuit was filed. *Dall. Area Rapid Transit v. Dall. Morning News*, 4 S.W.3d 469 (Tex. App.—Dallas 1999, no pet.) (ruling that the requested information was presumed to be public because the government body's request for an attorney general opinion was untimely); *Simmons v. Kuzmich*, 166 S.W.3d 342 (Tex. App.—Fort Worth 2005, no pet.) (same).

Here, the District concedes that its nearly two-year delay in seeking an Attorney General opinion as to Clarified Request II was untimely, but contends that the computer network security exception serves as a compelling reason to overcome the presumption of public disclosure. *See* AG Letter Ruling III. Not so. As explained above, the exception does not apply to the information requested, and even if it did, that fact in itself does not meet the Legislature's stringent requirement that "a justification for withholding information presumed public be 'compelling.'" *Tex. Comm'n on Env't Quality v. Sierra Club*, 712 S.W.3d 630, 642 (Tex. App.—Austin 2022, pet. granted), order withdrawn (June 21, 2024) (declining to hold that the deliberative process privilege constitutes a compelling reason to withhold information); *Doe*, 269 S.W.3d at 153. As the court emphasized in *Paxton v. City of Dallas*, "[t]he meaning of the term 'compelling' is of vital importance . . . because it represents a qualitative limitation on the justifications that permit withholding information from public disclosure." 509 S.W.3d 247, 258 (Tex. 2017). "Neither *a* reason nor even a *good* reason would be sufficient to rebut the public-disclosure presumption. The reason must be 'compelling.'" *Id*. (emphasis in original). Here, the District has failed to provide a

compelling justification justifying withholding of the requested information. It is therefore presumed to be public information.

III. The Institute is entitled to a fee waiver.

The Institute is entitled to a fee waiver for the cost of processing information responsive to its request. TPIA section 552.267(a) allows fees to be waived or reduced if disclosure would primarily benefit the general public. Disclosure of the information sought here would primarily benefit the public interest, as it would inform the public about actual or alleged government activity. Specifically, the requested information is necessary to the public's understanding of how the District utilizes surveillance software to monitor students' online speech and internet use. Moreover, disclosure would not further the Knight Institute's commercial interest. As discussed above, the Knight First Amendment Institute is a New York not-for-profit corporation based at Columbia University that works to preserve and expand the freedoms of speech and the press through strategic litigation, research, and public education. The Institute will make any information disclosed available to the public at no cost.

The District wrongfully denied the Institute's fee waiver request despite its clear showing that disclosure of the requested information would primarily benefit the public interest. Accordingly, the Court should order the District to reimburse the Institute for its $741.60 payment for the cost of processing its request.

CONCLUSION AND PRAYER FOR RELIEF

The Knight Institute's claim in this case involves no genuine issue of material fact. The claim turns solely on the legal issues discussed above. On each of these legal issues, the Knight Institute is entitled to summary judgment as a matter of law. Accordingly, the Knight Institute respectfully requests that this Court grant summary judgment in favor of the Plaintiff. Specifically, Plaintiff asks the Court to enter judgment against GCISD as follows:

(1) Enter a writ of mandamus requiring GCISD to produce to the Knight Institute the requested information in the Original Request.

(2) Alternatively, enter a writ of mandamus requiring GCISD to produce to the Knight Institute the requested information in Clarified Request I.

(3) Alternatively, enter a writ of mandamus requiring GCISD to produce to the Knight Institute the requested information in Clarified Request II.

(4) Order in camera inspection of information responsive to the Institute's request.

(5) Order that the Knight Institute is entitled to a fee waiver for its Request, and that GCISD reimburse the Knight Institute for its previous payment for public information.

(6) Award costs, attorney's fees, and pre-judgment and post-judgment interest to the extent permitted under the law

(7) Grant all such further relief as the Court deems proper and just.

January 30, 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 30th day of January 2026.

/s/ *Peter Steffensen*
Peter Steffensen

EXHIBIT A

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
info@knightcolumbia.org

March 29, 2023

Grapevine-Colleyville Independent School
District
Public Information Request
3051 Ira E. Woods Avenue
Grapevine, Texas 76051

Re: Texas Public Information Act Request

To whom it may concern,

This letter constitutes a request pursuant to the Texas Public Information Act ("TPIA"), Texas Government Code Ch. 552, for information related to the Grapevine-Colleyville Independent School District's ("District") use of surveillance systems to monitor students' activity on digital devices and accounts. This request is made for public and non-commercial purposes by the Knight First Amendment Institute at Columbia University ("Knight Institute" or "Institute").[1]

I. Background

As students across the country transitioned to remote learning in response to the COVID-19 pandemic, school administrators increasingly turned to surveillance companies to assist with monitoring students' activity on digital devices and school-issued Google and Microsoft accounts.[2] One of the most prevalent tools marketed by these companies is spy tech that uses artificial intelligence to track all student activity and communications on their digital devices and accounts. In practice,

[1] The Knight First Amendment Institute is a New York not-for-profit corporation based at Columbia University that works to preserve and expand the freedoms of speech and the press through strategic litigation, research, and public education.

[2] Mark Keierleber, *The spy tech that followed kids home for remote learning—and won't leave*, Fast Company (Sept. 20, 2021), https://www.fastcompany.com/90677509/the-spy-tech-that-followed-kids-home-for-remote-learning-and-wont-leave.

these systems typically work by restricting students' access to specific websites and/or applications, while scanning student emails, documents, chats, and more against a list of monitored words and phrases.[3] Any content that may indicate a student is engaging in "inappropriate behaviors" or poses "potential threats to self or others," including profanity, references to self-harm, violence, bullying, or drugs, is flagged by the tool and reviewed by human content moderators, who can pass the material to school administrators or law enforcement to take further action.[4] While surveillance companies typically have a standard list of keywords that will generate a flag, school administrators have the ability to customize this list to reflect local contexts.[5]

Surveillance companies claim that these systems protect student safety, but students, parents, and others have raised concerns that they actually cause serious harm, posing significant threats to students' privacy and free speech rights and contributing to a long legacy of policing and surveillance in public schools.[6] To learn more about how these systems are being deployed, this request seeks records related to the list of words, phrases, and websites that the District filters and/or monitors as part of its surveillance of students' digital activities.

II. Information requested

The Knight Institute requests the following information[7] related to the Grapevine-Colleyville Independent School District's use of surveillance systems to monitor student activity on digital devices and accounts, created on or after January 1, 2020:

a. Any information identifying the words or phrases the District has included, or plans to include, in its list(s) of blocked or monitored words;[8]

---

[3] Caroline Haskins, *Gaggle Knows Everything About Teens And Kids In School*, Buzzfeed News (Nov. 1, 2019, 3:48pm), https://perma.cc/7269-VTFS.

[4] *Id.*; Mark Keierleber, *Minneapolis Schools to Halt Controversial Student Surveillance Initiative*, The 74 (June 27, 2022), https://perma.cc/S6TA-6696.

[5] Mark Keierleber, *Gaggle Surveils Millions of Kids in the Name of Safety. Targeted Families Argue it's 'Not That Smart'*, The 74 (Oct. 12, 2021), https://perma.cc/Q94H-T6TG.

[6] Keierleber, *supra* note 4.

[7] For purposes of this request, "information" includes but is not limited to all records or communications preserved in written or electronic form, including but not limited to: correspondence, documents, data, videotapes, audio tapes, emails, faxes, files, guidance, guidelines, evaluations, instructions, analyses, memoranda, agreements, notes, orders, policies, procedures, protocols, reports, rules, training manuals, other manuals, or studies.

[8] For purposes of this request, "list of blocked or monitored words" means any specific word or phrase that may trigger an alert, flag, block, restriction,

b. Any information identifying the websites the District has included, or plans to include, in its list(s) of blocked or filtered websites;[9]

c. Any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications between District employees, and communications between the District and the company supplying the District's digital surveillance system.

III. Request for waiver or limitation of fees

The Knight Institute requests that you produce the information free of charge on the grounds that this request is made for public and non-commercial purposes and will benefit the general public. Tex. Gov't Code § 552.267. However, if you are unable to do so, the Institute will reimburse you for the reasonable costs associated with fulfilling this request if your office has a policy of requiring the payment of a copying charge for such information. **If you anticipate that the total costs associated with fulfilling this request will exceed $35, please contact me with an estimate of the likely cost before proceeding**.

IV. Information about the request

The Texas Public Information Act mandates that if you are unable to produce the requested information within 10 business days of this request, you certify that fact in writing and set a date within a reasonable time when the information will be available.

Should you elect to withhold or delete any information, please justify your decision by referencing specific exemptions under the Act. In doing so, we remind the District that Tex. Gov't Code § 552 establishes a strong presumption in favor of disclosure. *See* Open Records Decision 363 at 1 (1983) (explaining that records must be disclosed "unless they fall within one of the particular exceptions applicable"); Open Records

---

report, or notification by the District's digital monitoring system(s), whether that alert, flag, block, restriction, report, or notification is sent to the affected student, an employee or contractor of the surveillance provider, a District employee, or another individual. "List of blocked or monitored words" explicitly includes any "default" words or phrases suggested by the District's surveillance partner and adopted by the District, as well as any additional words or phrases added or requested by the District.

[9] For purposes of this request, "list of blocked or filtered websites" means any specific website, domain name, or keyword within a website name that is blocked, filtered, or otherwise restricted by the District, as well as any specific website, domain name, or keyword within a website name that may trigger an alert, flag, block, restriction, report, or notification by the District's digital monitoring system(s).

Decision 91 at 2 (1975) ("The Act makes all information public unless excepted."). These exemptions "should be construed narrowly." *Arlington Indep. Sch. Dist. v. Tex. Att'y Gen.*, 37 S.W.3d 152, 157 (Tex. App. 2001). If any exemption that you assert applies to only a portion of the information (as opposed to the entire record), please redact the portion you claim is exempt, provide copies of the remainder of the information, and detail your reasons for the modification.

We also ask that you provide responsive electronic information in its native file format. Alternatively, please provide the information electronically in a text-searchable, static-image format (e.g., PDF), in the best image quality in the District's possession, and in separate, Bates-stamped files.

We request that you produce responsive materials in their entirety, including all attachments, appendices, enclosures, and/or exhibits. To the extent that a response to this request would require you to provide multiple copies of identical material, the request is limited so that only one copy of identical material is requested.

* * *

Thank you for your attention to our request. We would be happy to discuss its terms with you over the phone or via email to clarify any aspect of it.

/s/ Jennifer Jones

Jennifer Jones
Stacy Livingston
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT B

Alexandra M. Williams
(817) 334-7292 (Direct Dial)
(817) 334-7290 (Direct Fax)
amwilliams@jw.com

April 20, 2023

VIA ONLINE SUBMISSION

The Honorable Ken Paxton
Attorney General, State of Texas
Open Records Section
P.O. Box 12548
Austin, Texas 78711-2548

Re: Open Records Request of Jennifer Jones of the Knight First Amendment Institute received on March 30, 2023
Internal Ref: P000953-033023

Dear Attorney General Paxton:

I am counsel to the Board of Trustees for Grapevine-Colleyville Independent School District (the "District"). The District received the public information request attached as Exhibit 1 on March 30, 2023 ("Request"). This firm, on behalf of the District, previously submitted a timely 10-day letter with respect to the Request. A copy of the District's 10-day letter is attached as Exhibit 2. The District now requests an opinion on certain documents attached as Exhibit 3.

This correspondence constitutes the District's submission required under Texas Government Code § 552.301(e). By copy of this letter, the District is informing the requestor of its submission of written comments to the Attorney General under Section 552.301(e). Tex. Gov't Code § 552.301(e-1).

The requestor made the following requests to the District:[1]

> *The Knight Institute requests the following information related to the Grapevine-Colleyville Independent School District's use of surveillance systems to monitor student activity on digital devices and accounts, created on or after January 1, 2020:*
>
> *a. Any information identifying the words or phrases the District has included, or plans to include, in its list(s) of blocked or monitored words;*

[1] *See* Exhibit 1.

b. *Any information identifying the websites the District has included, or plans to include, in its list(s) of blocked or filtered websites; and*
c. *Any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications between District employees, and communications between the District and the company supplying the District's digital surveillance system.*[2]

The Request seeks information the District contends is excepted from disclosure under the Act for reasons discussed with greater specificity, below.

Please find attached in Exhibit 3 the documents that the District contends are not subject to mandatory disclosure. The District believes these documents fall within the following applicable exception:

TEX. GOV'T CODE § 552.139 – Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers

Exhibit 3 contains the responsive information the District maintains is not subject to disclosure. Exhibit 3 shows certain information (*i.e.*, words, website addresses) the District has chosen to block or filter from its network for the purpose of protecting the safety and security of District employees and students, as well as to protect the safety and security of the District's network by preventing computer security incidents.

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. In other words, 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). The public disclosure of such words, website addresses, and other related information may expose the District to unnecessary security threats. As such, the District requests that Attorney General permit the District to withhold all information responsive to the Request (*i.e.*, the entirety of Exhibit 3).[3]

[2] The District sent a request for clarification to the requestor with respect to subsection (c) of the Request on April 5, 2023, inquiring whether the requestor intended for the District to search the e-mail accounts of each and every District employee and requesting whether requestor could identify search terms to be used in such a search. See Tex. Gov't Code § 552.222. The District has not received any response from the requestor. As such, this correspondence pertains only to subsections (a) and (b) of the Request.

[3] *See* Tex. Att'y Gen. Op. No. OR2019-01233 (finding that a school district must withhold information in response to a similar request for "all urls and keywords that are blocked on school and or district WiFi networks" as such information "relates to computer network security, and the design, operation, or defense of the district's computer network").

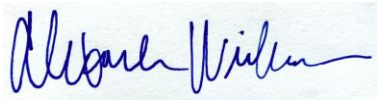
Conclusion

The District believes that the responsive documents contained in Exhibit 3 should be excepted from disclosure under the Act. This This correspondence constitutes the District's request to the Attorney General required under Texas Government Code § 552.301(e). The Attorney General has not made a previous determination regarding the specific information contained in Exhibit 3.

By copy of this letter, the District is informing the requestor of its request to the Attorney General, contained herein, for a decision regarding whether the information is within an exception and of its intent to withhold the requested information until a decision is made by your office pursuant to this request. Tex. Gov't Code § 552.301(e-1).

Should you have any questions, please do not hesitate to contact me.

Sincerely,



Alexandra M. Williams
Attorney

Enclosures as noted

cc: Requestor Jennifer Jones, The Knight First Amendment Institute, w/o enclosures (via email)

Paula Barbaroux, w/o enclosures (via email)

35902656v.1

EXHIBIT C

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
info@knightcolumbia.org

June 2, 2023

Alex Harlow
Grapevine-Colleyville Independent School
District
3051 Ira E. Woods
Grapevine, TX 76051

Re: Public Information Act Request No. P000953-033023

Dear Alex Harlow,

Thank you for your response to the Public Information Act request submitted by the Knight First Amendment Institute at Columbia University ("Institute") on March 29, 2023, Reference No. P000953-033023. We write in response to your email correspondence dated April 5, 2023.

First, you indicated that the Grapevine-Colleyville Independent School District ("District") has determined that some or all of the Institute's request is likely to fit within an exception to disclosure under Texas Government Code Section 552.139 and notified us of your intent to request an opinion of the Texas Attorney General regarding our request.[1] Second, you asked for clarity regarding the information the Institute seeks from the District. Specifically, you asked that the Institute identify search terms for the District to use in its search for responsive information. Finally, you asked whether we intend for the District to search every employee's email correspondence since January 1, 2020, or if there are specific individuals or positions whose email communications we would like you to search.

We address each of these items below.

[1] Since then, the Institute has received copies of the correspondence sent by Counsel to the Board of Trustees for Grapevine-Colleyville Independent School District to the Texas Attorney General on April 13, 2023, and April 20, 2023.

I. Proposed narrowing of the Request

To address the District's stated concerns that disclosing the information responsive to subsections (a) and (b) of our Request may jeopardize the safety and security of District employees and students and may expose the District to cybersecurity threats, we would like to narrow the entire Request, inclusive of subsections (a), (b), and (c), as follows[2]:

First, the Institute asks that the District limit its search to information related to the following:

i. monitoring and/or filtering teacher and student engagement[3] with current or historical events, political and social movements, and/or analysis of race, gender, and sexuality;
ii. compliance with Senate Bill 3[4]
iii. compliance with House Bill 3979,[5] or
iv. compliance with GCISD Board Policy EMB (LOCAL), EFA (LOCAL), EFB (LOCAL), and AIB (LOCAL)[6]

---

[2] Subsection (a) of our Request seeks "Any information identifying the words or phrases the District has included, or plans to include, in its list(s) of blocked or monitored words." Subsection (b) of our Request seeks "Any information identifying the websites the District has included, or plans to include, in its list(s) of blocked or filtered websites."

[3] For purposes of this Request, "engagement" includes but is not limited to classroom discussion, interpersonal communications, research, and writing.

[4] S.B. 3: Relating to civics training programs for certain public school social studies teachers and principals, parental access to certain learning management systems, and certain curriculum in public schools, including certain instructional requirements and prohibitions. S.B. 3, 87th Leg., Reg, Sess. (Tex. 2021), https://perma.cc/RB3Q-SDM4.

[5] H.B. 3979: Relating to civics instruction public school students and instruction policies in public schools. H.B. 3979, 87th Leg., Prior Sess. (Tex. 2021), https://perma.cc/9RH9-98WA.

[6] Grapevine-Colleyville Independent School District, *EMB – Miscellaneous Instructional Policies: Teaching About Controversial Issues*, Board Policy Manual (June 30, 2022), https://perma.cc/8JX7-ZP4W; Grapevine-Colleyville Independent School District, *EFA – Instructional Resources: Instructional Materials*, Board Policy Manual (Aug. 22, 2022), https://perma.cc/D47G-HU2V; Grapevine-Colleyville Independent School District, *EFB – Instructional Resources: Library Materials*, Board Policy Manual (Aug. 22, 2022), https://perma.cc/QN7E-HYFV; Grapevine-Colleyville Independent School District, *AIB – Accountability: Performance Reporting*, Board Policy Manual (Aug. 22, 2022), https://perma.cc/9BY3-9EZR.

Second, the Institute asks that the District exclude or redact any information from its search results that identifies words, phrases, or websites that could potentially identify methods of hacking or damaging the District's wireless or wired networks, databases, or computers. By excluding or redacting this specific information, the District can provide access to the government information requested by the Institute while avoiding public disclosure of information that may expose the District to security threats and/or threaten the safety and security of District employees and students.

II. Search terms and scope of subsection (c)

The Institute has identified search terms to clarify the information we seek related to subsection (c), which asks for "any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications between District employees and communications between the District and the company supplying the District's digital surveillance system." We have attached to this correspondence a spreadsheet identifying search terms. We also would like to clarify that we intend for the District to search every employee's email correspondence since January 1, 2020.

III. Additional information regarding our request

Finally, the District did not provide any information responsive to our request in the email dated April 5, 2023, including the names of the vendors the District contracts with to filter students' internet searches and/or monitor student activity on digital devices and accounts. We ask that the District confirm the name(s) of each vendor that it contracts with, or has previously contracted with, to provide these services since January 1, 2020.

* * *

Thank you for your attention to this matter. Please contact us directly if you have any questions.

/s/ Jennifer Jones

Jennifer Jones
Stacy Livingston
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
Jennifer.jones@knightcolumbia.org

EXHIBIT D

"CRT"
"anti-CRT"
"critical race theory"
"culturally responsive teaching"
"gender fluidity"
"non-binary" or "nonbinary"
"1619 Project"
"social construct"
"hormone therapy"
"gender reassignment"
"gender dysmorphia"
"gender expression"
"systemic racism"
"enslaved"
"slavery"
"feminism"
"white guilt"
"BLM"
"Black Lives Matter"
"intersex"
"pronouns"
"trans rights" or "transgender rights"
"transgender"
"TERF"
"AIDs"
"planned parenthood"
"ACLU"
"implicit racism"
"implicit bias"
"IAT" or "implicit association test"
"reparations"
"oppression" or "oppressed" or "oppress"
"eugenics"
"discrimination" or "discriminate" or "discriminatory"
"misogyny" or "misogynist"
"sexism" or "sexist"
"true founding"
"redlining" or "red-lining"
"police brutality"
"overpolicing"
"inequality"
"racial wealth gap"
"lynching"
"equity" or "equitable"
"diversity, equity, and inclusion" or "DEI"

"woke"
"marxism" or "marxist"
"communism" or "communist"
"socialism" or "socialist"
"same-sex"
"homosexuality" or "homosexual"
"heterosexuality" or "heterosexual"
"cisgender" or "cis"
"cultural appropriation"
"cultural competence" or "multicultural competence"
"institutional racism"
"colonialism" or "neo-colonialism" or "colonize" or "decolonize"
"cultural intelligence"
"anti-racism" or "anti-racist" or "antiracism" or "antiracist"
"social justice"
"restorative justice"
"internalized bias"
"bisexual" or "bisexuality"
"normative" or "heteronormative"
"disparate outcomes" or "disparate impact"
"inequity"
"power structure"
"racial hierarchy"
"caste"
"afrocentric" or "afrocentrism" or "eurocentric" or "eurocentrism"
"neoliberal"
"ethnocentric"
"microagression"
"people of color" or "POC" or "BIPOC"
"white privilege"
"underprivileged"
"marginalize"
"minority"
"whiteness"
"blackness"
"social emotional learning"
"Stamped"
"gender theory"
"racial profiling"
"colorblind"
"abortion"
"pregnant" or "pregnancy"
"mifepristone"
“transgenderism”
"gender transitioning"

"gender-affirming"
"hormone replacement therapy" or "HRT"
"sexual orientation"
"drag"
"say their names"
"S.B. 3" or "SB3" or "SB-3" or "senate bill 3"
"H.B. 3987" or "HB3987" or "house bill 3987"
"New York Times" or "NYT"
"Nikole Hannah-Jones" or "Nikole Hannah Jones"
"queer"

EXHIBIT E

Subject: Knight First Amendment Institute information request, Reference #P000953-033023
Date: Wednesday, June 14, 2023 at 6:51:57 PM Eastern Daylight Time
From: Jennifer Jones
To: Williams, Ali

Dear Ali,

Thank you again for speaking with us yesterday regarding the Knight First Amendment Institute's public information request, Reference #P000953-033023. As we discussed, it would be helpful if the District could address the following questions as we work to further clarify our request in response to its correspondence dated June 8, 2023.

First, it is our understanding that the Gaggle and Lightspeed Systems services the District uses to monitor students' digital activities provide a user interface, sometimes called a "dashboard," and that the dashboard generates analytics reports. These reports provide school district administrators with data about the types of content the monitoring software has flagged. See, for example, Lightspeed's Filter Reports and Gaggle's Dashboard Reports. These reports could potentially give us insight into how the District uses the Lightspeed and Gaggle systems, which could potentially aid us in narrowing the scope of our request. Can the District confirm whether it has possession of this information? If so, would it be willing to prioritize production of this information to the Institute?

Second, the District indicated in its correspondence dated June 8, 2023 that its search of all current and former employees' emails for the time period of January 1, 2020, to March 30, 2023, using the 140 search terms that we submitted, resulted in an email count of 2,400,179 potentially responsive emails. We'd like to know if the District is able to further limit these email search results to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle."

Please let me know if you have any questions.

Thank you,
Jennifer

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT F

Tex. Atty. Gen. Op. OR2023-20568 (Tex.A.G.), Tex. Atty. Gen. Op. 2023-20568, 2023 WL 4332799

Office of the Attorney General

State of Texas
Informal Letter Ruling No. OR2023-20568
June 16, 2023

***1** Ms. Alexandra M. Williams
Counsel for Grapevine-Colleyville Independent School District
Jackson Walker, L.L.P.
777 Main Street, Suite 2100
Fort Worth, Texas 76102

Dear Ms. Williams:
You ask whether certain information is subject to required public disclosure under the Public Information Act (the "Act"), chapter 552 of the Government Code. Your request was assigned ID# 062638 (Internal Ref: P000953-033023).

The Grapevine-Colleyville Independent School District (the "district"), which you represent, received a request for information, including communications, regarding the district's digital surveillance system. You claim the submitted information is excepted from disclosure under section 552.139 of the Government Code. We have considered the exception you claim and reviewed the submitted information.

Section 552.139 of the Government Code provides, in relevant part:
(a) Information is excepted from [required public disclosure] if it is information that relates to computer network security, to restricted information under Section 2059.055 [of the Government Code], or to the design, operation, or defense of a computer network.

(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; [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.

Id. § 552.139(a), (b)(1)-(2), (4). Section 2059.055 of the Government Code provides, in pertinent part:
(b) Network security information is confidential under this section if the information is:
(1) related to passwords, personal identification numbers, access codes, encryption, or other components of the security system of a governmental entity;

(2) collected, assembled, or maintained by or for a governmental entity to prevent, detect, or investigate criminal activity; or

 © 2023 Thomson Reuters. No claim to original U.S. Government Works.

(3) related to an assessment, made by or for a governmental entity or maintained by a governmental entity, of the vulnerability of a network to criminal activity.

Id. § 2059.055(b). You state the submitted information reveals "certain words and website addresses which the [d]istrict has chosen to block or filter ... because of their propensity to expose the [district's computers and networks to malicious sites and other risks." You state the information at issue, if released, "may expose the [d]istrict to unnecessary security threats." Based on these arguments and our review of the information, we find the information we marked relates to computer network security, and the design, operation, or defense of the district's computer network. Accordingly, the district must withhold the information we marked under section 552.139 of the Government Code. However, we find you have not demonstrated the remaining information is subject to section 552.139. Accordingly, the district may not withhold any of the remaining information under section 552.139 of the Government Code. The district must release the remaining information.

***2** This letter ruling is limited to the particular information at issue in this request and limited to the facts as presented to us; therefore, this ruling must not be relied upon as a previous determination regarding any other information or any other circumstances.

This ruling triggers important deadlines regarding the rights and responsibilities of the governmental body and of the requestor. For more information concerning those rights and responsibilities, please visit our website at https://www.texasattorneygeneral.gov/open-government/members-public/what-expect-after-ruling-issued or call the OAG's Open Government Hotline, toll free, at (877) 673-6839. Questions concerning the allowable charges for providing public information under the Public Information Act may be directed to the Cost Rules Administrator of the OAG, toll free, at (888) 672-6787.

Sincerely,

D. Michelle Case
Assistant Attorney General
Open Records Division

Tex. Atty. Gen. Op. OR2023-20568 (Tex.A.G.), Tex. Atty. Gen. Op. 2023-20568, 2023 WL 4332799

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

EXHIBIT G

Subject: RE: Knight First Amendment Institute information request, Reference #P000953-033023
Date: Wednesday, June 21, 2023 at 4:27:11 PM Eastern Daylight Time
From: Williams, Ali
To: Jennifer Jones
Attachments: image001.png

Good afternoon, Jennifer:

I have communicated with Grapevine-Colleyville ISD ("GCISD") regarding your email below, which GCISD construes to be a clarification of your clarified request provided in your correspondence to GCISD dated June 2, 2023.

With regard to your first clarification, GCISD has identified reports associated with Lightspeed and/or Gaggle. However, GCISD does not believe such reports are subject to disclosure and will be seeking an opinion from the Attorney General regarding the withholding of such reports.

With regard to your second clarification, pertaining to further limiting the email search results to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle," GCISD has further limited such search. 824 responsive emails have been identified. As required by Texas Gov't Code Sec. 552.2615, GCISD is providing a cost estimate for this part of your records request. GCISD is not waiving its right to charge fees as allowed by law. The estimate includes the time to review each potentially responsive email and its attachments and to redact any information as allowed by law, including but not limited to personally identifiable information of students. GCISD reserves the right to submit other information it finds in these emails to the Attorney General's Office for a determination about its withholding. The cost estimate for your clarified request as provided in your email correspondence below dated June 14, 2023 is as follows:

- Compiling, reviewing, and redacting potentially responsive emails: 824 x 3 minutes = 41.2 hours at $15.00 per hour = $618
- Overhead fee at 20% = $123.6
- Total charges = $741.60

Please note that this is an estimate and the actual cost could be higher.

This cost estimate is being provided in accordance with Texas Gov't Code Sec. 552.2615. Your clarified request will be considered automatically withdrawn if you do not respond in writing within ten business days that you (a) accept the estimated charges, (b) are modifying the request in response to this cost estimate, or (c) have sent a complaint regarding these estimated charges to the attorney general. Your response may be sent by e-mail correspondence or regular mail to me as counsel for GCISD as well as by regular mail, in person, or through communication utilizing GCISD's PIA portal.

Additionally, GCISD, through counsel, received yesterday a ruling made by the Attorney General regarding the correspondence submitted by GCISD, through counsel, on April 13, 2023 and April 20, 2023 regarding your public information request #P000953-033023. The Attorney General ruled that some information shall be released to you and some information shall be withheld. GCISD personnel will release to you the information not subject to be withheld within the required time period.

Regards,
Ali

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com



From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Wednesday, June 14, 2023 5:52 PM
To: Williams, Ali <amwilliams@jw.com>
Subject: Knight First Amendment Institute information request, Reference #P000953-033023

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Dear Ali,

Thank you again for speaking with us yesterday regarding the Knight First Amendment Institute's public information request, Reference #P000953-033023. As we discussed, it would be helpful if the District could address the following questions as we work to further clarify our request in response to its correspondence dated June 8, 2023.

First, it is our understanding that the Gaggle and Lightspeed Systems services the District uses to monitor students' digital activities provide a user interface, sometimes called a "dashboard," and that the dashboard generates analytics reports. These reports provide school district administrators with data about the types of content the monitoring software has flagged. See, for example, Lightspeed's Filter Reports and Gaggle's Dashboard Reports. These reports could potentially give us insight into how the District uses the Lightspeed and Gaggle systems, which could potentially aid us in narrowing the scope of our request. Can the District confirm whether it has possession of this information? If so, would it be willing to prioritize production of this information to the Institute?

Second, the District indicated in its correspondence dated June 8, 2023 that its search of all current and former employees' emails for the time period of January 1, 2020, to March 30, 2023, using the 140 search terms that we submitted, resulted in an email count of 2,400,179 potentially responsive emails. We'd like to know if the District is able to further limit these email search results to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle."

Please let me know if you have any questions.

Thank you,
Jennifer

Jennifer Jones (she/her)
Staff Attorney

Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT H

Alexandra M. Williams
(817) 334-7292 (Direct Dial)
(817) 334-7290 (Direct Fax)
amwilliams@jw.com

June 28, 2023

VIA ONLINE SUBMISSION

The Honorable Ken Paxton
Attorney General, State of Texas
Open Records Section
P.O. Box 12548
Austin, Texas 78711-2548

Re: Clarified Open Records Request of Jennifer Jones of the Knight First Amendment Institute received on June 14, 2023
Internal Ref: P000953-033023

Dear Attorney General Paxton:

I am counsel to the Board of Trustees for Grapevine-Colleyville Independent School District (the "District"). The District received the public information request attached as Exhibit 1[1] on March 30, 2023 ("Original Request"). The District timely requested and obtained a ruling from the Attorney General regarding part of the Original Request.[2] The requestor responded to the District's request for clarification of the remainder of the Original Request on June 14, 2023 ("Clarified Request"), which is attached as Exhibit 2.[3]

In response to the Clarified Request, the District informed the requestor it intended to seek a ruling from the Attorney General with respect to the first part of the Clarified Request and provided a cost estimate pursuant to Texas Government Code § 552.2615 with respect to the second part of the Clarified Request.[4]

[1] Exhibit 1 also contains the District's correspondence to the Attorney General regarding the Original Request as well as the Attorney General's ruling pertaining to same.

[2] Following the receipt of the Attorney General's ruling on part of the Original Request, the District timely produced the documents identified by the Attorney General as not subject to withholding. The Attorney General assigned the District's request pertaining to the Original Request ID# 062638.

[3] The requestor's correspondence containing the clarification followed a telephone call with undersigned counsel regarding the substance of the request, and such correspondence was sent directly to counsel for the District, to be received on behalf of the District.

[4] As of the date of this correspondence, the District has not yet received a response from the requestor regarding the cost estimate. The District reserves the right to seek a ruling from the Attorney General with respect to the information responsive to the second part of the Clarified Request should the requestor timely indicate that she intends to move forward with this portion of the request.

As such, the District now requests an opinion on certain documents attached as Exhibit 3, which are responsive to the first part of the Clarified Request. The first part of the Clarified Request seeks reports from Gaggle and Lightspeed Systems which provide data to District personnel regarding content flagged by Gaggle and Lightspeed Systems during students' and employees' use of District technology.[5]

This correspondence constitutes the District's submission required under Texas Government Code § 552.301(b) and (e) with respect to the Clarified Request. By copy of this letter, the District is informing the requestor of its submission of written comments to the Attorney General regarding the Clarified Request under Section 552.301(b) and (e). Tex. Gov't Code § 552.301(d), (e-1).

TEX. GOV'T CODE § 552.139 – Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers

Exhibit 3 contains the responsive information the District maintains is not subject to disclosure. Exhibit 3 contains a report generated by Gaggle which identifies words and/or subjects monitored by Gaggle and shows the number of instances in which such word and/or subject is flagged by the Gaggle program within the District's technology systems. The District has engaged the services of Gaggle for the purpose of protecting the safety and security of District employees and students, as well as to protect the safety and security of the District's network by preventing computer security incidents.

Certain words, subjects, and/or 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. In other words, 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). The public disclosure of such words, website addresses, and other related information may expose the District to unnecessary security threats. As such, the District requests that Attorney General permit the District to withhold all information responsive to the Request (*i.e.*, the entirety of Exhibit 3).[6]

Conclusion

The District believes that the responsive documents contained in Exhibit 3 should be excepted from disclosure under the Act. The Attorney General has not made a previous determination regarding the specific information contained in Exhibit 3.

By copy of this letter, the District is informing the requestor of its request to the Attorney General, contained herein, for a decision regarding whether the information is within an exception and of

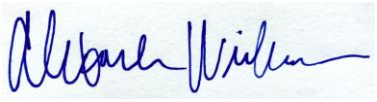
[5] *See* Exhibit 2.

[6] *See* Tex. Att'y Gen. Op. No. OR2019-01233 (finding that a school district must withhold information in response to a similar request for "all urls and keywords that are blocked on school and or district WiFi networks" as such information "relates to computer network security, and the design, operation, or defense of the district's computer network").

its intent to withhold the requested information until a decision is made by your office pursuant to this request. Tex. Gov't Code § 552.301(d), (e-1).

Should you have any questions, please do not hesitate to contact me.

Sincerely,



Alexandra M. Williams
Attorney

Enclosures as noted

cc: Requestor Jennifer Jones, The Knight First Amendment Institute, w/o enclosures (via email)

Paula Barbaroux, Gema Padgett, Alex Harlow w/o enclosures (via email)

EXHIBIT I

Subject: RE: Knight First Amendment Institute information request, Reference #P000953-033023
Date: Thursday, July 20, 2023 at 10:47:23 AM Eastern Daylight Time
From: Williams, Ali
To: Jennifer Jones
CC: Stacy Livingston, Alexander A Abdo
Attachments: image001.png

Jennifer,

I checked with the District regarding payment method, and the District cannot accept a credit card payment. Once the District receives the Institute's payment, it can begin to review the responsive records.

Given the volume of the records and the need to review for FERPA-protected information as well as information that should be presented to the Attorney General for a determination for withholding under the Public Information Act, as well as the other duties of the District employee assisting with this request given that the school year will soon be starting, the District will not be able to provide the responsive documents to the Institute within 10 business days after receiving payment. The District estimates needing 25 business days to review the records and provide responsive documents to the Institute.

Additionally, as noted in my e-mail correspondence to you on June 21, 2023 including the cost estimate, the cost estimate is just an estimate and could be higher. This will not be able to be precisely determined until the conclusion of the District's work in compiling and providing the responsive records is complete. If the District determines before it makes the records available to the Institute that the estimated charges will exceed the charges detailed in the previous written itemized statement (in my June 21, 2023 email) by 20 percent or more, the District will send to the Institute a written updated itemized statement that details all estimated charges that will be imposed, including any allowable charges for labor or personnel costs. If the Institute does not respond in writing to this updated estimate in the time and manner described by Tex. Gov't Code 552.2615(b), the request will be considered to have been withdrawn by the Institute.

Finally, your email below states that the Institute will pay the fees for the request, conditional on the Institute's right to seek judicial review of the denial of the request for a fee waiver. The determination made with regard to the requested fee waiver pursuant to Tex. Gov't Code 552.267(a) lies solely with the District. As stated herein, the District requires the Institute's payment to begin work on this request. Such payment is not conditional.

Please let me know if there is specific information you need in order to provide payment to the District for this request.

Ali

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com

Jackson Walker LLP

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Thursday, July 13, 2023 3:02 PM
To: Williams, Ali <amwilliams@jw.com>
Cc: Stacy Livingston <stacy.livingston@knightcolumbia.org>; Alexander A Abdo <alex.abdo@knightcolumbia.org>
Subject: Re: Knight First Amendment Institute information request, Reference #P000953-033023

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Dear Ali,
Thank you for your response. The Institute will pay for the fees associated with request #P000953-033023, conditional on our right to seek judicial review of the denial of our request for a fee waiver. Please let us know how we can remit payment for information responsive to this request. In the interest of obtaining the information as soon as possible, the Institute would prefer to pay via credit card. Please note that if the District requires payment via check, the Institute would need at least 3 weeks to process the check in accordance with Columbia University's payment processing timeline.
Thank you,

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

From: Williams, Ali <amwilliams@jw.com>
Date: Friday, July 7, 2023 at 10:46 AM
To: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Cc: Stacy Livingston <stacy.livingston@knightcolumbia.org>, Alexander A Abdo <alex.abdo@knightcolumbia.org>
Subject: RE: Knight First Amendment Institute information request, Reference #P000953-033023

Jennifer,

The District does not determine that the standard in Tex. Gov't Code Sec. 552.267(a) is met in this instance, and, therefore, will not waive or reduce the charges associated with the Knight First Amendment Institute's request.

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Friday, June 30, 2023 1:10 PM
To: Williams, Ali <amwilliams@jw.com>
Cc: Stacy Livingston <stacy.livingston@knightcolumbia.org>; Alexander A Abdo <alex.abdo@knightcolumbia.org>
Subject: Re: Knight First Amendment Institute information request, Reference #P000953-033023

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Dear Ali,

Thank you for your response. We write to ask that the District reconsider its decision regarding the Institute's request for a fee waiver, which was included in its public information request #P000953-033023. The Texas Public Information Act allows fees to be waived or reduced if the governmental body determines that providing a copy of the information primarily benefits the general public. Tex. Gov. Code § 552.267(a). Disclosure of the information sought here would primarily benefit the public interest, as it would inform the public about actual or alleged government activity. Specifically, the requested information is necessary to the public's understanding of how schools enforce rules concerning classroom discussions about sexuality, gender, and race. *See, e.g.*, Mark Keierleber, *The risks of student surveillance amid abortion bans and LGBTQ restrictions*, THE GUARDIAN (Sep. 8, 2022, 6:00 PM), https://www.theguardian.com/education/2022/sep/08/abortion-bans-school-surveillance-lgbtq-restrictions; Brian Lopez, *Republican bill that limits how race, slavery and history are taught in Texas schools becomes law*, THE TEXAS TRIBUNE (Dec. 2, 2021, 6:00 PM), https://www.texastribune.org/2021/12/02/texas-critical-race-theory-law/#:~:text=Republican%20bill%20that%20limits%20how,public%20policy%20or%20social%20affairs.%E2%80%9D. Moreover, disclosure would not further the Knight Institute's commercial interest. As indicated in our request, The Knight First Amendment Institute is a New York not-for-profit corporation based at Columbia University that works to preserve and expand the freedoms of speech and the press through strategic litigation, research, and public education. The Institute will make any information disclosed available to the public at no cost.

In light of the above, we ask that the District waive or reduce the $741.60 fee estimate it provided in its correspondence below, dated June 21, 2023. Thank you for considering our request.

Regards,
Jennifer

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

From: Williams, Ali <amwilliams@jw.com>
Date: Wednesday, June 21, 2023 at 4:27 PM
To: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Subject: RE: Knight First Amendment Institute information request, Reference #P000953-033023

Good afternoon, Jennifer:

I have communicated with Grapevine-Colleyville ISD ("GCISD") regarding your email below, which GCISD construes to be a clarification of your clarified request provided in your correspondence to GCISD dated June 2, 2023.

With regard to your first clarification, GCISD has identified reports associated with Lightspeed and/or Gaggle. However, GCISD does not believe such reports are subject to disclosure and will be seeking an opinion from the Attorney General regarding the withholding of such reports.

With regard to your second clarification, pertaining to further limiting the email search results to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle," GCISD has further limited such search. 824 responsive emails have been identified. As required by Texas Gov't Code Sec. 552.2615, GCISD is providing a cost estimate for this part of your records request. GCISD is not waiving its right to charge fees as allowed by law. The estimate includes the time to review each potentially responsive email and its attachments and to redact any information as allowed by law, including but not limited to personally identifiable information of students. GCISD reserves the right to submit other information it finds in these emails to the Attorney General's Office for a determination about its withholding. The cost estimate for your clarified request as provided in your email correspondence below dated June 14, 2023 is as follows:

- Compiling, reviewing, and redacting potentially responsive emails: 824 x 3 minutes = 41.2 hours at $15.00 per hour = $618
- Overhead fee at 20% = $123.6
- Total charges = $741.60

Please note that this is an estimate and the actual cost could be higher.

This cost estimate is being provided in accordance with Texas Gov't Code Sec. 552.2615. Your clarified request will be considered automatically withdrawn if you do not respond in writing within ten business days that you (a) accept the estimated charges, (b) are modifying the request in response to this cost estimate, or (c) have sent a complaint regarding these estimated charges to the attorney general. Your response may be sent by e-mail correspondence or regular mail to me as counsel for GCISD as well as by regular mail, in person, or through communication utilizing GCISD's PIA portal.

Additionally, GCISD, through counsel, received yesterday a ruling made by the Attorney General regarding the correspondence submitted by GCISD, through counsel, on April 13, 2023 and April 20, 2023 regarding your public information request #P000953-033023. The Attorney General ruled that some information shall be released to you and some information shall be withheld. GCISD personnel will release to you the information not subject to be withheld within the required time period.

Regards,
Ali

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com



From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Wednesday, June 14, 2023 5:52 PM
To: Williams, Ali <amwilliams@jw.com>
Subject: Knight First Amendment Institute information request, Reference #P000953-033023

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Dear Ali,

Thank you again for speaking with us yesterday regarding the Knight First Amendment Institute's public information request, Reference #P000953-033023. As we discussed, it would be helpful if the District could address the following questions as we work to further clarify our request in response to its correspondence dated June 8, 2023.

First, it is our understanding that the Gaggle and Lightspeed Systems services the District uses to monitor students' digital activities provide a user interface, sometimes called a "dashboard," and that the dashboard generates analytics reports. These reports provide school district administrators with data about the types of content the monitoring software has flagged. See, for example, Lightspeed's Filter Reports and Gaggle's Dashboard Reports. These reports could potentially give us insight into how the District uses the Lightspeed and Gaggle systems, which could potentially aid us in narrowing the scope of our request. Can the District confirm whether it has possession of this information? If so, would it be willing to prioritize production of this information to the Institute?

Second, the District indicated in its correspondence dated June 8, 2023 that its search of all current and former employees' emails for the time period of January 1, 2020, to March 30, 2023, using the 140 search terms that we submitted, resulted in an email count of 2,400,179 potentially responsive emails. We'd like to know if the District is able to further limit these email search results to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle."

Please let me know if you have any questions.

Thank you,
Jennifer

Jennifer Jones (she/her)
Staff Attorney

Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT J

Tex. Atty. Gen. Op. OR2023-30020 (Tex.A.G.), Tex. Atty. Gen. Op. 2023-30020, 2023 WL 6369986

Office of the Attorney General

State of Texas
Informal Letter Ruling No. OR2023-30020
August 31, 2023

***1** Ms. Alexandra M. Williams
Counsel for Grapevine-Colleyville Independent School District
Jackson Walker, L.L.P.
777 Main Street, Suite 2100
Fort Worth, Texas 76102

Dear Ms. Williams:
You ask whether certain information is subject to required public disclosure under the Public Information Act (the "Act"), chapter 552 of the Government Code. Your request was assigned ID# 077074 (Internal Ref: P000953-033023).

The Grapevine-Colleyville Independent School District (the "district"), which you represent, received a request for information, including a report regarding the district's digital surveillance system. [1] You claim the submitted information is excepted from disclosure under section 552.139 of the Government Code. We have considered the exception you claim and reviewed the submitted information.

Section 552.139 of the Government Code provides, in relevant part:
(a) Information is excepted from [required public disclosure] if it is information that relates to computer network security, to restricted information under Section 2059.055 [of the Government Code], or to the design, operation, or defense of a computer network.

(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; [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.

Id. § 552.139(a), (b)(1)-(2), (4). You state the submitted information consists of a report generated by the district's digital surveillance system that reveals the words and subjects that are being monitored by the system and the number of instances they are flagged by the program. You explain that the district has engaged these services to protect the safety and security of

 © 2025 Thomson Reuters. No claim to original U.S. Government Works.

district students and employees and the safety and security of the district's network by preventing computer security incidents. Based on these arguments and our review of the information, we agree the information you marked relates to computer network security, and the design, operation, or defense of the district's computer network. Accordingly, the district must withhold the information you marked under section 552.139 of the Government Code.

***2** This letter ruling is limited to the particular information at issue in this request and limited to the facts as presented to us; therefore, this ruling must not be relied upon as a previous determination regarding any other information or any other circumstances.

This ruling triggers important deadlines regarding the rights and responsibilities of the governmental body and of the requestor. For more information concerning those rights and responsibilities, please visit our website at https://www.texasattorneygeneral.gov/open-government/members-public/what-expect-after-ruling-issued or call the OAG's Open Government Hotline, toll free, at (877) 673-6839. Questions concerning the allowable charges for providing public information under the Public Information Act may be directed to the Cost Rules Administrator of the OAG, toll free, at (888) 672-6787.

Sincerely,

Michelle Garza
Assistant Attorney General
Open Records Division

Footnotes

1 You state the district sought and received clarification of the information requested. *See* Gov't Code § 552.222 (providing if request for information is unclear, governmental body may ask requestor to clarify request); *see also City of Dallas v. Abbott*, 304 S.W.3d 380, 387 (Tex. 2010) (holding that when a governmental entity, acting in good faith, requests clarification or narrowing of an unclear or overbroad request for information, the ten-day period to request an attorney general ruling is measured from the date the request is clarified or narrowed).

Tex. Atty. Gen. Op. OR2023-30020 (Tex.A.G.), Tex. Atty. Gen. Op. 2023-30020, 2023 WL 6369986

End of Document © 2025 Thomson Reuters. No claim to original U.S. Government Works.

EXHIBIT K

Subject: [Records Center] Open Public Records Request :: P000953-033023
Date: Monday, October 23, 2023 at 10:17:06 AM Eastern Daylight Time
From: GCISD Support
To: Jennifer Jones

--- Please respond above this line ---

GRAPEVINE COLLEYVILLE INDEPENDENT SCHOOL DISTR CT

RE: PUBLIC RECORDS REQUEST of March 30, 2023, Reference # P000953-033023

Dear Ms. Jones,

Upon receipt of your payment, the District downloaded the 824 responsive emails and began its review for the purposes of redacting confidential information. In doing so, we discovered that almost all emails contain the very information the Texas Attorney General agreed must be withheld. The emails contain information about subjects being searched, keywords being monitored, threat types, and why the communication was flagged for review by District personnel. All of that information would be redacted and the result would be emails with very little information. We have attached a sample of a redacted email to illustrate the point.

If you agree that once redacted the information is of no use, the District is willing to refund the payment and close this request. If not, the District will once again seek an opinion of the Attorney General's office. I have attached a copy of the previous Attorney General's ruling.

Please let me know how you would like to proceed.

Sincerely,

Paula Barbaroux

Chief Operations Officer

To monitor the progress or update this request please log into the Open Public Records Center

Powered by GovQA

EXHIBIT L

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
info@knightcolumbia.org

November 7, 2023

Ali Williams
Jackson Walker LLP
777 Main Street Suite 2100
Fort Worth, TX 76102
amwilliams@jw.com

Re: Public Information Act request, Reference # P000953-033023

Counsel,

The Knight First Amendment Institute at Columbia University received an email from Grapevine-Colleyville Independent School District dated October 23, 2023 offering to refund our payment for the processing of 824 emails responsive to subsection (c) of our information request because, according to the District, most of the information in those emails would be redacted. The District also stated that, if the Institute nonetheless insisted on the processing and production of those emails, the District would seek an opinion from the Attorney General's office. We would like the District to continue to process and disclose the 824 emails it has identified as responsive to our request.

Moreover, we do not agree with the District that the information it intends to redact from the emails falls within any disclosure exception. On June 2, 2023 the Institute identified search terms to clarify the information we seek related to subsection (c) of our original request, and on June 14, 2023, we sent an email further narrowing the scope of information requested in subsection (c) to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle." The search terms that we provided specifically relate to concepts and terminology associated with social and political issues and identities such as race, gender, and sexual orientation. Neither these terms nor their presence in the emails at issue would reveal information related to the "design, operation, or defense of a computer network." Tex. Gov't Code § 552.139(a). Previously, you indicated that the District had blocked or

filtered from its network "[c]ertain words and website addresses" because of their propensity to expose the District's network to "malicious sites." But the search terms we've provided are not the kind of terms that could expose the District's network to a "computer security incident." *See* Tex. Gov't Code § 552.139(b)(4) (limiting excepted information to that which "directly "aris[es]" from "routine efforts" to address a "*computer* security incident") (emphasis added). At most, they would reveal that the District monitors its students' reading of material related to certain political and social topics, but that is no basis for redacting the search terms.

Finally, while we understand that you intend to seek an opinion from the Attorney General, we believe that such a request would be untimely. We sent (and the District received) our final clarification of the request on June 14, 2023. If the District wished to withhold any requested information, it was required to ask for an Attorney General opinion within ten days of receiving the clarified request. Tex Gov't Code § 552.301(b); *see also City of Dallas v. Abbott*, 304 S.W.3d 380, 387 (Tex. 2010) (when a governmental entity requests a good-faith clarification of a request, the ten-day period to request an attorney general ruling is measured from the date of clarification). In your June 21 correspondence to us and in your June 28 request to the Attorney General, you indicated that the District "reserves the right to submit other information it finds in these emails to the Attorney General's Office for a determination about its withholding." But the Public Information Act is clear that the ten-day clock to request an Attorney General opinion runs from the day the request is received or clarified. *See Dallas Area Rapid Transit v. Dallas Morning News,* 4 S.W.3d 469, 475 (Tex. App. 1999) (finding that the ten-day clock for requesting Attorney General opinion ran from the date of the request where the government agency was capable of perceiving the connection between requested information and an exemption that could apply in the future). As such, the information at issue is presumptively subject to disclosure. Tex. Gov't Code § 552.302; *Simmons v. Kuzmich*, 166 S.W.3d 342, 350 (Tex. App. 2005).

* * *

Accordingly, we ask that the District complete its processing and disclosure of the 824 emails responsive to our June 14 clarified request. Please let me know if you have any questions. Thank you.

/s/ Jennifer Jones
Jennifer Jones
Knight First Amendment Institute
at Columbia University

475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT M

Subject: RE: Knight Institute Public Information Act request, Reference # P000953-033023.
Date: Tuesday, November 14, 2023 at 5:38:20 PM Eastern Standard Time
From: Williams, Ali
To: Jennifer Jones
CC: Alexander A Abdo, Hannah Vester
Attachments: image001.png

Jennifer,

Pursuant to the request in your correspondence, the District will continue to process for production the emails it has identified as responsive to KFAI's request, as clarified, noting it has KFAI's payment on file. The District estimates it will be able to complete the review of such emails for production by end of the week, and production will be made to KFAI through the PIA portal utilized by the District (through which KFAI has received other correspondence from the District). The District's continued review will be for the purpose of making redactions in accordance with the Family Educational Rights and Privacy Act (FERPA) and with the Attorney General's ruling that certain information should be withheld as it relates to computer network security, and the design, operation, or defense of the District's computer network.

Best,
Ali

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com

JW | Jackson Walker LLP

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Tuesday, November 7, 2023 3:28 PM
To: Williams, Ali <amwilliams@jw.com>
Cc: Alexander A Abdo <alex.abdo@knightcolumbia.org>; Hannah Vester <hannah.vester@knightcolumbia.org>
Subject: Knight Institute Public Information Act request, Reference # P000953-033023.

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Ali,

Please see the attached correspondence regarding the Knight First Amendment Institute's Public Information Act request, Reference # P000953-033023.

Please let me know if you have any questions.

Thank you,
Jennifer

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT N

Subject: Re: Knight Institute Public Information Act request, Reference # P000953-033023.
Date: Thursday, November 16, 2023 at 4:38:35 PM Eastern Standard Time
From: Jennifer Jones
To: Williams, Ali
CC: Alexander A Abdo, Hannah Vester
Attachments: image001.png

Ali,

We appreciate your update that the District will continue to process the emails responsive to the Institute's request. However, we object to the District's reliance on the previous Attorney General opinions dated June 16 and August 31, 2023 to redact information in the emails under section 552.139 of the Government Code. Those opinions made clear that the Attorney General's rulings are "limited to the particular information" presented for review and "must not be relied upon as a previous determination regarding any other information or any other circumstances." Tex. Atty. Gen. Op. 2023-20568 (June 16, 2023); Tex. Atty. Gen. Op. 2023-30020 (Aug. 31, 2023).

Accordingly, the previous opinions do not authorize redactions made in response to the second part of our clarified request, which the District expressly excluded from its June 28 submission to the Attorney General.

As we explained in our correspondence dated November 7, if the District contends that information responsive to part two of the Institute's clarified request is excludable, it was required to request an additional opinion within ten days of receiving that clarification on June 14. Because the District missed this deadline and is not permitted to rely on previous Attorney General opinions, it is not permitted to redact any information responsive to our clarified request under section 552.139.

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

From: Williams, Ali <amwilliams@jw.com>
Date: Tuesday, November 14, 2023 at 5:38 PM
To: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Cc: Alexander A Abdo <alex.abdo@knightcolumbia.org>, Hannah Vester <hannah.vester@knightcolumbia.org>
Subject: RE: Knight Institute Public Information Act request, Reference # P000953-033023.

Jennifer,

Pursuant to the request in your correspondence, the District will continue to process for production the

emails it has identified as responsive to KFAI's request, as clarified, noting it has KFAI's payment on file. The District estimates it will be able to complete the review of such emails for production by end of the week, and production will be made to KFAI through the PIA portal utilized by the District (through which KFAI has received other correspondence from the District). The District's continued review will be for the purpose of making redactions in accordance with the Family Educational Rights and Privacy Act (FERPA) and with the Attorney General's ruling that certain information should be withheld as it relates to computer network security, and the design, operation, or defense of the District's computer network.

Best,
Ali

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com

JW | Jackson Walker LLP

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Tuesday, November 7, 2023 3:28 PM
To: Williams, Ali <amwilliams@jw.com>
Cc: Alexander A Abdo <alex.abdo@knightcolumbia.org>; Hannah Vester <hannah.vester@knightcolumbia.org>
Subject: Knight Institute Public Information Act request, Reference # P000953-033023.

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Ali,

Please see the attached correspondence regarding the Knight First Amendment Institute's Public Information Act request, Reference # P000953-033023.

Please let me know if you have any questions.

Thank you,
Jennifer

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT O

From: **Lightspeed Systems** do_not_reply@lightspeedsystems.com
Subject: [EXTERNAL] Lightspeed Systems Notification for [redacted]: Self-Harm
Date: August 24, 2022 at 6:08 PM
To:

Lightspeed Systems®

Incident: Self-Harm

[redacted]

06:07:53 PM

Search: can you die from abortion

https://www.google.com/search

View Student Activity

Lightspeed Systems

2500 Bee Cave Road | Building One, Suite 350 | Austin, TX 78746

Notification Settings.

From: **Lightspeed Systems** do_not_reply@lightspeedsystems.com
Subject: [EXTERNAL] Lightspeed Systems Notification for [redacted]: Self-Harm
Date: October 24, 2022 at 11:12 PM
To:

Lightspeed Systems®

Incident: Self-Harm

[redacted]

11:12:08 PM

Search: can you die from bedbug bites

https://www.google.com/search

View Student Activity

Lightspeed Systems

2500 Bee Cave Road | Building One, Suite 350 | Austin, TX 78746

Notification Settings.

EXHIBIT P

Alexandra M. Williams
(817) 334-7292 (Direct Dial)
(817) 334-7290 (Direct Fax)
amwilliams@jw.com

April 17, 2025

VIA ONLINE SUBMISSION

The Honorable Ken Paxton
Attorney General, State of Texas
Open Records Section
P.O. Box 12548
Austin, Texas 78711-2548

Re: Clarified Open Records Request of Jennifer Jones of the Knight First Amendment Institute received on June 14, 2023
Internal Ref: P000953-033023

Dear Attorney General Paxton:

I am counsel to the Board of Trustees for Grapevine-Colleyville Independent School District (the "District"). The District received the public information request attached as Exhibit 1[1] on March 30, 2023 ("Original Request"). The District requested and obtained a ruling from the Attorney General regarding part of the Original Request.[2] The requestor responded to the District's request for clarification of the remainder of the Original Request on June 14, 2023 ("Clarified Request"), which is attached as Exhibit 2.[3]

The requestor divided the Clarified Request into two separate but related portions. The first portion pertained to analytics reports generated by Lightspeed and Gaggle, which was the subject of correspondence to the Attorney General submitted by this office on June 28, 2023, on which the Attorney General made a determination on August 31, 2023.[4] The Attorney General determined that the District must withhold the information submitted under Section 552.139 as the information related to computer network security, and the design, operation, or defense of the District's

[1] Exhibit 1 also contains the District's 10-day and 15-day correspondence to the Attorney General regarding the Original Request and documents sought to be withheld in response to the Original Request as well as the Attorney General's ruling pertaining to same.

[2] Following the receipt of the Attorney General's ruling on part of the Original Request, the District timely produced the documents identified by the Attorney General as not subject to withholding.

[3] The requestor's correspondence containing the clarification followed a telephone call with undersigned counsel regarding the substance of the request, and such correspondence was sent directly to counsel for the District, to be received on behalf of the District.

[4] This June 28, 2023 correspondence to the Attorney General and August 31, 2023 correspondence from the Attorney General are attached together as Exhibit 3.

computer network.[5] The documents were withheld accordingly. The Attorney General directly provided the requestor with a copy of the Attorney General's determination and ruling.

The second part of the Clarified Request sought a narrowing of 2,400,179 potentially responsive e-mails of current and former District employees using 140 search terms provided by the requestor by limiting these communications to (1) e-mails to and from "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle." The clarification narrowed the number of responsive records to 824 e-mails. The District sent a cost estimate to the requestor pursuant to Texas Government Code § 552.2615 regarding these 824 e-mails responsive to the clarified version of the second part of the Clarified Request. The requestor paid the amount sent in the cost estimate for the processing and production of these communications. The 824 e-mails included keywords that corresponded to the information the Attorney General determined must be withheld in its August 31, 2023 correspondence. As such, the District redacted that information previously determined to be required to be withheld pursuant to Section 552.139 when producing the 824 e-mails to the requestor.

The requestor has contested the District's redaction of those terms despite the Attorney General's determination that such information must be withheld.[6] As such, the District now specifically requests an opinion on certain documents attached as Exhibit 4, which is a representative sample of documents responsive to the clarified second part of the Clarified Request.[7]

This correspondence constitutes the District's submission required under Texas Government Code § 552.301(b) and (e) with respect to the Clarified Request. By copy of this letter, the District is informing the requestor of its submission of written comments to the Attorney General regarding the Clarified Request under Section 552.301(b) and (e). Tex. Gov't Code § 552.301(d), (e-1).

TEX. GOV'T CODE § 552.139 – Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers

Exhibit 4 contains a representative sample of the responsive information the District maintains is not subject to disclosure.[8] The records in the representative sample are e-mails either to and from "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle." These e-mails contain keywords, a notation about "threat type" and a note about why the incident was flagged, which is information that corresponds to the analytics reports responsive to the first part of the Clarified Request, which the Attorney General determined must be withheld pursuant to Section 552.139. The District has engaged the services of Gaggle for the purpose of protecting the safety and security of District employees and students, as well as to

[5] *See* Exhibit 3.

[6] The requestor has filed suit against the District regarding this redacted information. This litigation, *Knight First Amendment Institute at Columbia University v. Grapevine-Colleyville Independent School District*, Cause No. 348-362718-25, is currently pending in the 348th District Court, Tarrant County, Texas.

[7] The documents in Exhibit 4 are a representative sample of the 824 e-mails as referenced herein.

[8] The records in Exhibit 4 have been marked to indicate the portions the District is requesting to redact before production. Additionally, FERPA information has already been redacted on the records in Exhibit 4.

protect the safety and security of the District's network by preventing computer security incidents. These e-mails demonstrate the services provided by Gaggle in order to provide that safety and security to the District's network.

Certain words, subjects, and/or website addresses have been chosen by Gaggle and/or Lightspeed because of their propensity to expose the District's computers and network to malicious sites and other risks.[9] In other words, 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). The public disclosure of the keywords, threat types, and other related information may expose the District to unnecessary security threats. As such, the District requests that Attorney General permit the District to withhold the marked information in Exhibit 4.[10]

Finally, the District is aware that more than 10 business days have passed since receiving the Request. The Act provides that an untimely request for an Attorney General decision causes the information to be presumed to be subject to required public disclosure "unless there is a compelling reason to withhold the information." Tex. Gov't Code § 552.302. However, the Attorney General has routinely determined that Section 552.139 provides a compelling reason to overcome the presumption of openness and will evaluate the applicability of that section to information submitted by a governmental body past the 10-day deadline. *See* Tex. Atty. Gen. Op. OR2020-15920, 2020 WL 3120750; Tex. Atty. Gen. Op. OR2018-02510, 2018 WL 871288. As such, the District requests the Attorney General consider the applicability of Section 552.139 to the representative sample of responsive records contained in Exhibit 4.

Conclusion

The District believes that the representative sample of responsive documents contained in Exhibit 4 should be excepted from disclosure under the Act. The District maintains that the Attorney General has made a previous determination regarding this information in its determination dated August 31, 2023 in opining that the related information in the analytics reports must be withheld, but now submits this separate request for ruling so as to obtain the Attorney General's determination regarding these specific records.

By copy of this letter, the District is informing the requestor of its request to the Attorney General, contained herein, for a decision regarding whether the information is within an exception and of its intent to withhold the requested information until a decision is made by your office pursuant to this request. Tex. Gov't Code § 552.301(d), (e-1).

[9] The District uses the products provided by Gaggle and Lightspeed, including the words, subjects, and website addresses to be caught by the products' filters, as provided and without further customization by the District.

[10] *See* Tex. Att'y Gen. Op. No. OR2019-01233 (finding that a school district must withhold information in response to a similar request for "all urls and keywords that are blocked on school and or district WiFi networks" as such information "relates to computer network security, and the design, operation, or defense of the district's computer network").

Should you have any questions, please do not hesitate to contact me.

Sincerely,



Alexandra M. Williams
Attorney

Enclosures as noted

cc: Requestor Jennifer Jones, The Knight First Amendment Institute, w/o enclosures (via email)

Paula Barbaroux, Alex Harlow (via email)

Charles Crawford, Lucas Henry (via email)

EXHIBIT Q

May 27, 2025

Honorable Ken Paxton
Texas Attorney General
Open Records Division
P.O. Box 12548
Austin, Texas 78711-2548

Via: PIA Electronic Filing System

Re: Public Records Request of Knight First Amendment Institute at Columbia University to Grapevine-Colleyville Independent School District (No. P000953-033023).

Dear General Paxton,

We represent the Knight First Amendment Institute at Columbia University ("Knight Institute"), the requestor of the public information at issue in the above-referenced matter. On April 17, 2025, Grapevine-Colleyville Independent School District ("District") submitted an untimely request for an opinion from your office, seeking retroactive authorization to withhold public records sought by the Knight Institute nearly two years ago that are now the subject of active litigation. *See* Plaintiff's Original Petition and Request for Writ of Mandamus, *Knight First Amend. Inst. at Colum. Univ. v. Grapevine-Colleyville Indep. Sch. Dist.*, No. 348-362718-25 (348th Dist. Ct., Tarrant Cnty., Mar. 12, 2025) (attached as Exhibit A).

As the District acknowledges in its Request Letter, it should have sought an opinion from your office at the time the Knight Institute paid the fees to process the records it requested in the second part of its Clarified Request No. 2. *See* Request Letter at 3. Its failure to do so requires the District to show a "compelling" reason to withhold the responsive records to overcome the presumption that those records are now "subject to required public disclosure[.]" Gov't Code § 552.302. Whether or not the District can establish a "compelling" reason is a question now before the district court and, therefore, a question your office should decline to consider. *See* Ex. A ¶¶ 26-38, 43; *Kallinen v. City of Houston*, 462 S.W.3d 25, 28 (Tex. 2015) (Attorney General "does not claim exclusive jurisdiction to decide open records issues"); *cf.* Tex. Atty. Gen. Op. No. KP-0304 at 1, n.3 (2020) (noting Attorney General's "long-standing policy of generally refraining from addressing issues involved in pending litigation").

Abstention is particularly appropriate here because factual issues that cannot be resolved by your office affect the District's ability to establish a "compelling" justification for withholding. *See Paxton v. City of Dallas*, 509 S.W.3d 247, 259 (Tex. 2017) ("[A] reason to withhold information will be 'compelling' only when it is of such a pressing nature (e.g., urgent, forceful, or demanding)

that it outweighs the interests favoring public access to the information and overcomes section 552.302's presumption that disclosure is required.");[1] Open Records Decision No. 592 at 2 (1991) (Attorney General cannot resolve factual disputes in the opinion process). Indeed, the District originally informed the Knight Institute of its intent to seek an untimely Attorney General decision a year-and-a-half ago, on October 23, 2023, after being instructed by the Knight Institute to proceed with processing the records at issue in the second part of Clarified Request No. 2. Ex. A ¶¶ 34-35. But the District chose not to act until after the Knight Institute filed suit in March of this year. The District's lack of urgency in protecting the responsive records severely undercuts its position that the computer network security exception, Gov't Code § 552.139, if it even applies to these records,[2] is alone a compelling reason to withhold them.

Alternatively, if you do address the question of whether the District has met its burden to establish a compelling justification for continued withholding, you should find that the District has not. On the record before it, your office can (and should) find that:

1) The District was informed by your office in its August 31, 2023 opinion that the ruling "must not be relied upon as a previous determination regarding any other information or any other circumstances[,]" Atty. Gen. Op. OR2023-30020, 2023 WL 6369986, at *2 (Aug. 31, 2023);
2) The District was aware of this when it processed the second part of the Knight Institute's Clarified Request No. 2, which sought records materially different from the part of Clarified Request No. 2 for which the District requested an opinion, *see* Opinion Request Letter at 1-2 (describing its reliance on the Aug. 31, 2023 opinion in handling the second part of Clarified Request No. 2);
3) The District's reliance on the Aug. 31, 2023 opinion to withhold the responsive records at issue in the second part of Clarified Request No. 2 was improper given your office's admonishment not to use the Aug. 31, 2023 opinion as a previous determination;
4) By waiting a year-and-a-half to seek an Attorney General opinion—opting only to do so after the filing of litigation seeking disclosure of the responsive records—the District declined to act with the kind of urgency needed to show that continued withholding is "of such a pressing nature … that it outweighs the interests favoring public access[.]" *Paxton*, 509 S.W.3d at 259.

[1] *See also id.* at 258 ("The meaning of the term 'compelling' is of vital importance to our analysis because it represents a qualitative limitation on the justifications that permit withholding information from public disclosure.").

[2] The Knight Institute reserves its position on the substantive applicability of the computer network security exception for the proceedings before the district court in its pending litigation over these records.

The District offers little to meet its burden to overcome the presumption of public disclosure that has attached to these records. Its own conduct demonstrates that the District did not view as urgent the need to protect the responsive records, and its application of the computer network security exception to a representative sample of the responsive records is insufficient.[3]

The District could have made a more particularized showing to establish an imminent need to protect *specific* records under the computer network security exception. *See* PUBLIC INFORMATION ACT HANDBOOK 2024, at 43 ("Conclusory assertions that a particular exception applies to requested information will not suffice."). On the other side of the equation—the interests favoring public access—it defies belief that the District has an ongoing need for blanket permission to apply the computer network security exception to nearly two-year-old records containing keywords such as "New York Times," "ACLU," "inequality" or "social construct." Ex. A, pp. 46-47 of 94.

Accordingly, the Knight Institute respectfully requests that your office either (1) abstain from issuing a decision in this matter due to pending litigation; or (2) find that the District has not met its burden to establish a compelling justification to withhold the records at issue here.

Respectfully Submitted,

/s/ Peter B. 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
psteffensen@mail.smu.edu

Thomas S. Leatherbury
State Bar No. 12095275
THOMAS S. LEATHERBURY LAW, PLLC
1901 N. Akard St.
Dallas, TX 75201

[3] Nor, given the District's actions here, should the interests that "animate" the computer network security exception mandate that the exception itself be treated as "compelling in [its] own right." *Paxton*, 509 S.W.3d at 256; *see Tex. Comm'n on Env't Quality v. Sierra Club*, No. 03-21-00256-CV, 2022 WL 17096693, at *6 (Tex. App.—Austin Nov. 22, 2022, pet. denied) (holding the deliberative process privilege on its own does not constitute a compelling reason to overcome the presumption of public disclosure); *see also* OFFICE OF THE ATTORNEY GENERAL OF TEXAS, PUBLIC INFORMATION ACT HANDBOOK 2024, at 44 ("In the great majority of cases, the governmental body will not be able to overcome that presumption and must promptly release the requested information.").

Tel. (214) 213-5004
tom@tsleatherbury.com

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

Attorneys for Knight First Amendment Institute at Columbia University

cc: Alexandra M. Williams, Attorney for the Board of Trustees for Grapevine-Colleyville Independent School District, without enclosures (via email)

Charles Crawford, Lucas Henry, without enclosures (via email)

EXHIBIT R

KEN PAXTON
ATTORNEY GENERAL OF TEXAS

June 26, 2025

Ms. Alexandra M. Williams
Counsel for the Grapevine-Colleyville Independent School District
Jackson Walker LLP
777 Main Street, Suite 2100
Fort Worth, Texas 76102

OR2025-022099

Dear Ms. Williams:

You ask whether certain information is subject to required public disclosure under the Public Information Act (the "Act"), chapter 552 of the Government Code. Your request was assigned ID# 25-016471 (Ref. ID # P000953-033023).

The Grapevine-Colleyville Independent School District (the "district"), which you represent, received a request for information, including reports pertaining to the district's use of digital surveillance systems.[1] You state you have redacted student-identifying information from the submitted documents pursuant to the Family Educational Rights and Privacy Act ("FERPA"), section 1232g of title 20 of the United States Code.[2] You claim some of the submitted information is excepted from disclosure under section 552.139 of

[1] You state, and provide documentation demonstrating, the district sought and received clarification of the information requested. *See* Gov't Code § 552.222(b) (stating if information requested is unclear to governmental body or if large amount of information has been requested, governmental body may ask requestor to clarify or narrow request, but may not inquire into purpose for which information will be used); *City of Dallas v. Abbott*, 304 S.W.3d 380 (Tex. 2010) (holding when governmental entity, acting in good faith, requests clarification of unclear or overbroad request for public information, ten-business-day period to request attorney general opinion is measured from date request is clarified or narrowed).

[2] The United States Department of Education Family Policy Compliance Office (the "DOE") has informed this office FERPA does not permit state and local educational authorities to disclose to this office, without parental or student consent, unredacted, personally identifiable information contained in education records for the purpose of our review in the open records ruling process under the Act. The DOE has determined FERPA determinations must be made by the educational authority in possession of the education records. A copy of this letter may be found on the Office of the Attorney General's website: https://www.texasattorneygeneral.gov/files/og/20060725usdoe.pdf.

the Government Code.[3] We have considered the exception you claim and reviewed the submitted representative sample of information.[4] We have also received and considered comments submitted on behalf of the requestor. *See* Gov't Code § 552.304 (interested party may submit comments stating why information should or should not be released).

Section 552.139 of the Government Code provides, in relevant part:

> (a) Information is excepted from [required public disclosure] if it is information that relates to computer network security, to restricted information under Section 2059.055 [of the Government Code], or to the design, operation, or defense of a computer network.
>
> (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; [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.

Id. § 552.139(a), (b)(1)-(2), (4). You state the submitted information consists of a report generated by the district's digital surveillance system that reveals the words and subjects that are being monitored by the system and the number of instances they are flagged by the program. You explain that the district has engaged these services to protect the safety and security of district students and employees and the safety and security of the district's

[3] We note, and the district acknowledges, the district did not comply with section 552.301 of the Government Code in requesting a ruling from this office. *See* Gov't Code § 552.301(b), (e). Nonetheless, because section 552.139 can provide a compelling reason to overcome the presumption of openness, we will consider the applicability of this exception to the information at issue. *See id.* §§ 552.007, .302, .352.

[4] We assume the "representative sample" of records submitted to this office is truly representative of the requested records as a whole. *See* Open Records Decision Nos. 499 (1988), 497 (1988). This open records letter does not reach, and therefore does not authorize the withholding of, any other requested records to the extent those records contain substantially different types of information than that submitted to this office.

network by preventing computer security incidents. Based on these arguments and our review of the information, we agree the information you marked relates to computer network security, and the design, operation, or defense of the district's computer network. Accordingly, the district must withhold the information you marked under section 552.139 of the Government Code. The district must release the remaining information.

This letter ruling is limited to the particular information at issue in this request and limited to the facts as presented to us; therefore, this ruling must not be relied upon as a previous determination regarding any other information or any other circumstances.

This ruling triggers important deadlines regarding the rights and responsibilities of the governmental body and of the requestor. For more information concerning those rights and responsibilities, please visit our website at https://www.texasattorneygeneral.gov/open-government/members-public/what-expect-after-ruling-issued or call the OAG's Open Government Hotline, toll free, at (877) 673-6839. Questions concerning the allowable charges for providing public information under the Public Information Act may be directed to the Cost Rules Administrator of the OAG, toll free, at (888) 672-6787.

Sincerely,

Simone L. Nisbett
Assistant Attorney General
Open Records Division

SLN/tb

Ref: ID# 25-016471

c: Requestor

Third Party

EXHIBIT S

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.		

DECLARATION OF JENNIFER JONES

I, Jennifer Jones, being duly sworn, do hereby state as follows:

1. I am attorney with the Knight First Amendment Institute at Columbia University ("Knight Institute"), and I represent Plaintiff Knight Institute in the above-captioned action.

2. I am competent to make this declaration. The facts stated in this declaration are within my personal knowledge and are true and correct.

3. Attached as Exhibit A is a true and correct copy of the original public informatino request, sent by from Knight Institute to the Grapevine-Colleyville Independent School District ("District") pursuant to the Texas Public Information Act ("TPIA"), Tex. Gov't Code § 552, sent on March 29, 2023.

4. Attached as Exhibit B is a true and correct copy of the 15-day request for an Attorney General opinion sent by the District to the Attorney General on April 20, 2023.

5. Attached as Exhibit C is a true and correct copy of a letter sent by me, on behalf of the Knight Institute, to the District narrowing and clarifying the scope of the original request sent on June 2, 2023. This is referred to as "Clarified Request I."

6. Attached as Exhibit D is a true and correct copy of a list of search terms provided by the Knight Institute to the District on June 2, 2023, as an attachment to Clarified Request I, to assist with the District's search of responsive emails for that request.

7. Attached as Exhibit E is a true and correct copy of an email sent by me, on behalf of the Knight Institute, to the District on June 14, 2023, memorializing the terms of Clarified Request II, based on an agreement reached by both parties on the same day.

8. Attached as Exhibit F is a true and correct copy of a written Attorney General Informal Letter Ruling No. OR2023-2056 issued on June 16, 2023, corresponding to parts (a) and (b) of the Original Request.

9. Attached as Exhibit G is a true and correct copy of an email the District sent to the Knight Institute on June 21, 2023, discussing the volume of potentially responsive records, denying the Knight Institute's request for a fee waiver, and estimating charges to search and process the responsive records. This email was in response to an email I sent on June 14, 2023, included here as Exhibit E, but is also included as part of this email thread for context.

10. Attached as Exhibit H is a true and correct copy of a letter the District sent to the Attorney General requesting a ruling on part of Clarified Request II, on June 28, 2023.

11. Attached as Exhibit I is a true and correct copy of an email I sent on behalf of the Knight Institute to the District regarding the fee waiver request on June 30, 2023. The email thread includes previous emails sent by representatives of the District and I for context.

12. Attached as Exhibit J is a true and correct copy of Attorney General Letter Ruling No. OR2023-30020 issued on August 31, 2023, responding to the District's request for an opinion on a portion of Clarified Request II.

13. Attached as Exhibit K is a true and correct copy of an email from GCISD to the Knight Institute confirming its receipt of the Institute's payment and processing of 824 responsive emails on October 23, 2023.

14. Attached as Exhibit L is a true and correct copy of a letter from Knight Institute to the District requesting the continued processing and disclosure of the 824 responsive emails on November 7, 2023.

15. Attached as Exhibit M is a true and correct copy of an email from the District to the Knight Institute regarding redactions the District included in its responsive records, and its proactive claim of exceptions under the TPIA on November 14, 2023.

16. Attached as Exhibit N is a true and correct copy of an email from the Knight Institute to the District from November 16, 2023, objecting to the District's claim to withholdings and noting that requesting the Attorney General's opinion here would be untimely.

17. Attached as Exhibit O is a true and correct copy of correspondence from GCISD to the Knight Institute, sharing two redacted responsive emails on November 17, 2023.

18. Attached as Exhibit P is a true and correct copy of a letter sent by the District to the Attorney General on April 17, 2025, seeking retroactive authorization to withhold information from the 824 responsive emails.

19. Attached as Exhibit Q is a response letter issued by the Knight Institute to the Attorney General on May 27, 2025, regarding the District's request to seek retroactive and untimely authorization to withhold information from the responsive emails.

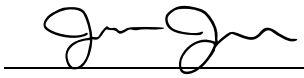
20. Attached as Exhibit R is a true and correct copy of Attorney General Letter Ruling No. OR2025-022099, issued on June 26, 2025, regarding the District's April 17 request.

21. Attached as an addendum to Exhibit T is a true and correct copy of an expert report from Bruce Schneier, submitted on behalf of the Knight Institute on October 31, 2025.

22. Attached as Exhibit U is a true and correct copy of an expert report from Kyle Berger, submitted on the behalf of the District on November 19, 2025.

23. My name is Jennifer Jones, my date of birth is December 27, 1985, and my address is 475 Riverside Drive Suite 302, New York, New York 10115, United States of America. I declare under penalty of perjury that the foregoing is true and correct.

Executed in Philadelphia County, State of Pennsylvania, on the 30th day of January of 2026.



Jennifer Jones

EXHIBIT T

Expert Report of Bruce Schneier

Name of Expert: Bruce Schneier
Area of Expertise: Computer Security
Representing: Plaintiff
Jurisdiction: Tarrant County, Texas

Knight First Amendment Institute at Columbia University v. Grapevine-Colleyville Independent School District
In the District Court for Tarrant County, Texas in the 348th Judicial District
Cause No. 348-362718-25

I. Introduction

Counsel for the Plaintiff in this action ("Counsel") retained me to provide my opinion about the meanings of "computer network security" and "computer security incident," and whether the public disclosure of information Plaintiff seeks in this action would threaten the security of Defendant's computer network.

I am an internationally renowned, award-winning computer security technologist and New York Times best-selling author of sixteen books covering the topic of computer security. As detailed in this report, professionals and scholars in my industry define computer network security as the protection of an organization's computer systems, networks, and data from cyberattacks and unauthorized access. A computer security incident occurs when an unauthorized individual attempts to, or succeeds in, gaining such access.

In reviewing the Plaintiff's request for public information, I have concluded that none of the information they seek would increase the threat of a security incident against Defendant's computer network if it were disclosed. I understand Plaintiff's request is a request for information about how Defendant monitors impermissible uses of its devices by authorized users. However, information that reveals what an organization deems to be an impermissible use of its computers would not in any way enable an external actor to access its computer network without authorization.

I am compensated at a flat rate of $2500 for drafting this expert report, and an hourly rate of $250 for any time spent preparing for and attending a deposition taken by Defendant (if any). My compensation does not depend upon the outcome of the case.

In preparing my report I have been given unrestricted access to all documents that I believe are relevant to my expert analysis and opinion. I have considered the documents identified herein, as well as those documents which are listed in Appendix 1.

II. Expertise

My name is Bruce Schneier. I hold an MS Degree in Computer Science, which I received from American University in 1986, and a BS Degree in Physics, which I obtained from the University of Rochester in 1984. In 2011, I received an honorary Ph.D. from the University of Westminster.

I have spent my entire career focused on issues relating to computer network security. I work internationally as a security technologist, and currently hold the titles of Partner at Alchemist Associates and Chief of Security Architecture at Inrupt, Inc. From 2016 until 2019, I held the titles of Chief Technology Officer of Resilient Systems, Inc., then Special Advisor to IBM Security. Prior to that, from 1999 until 2016, I was Chief Technology Officer of Counterpane Internet Security, Inc., and Chief Security Technology Officer of BT.

I am a Lecturer in Public Policy at the Harvard Kennedy School, where I teach cybersecurity policy. I also teach cybersecurity policy at the University of Toronto Munk School.

I am a fellow at the Berkman Klein Center for Internet and Society at Harvard University. I am a fellow at the Belfer Center for Science and International Affairs and the Ash Center for Democracy and Technology, which are both at the Harvard Kennedy School.

I serve as board member of the Electronic Frontier Foundation and Access Now. I have formerly been a board member of the Electronic Privacy Information Center and the Tor Project. I serve as an advisory board member for the Electronic Privacy Information Center and Verified Voting.org.

I am a *New York Times* best-selling author of fifteen books on the topics of cryptography, computer security, general security technology, trust, surveillance, and privacy, including *Applied Cryptography* (1994 and 1996), *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (2003), *Schneier on Security* (2008), *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (2018), and *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back* (2023). My latest book, *Rewiring Democracy: How AI Will Transform Our Politics, Government, and Citizenship* (with Nathan Sanders) was published by MIT Press in 2025.

I have also authored hundreds of articles, essays, and academic papers on security technology subjects, such as cryptographic design and analysis, security protocol design and analysis, software security, information security, internet security, security technologies, data privacy, data anonymity, AI security, security policy, privacy policy, cyberespionage, and cyberwarfare.

I have published numerous articles on the subject of security technology and its effects at personal, corporate, and national levels. I have also testified before Congress several times on these topics, and have served on several national and international committees.

I am the recipient of numerous awards, including: (1) being named one of the 20 top security influencers by *eSecurity Planet*, June 2015; (2) Electronic Privacy Information Center Lifetime

2

Achievement Award, June 2015; (3) being named one of the IFSEC 40: The Most Influential People in Security & Fire, January 2013; (4) CSO Compass Award, May 2010; (5) Computer Professionals for Social Responsibility (CPSR) Norbert Weiner Award, January 2008; (6) Electronic Frontier Foundation (EFF) Pioneer Award, March 2007; (7) Dr. Dobb's Journal Excellence in Programming Award, April 2006; (8) InfoWorld CTO 25 Award, April 2005; and (9) Productivity Award for Secrets and Lies in the 13th Annual Software Development Magazine Product Excellence Awards, 2000.

I publish a monthly email newsletter about security called Crypto-Gram, and a blog called "Schneier on Security," which together are read by more than 250,000 people.

Before being retained as an expert in this litigation, I was familiar with computer monitoring software generally but was unaware of the details of the issue in this litigation. Specifically, I was unaware of the Grapevine Colleyville Independent School District's ("the District") use of Gaggle and Lightspeed systems to block access to certain websites on its computer network, and to monitor certain words typed by individuals with access to the District's computer network. It was only through reviewing Plaintiff's public information request, Defendant's responses to that request, the pleadings in this litigation, and public reporting on Gaggle and Lightspeed that I understood how these particular computer software applications operate, and how school districts use them.

My CV is attached as Appendix 2 to this report. The last page of that CV lists declarations and depositions I have given as an expert witness in previous litigations.

III. Computer Network Security

i. Computer Network Security Has a Specific Meaning

I have been asked to give an opinion on the common understanding of the phrases "computer network security" and "computer security incident," as those phrases are used in my field.

In the cybersecurity industry, the term "computer network security" is used to refer to defenses of computers, servers, and other networked devices against unauthorized access.

By contrast, the term "computer network security" is not used to refer to defenses against unexpected or prohibited uses of access that was authorized. As an example, computer network security measures are designed to prevent hackers from breaking into a computer and stealing confidential data. Computer network security products and services do not, and cannot, prevent someone who is authorized to copy that data from doing so. Computer network security products and services do not prevent someone from doing something prohibited with that data after they copy it.

Both the ordinary meaning and industry understanding of the term "computer network security" are consistent with the Merriam Webster Dictionary definition of the word "cybersecurity,"

which refers to measures taken to protect a computer or computer system "against unauthorized access or attack."[1]

Relatedly, the term "computer security incident" refers to incidents where an unauthorized individual succeeds in gaining access to servers and other networked computers. In common parlance, we might call that kind of unauthorized access a "hack"[2] or a "breach."[3]

To provide context for this terminology, I'll begin by providing a general overview of what computer network security professionals actually do. The mandate of cybersecurity industry professionals is consistent with the computer network security definition I articulated above. Cybersecurity professionals like myself typically work to keep an organization's internal computer network safe and secure from threats such as cyber-attacks,[4] viruses,[5] malware,[6] phishing,[7] password attacks,[8] denial of service attacks,[9] ransomware,[10] and other intrusions by external actors. We do this either by preventing these attacks before they occur, or detecting them as quickly as possible as they are occurring.

These different attacks can be serious. Cybersecurity breaches pose significant consequences for organizations' computer networks and individual computer users. Viruses and other malware can harm or even destroy computers as well as digital devices like tablets and smartphones. Phishing and password attacks can deceive people into giving out their login information, and consequently give hackers access to sensitive financial, health, and work information. Denial of service attacks prevent legitimate users from accessing information systems, devices, and other network resources.

As a cybersecurity professional, I have always understood the goal of my work to be to defend computer networks from unauthorized *access*, not unauthorized *use* by someone with authorized access. To put it another way, I work to prevent bad actors from trespassing within,

---

[1] *See* Merriam-Webster, *cybersecurity*, https://perma.cc/5T36-N5EN.
[2] A hacker is an unauthorized user who attempts to or gains access to an information system. *See* NICCS, *Glossary*, https://perma.cc/8DAM-XJVR.
[3] A data breach is "the unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information." *See id.*
[4] "A cyber- attack is any unauthorized attempt to access, disrupt, steal, or damage computer systems, networks, or data." *See* Sans, *Glossary of Cyber Security Terms*, https://perma.cc/DLQ5-TQ7E.
[5] "A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active." *See id.*
[6] "A generic term for a number of different types of malicious code." *See id.*
[7] "The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with." *See id.*
[8] "Password cracking is the process of attempting to guess passwords, given the password file information." *See id.*
[9] "The prevention of authorized access to a system resource or the delaying of system operations and functions." *See id.*
[10] "A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again." *See id.*

4

communicating with, storing data in, retrieving data from, or otherwise intercepting and changing computer resources without the computer owner's or user's consent.

For example, in 1999 I founded Counterpane Internet Security. Inc. This was the world's first managed security monitoring company. We continuously monitored our customers' networks for signs of unauthorized intrusion, and worked to repel the attackers before they were able to damage the network or steal any data.

Generally, my work does not involve investigating or intercepting prohibited *uses* of computers, such as violations of an organization's terms of service or the improper use of data that was otherwise retrieved via authorized access.

ii. The Context of the Emergence of the Cybersecurity Industry Supports This Reading

In an effort to combat the new security threats posed by the widespread use of computers and the advent of the internet, anti-hacking laws started to be passed at the state and federal levels in the late 1980's. The federal Computer Fraud and Abuse Act ("CFAA"), which prohibits intentionally accessing a computer without authorization or in excess of authorization, was passed in 1986.[11] This federal law was soon followed by passage of anti-hacking laws in all fifty states, with most statutes similarly addressing unauthorized access or computer trespass.[12]

It was around this same time that the cybersecurity industry emerged to address the very threats that were contemplated by federal and state anti-hacking legislation. In 1987, the first commercial antivirus programs were released. [13]By the 1990's, the cybersecurity sector expanded to address the rapid growth of the internet.[14] New cybersecurity products were invented: firewalls,[15] intrusion detection systems,[16] authentication systems,[17] incident response systems,[18] and so on.

The Supreme Court's recent decision in *Van Buren v. United States*, 593 U.S. 374 (2021) reaffirmed the meaning and purpose of the federal CFAA by holding the statute cannot be used to enforce limitations on how or why an individual uses a computer.

---

[11] 18 U.S. Code § 1030.
[12] *Computer Crime Statutes*, NCSL (May 4, 2022), https://perma.cc/4BH8-JVJ6.
[13] Akhil Bhadwal, *The History of Cyber Security: A Detailed Guide [Updated]*, KnowledgeHut (May 22, 2025), https://perma.cc/WX3A-LZ4Y.
[14] *Id*.
[15] "A logical or physical discontinuity in a network to prevent unauthorized access to data or resources." *See* Sans, *Glossary of Cyber Security Terms*, https://perma.cc/DLQ5-TQ7E.
[16] "A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization)." *See id.*
[17] "Authentication is the process of confirming the correctness of the claimed identity." *See id.*
[18] "Incident response is the structured process of identifying, managing, and mitigating the effects of cybersecurity incidents to minimize damage, recover operations, and prevent future occurrences." *See id.*

5

My understanding of my role as a cybersecurity professional is consistent with this historical and legal context. That is, I work primarily to protect computer networks from unauthorized access by external actors. This is what I write about in my books, and this is what I do.

IV. The Information the Institute Seeks Does Not Implicate Computer Network Security

I understand from Counsel that Plaintiff seeks information about the specific websites the District has elected to block students from accessing, and the specific keywords the District monitors, purportedly for safety reasons.

From reviewing the pleadings, I also understand that the District contends that disclosure of this information would undermine the District's efforts to protect the security of its computer network and prevent computer security incidents.

In my opinion, this contention makes no sense and has no basis in fact. None of the information that Plaintiff has requested would pose a threat to the District's computer network. Disclosing the information, either to the Plaintiff or to the general public, would not increase the likelihood of a computer security incident.

To be more specific, none of the information that Plaintiff has requested, if disclosed to the public, would facilitate the harm or destruction of the District's computers and digital devices. Nor would disclosure of the information enable phishing and password attacks that can deceive people into giving out their login information, or prevent legitimate users from accessing information systems, devices, and other network resources.

For example, imagine that a school district installed Microsoft Word on its employees' computers. Experts in computer network security would be concerned with the question of whether Word had vulnerabilities in its design that could be exploited by outside actors to gain unauthorized access to the school district's computers. But they would not be concerned with the question of whether Word allowed its users to compose inappropriate messages, or whether Word properly flagged ungrammatical uses of language. A school district might very well care about those questions, but they would not be questions of *computer network security*.

If a school district publicly shared information about the specific network products they used, or the specific cloud services they used, or the specific security products and services they used and their configurations, that would potentially implicate the security of the District's computer network. But based on my review of the pleadings, no such information has been requested here.

V. Conclusion

My extensive experience in the field of computer security and the facts presented in this case lead me to conclude that the public disclosure of the information sought by Plaintiff would pose no threat to the security of Defendant's computer network.

APPENDIX 1

FILED
TARRANT COUNTY
9/23/2025 4:57 PM
THOMAS A. WILDER
DISTRICT CLERK

Cause No. 348-362718-25

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

PLAINTIFF'S AMENDED PETITION AND REQUEST FOR WRIT OF MANDAMUS

Plaintiff Knight First Amendment Institute at Columbia University (the "Knight Institute") files this original petition against Grapevine-Colleyville Independent School District ("GCISD" or the "District"), to remedy violations of the Texas Public Information Act ("TPIA"), Texas Government Code Chapter 552, and will show:

STATEMENT OF CLAIM

1. On March 29, 2023, the Knight Institute submitted a request for records under the TPIA to the Grapevine-Colleyville Independent School District. The Knight Institute's request sought records related to the District's use of surveillance systems to monitor students' school-issued devices and software. The District refuses to produce this information, claiming that the requested records are excepted from disclosure under the TPIA. Accordingly, the Knight Institute seeks a writ of mandamus and attorneys' fees and costs to vindicate its right to receive the public information that GCISD has failed to disclose. Specifically, the Knight Institute seeks the information sought in its Original Request, or alternatively, in its Clarified Request I or Clarified Request II.

DISCOVERY CONTROL PLAN

2. Discovery in this matter will proceed under Level 2. *See* Tex. R. Civ. P. 190.3.

JURISDICTION AND VENUE

3. This Court has jurisdiction under Texas Government Code Section 552.321(a)–(b), which authorizes "a writ of mandamus compelling a governmental body to make information available for public inspection if the governmental body . . . refuses to supply public information." Tex. Gov't Code § 552.321(a)–(b).

4. GCISD's main offices are in Tarrant County, Texas. Venue in this case is proper because this petition was "filed in a district court for the county in which the main offices of the governmental body are located." Tex. Gov't Code § 552.321(b).

PARTIES

5. Plaintiff Knight Institute at Columbia University is a not-for-profit corporation based at Columbia University in New York, New York. The Knight Institute defends the freedoms of speech and the press in the digital age through strategic litigation, research, policy advocacy, and public education, and aims to promote a system of free expression that fosters effective self-government. Defending and promoting the public's right to access information is a core part of this mission.

6. Defendant Grapevine-Colleyville Independent School District ("GCISD") is an entity of the State of Texas and a "governmental body" for purposes of the Act. *See* Tex. Gov't Code § 552.003(1). GCISD maintains an office at 3051 Ira E. Woods Avenue, Grapevine, TX 76051.

TEXAS PUBLIC INFORMATION ACT

7. The Texas Public Information Act reflects the state's policy "that each person is entitled . . . at all times to complete information about the affairs of government and the official acts of public officials and employees." Tex. Gov't Code § 552.001(a). Accordingly, the Act's disclosure mandates should "be liberally construed in favor of granting a request for information,"

id. § 552.001(b), and exemptions to public disclosure "should be construed narrowly." *Arlington Indep. Sch. Dist. v. Tex. Att'y Gen.*, 37 S.W.3d 152, 157 (Tex. App.—Austin 2001, no pet.).

8. The TPIA broadly defines "public information" as information that is "written, produced, collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business." Tex. Gov't Code § 552.002(a). That information must be maintained: (1) "by a governmental body;" (2) "for a governmental body" that "owns the information; has a right of access to the information; or spends or contributes public money for the purpose of writing, producing, collecting, assembling, or maintaining the information;" or (3) "by an individual officer or employee of a governmental body in the officer's or employee's official capacity and the information pertains to official business of the governmental body." *Id.* § 552.002(a)(1)–(3). The statute further clarifies that information is "in connection with the transaction of official business" if it is "created by, transmitted to, received by, or maintained by an officer or employee of the governmental body in the officer's or employee's official capacity, or a person or entity performing official business or a governmental function on behalf of a governmental body, and pertains to official business of the governmental body." *Id.* § 552.002(a-1).

9. Among the types of information singled out by the Act for presumptive disclosure, "contracting information is public and must be released," unless it is excepted from disclosure under some other identifiable provision of the Act. *Id.* § 552.0222(a). Relevant here, the Act defines "[c]ontracting information" to include "communications and other information sent between a governmental body and a vendor or contractor related to the performance of a final contract with the governmental body or work performed on behalf of the governmental body." *Id.* § 552.003(1-a)(E).

10. Once a requester submits a request for information, a governmental body "shall promptly produce public information for inspection, duplication, or both." *Id.* § 552.221(a). Under the statute, "promptly" means within ten business days after the date of the request or "as soon as possible under the circumstances, that is, within a reasonable time, without delay." *Id.*

11. If a governmental body wants to withhold public information under a statutory exception, it must inform the requestor of its intent to do so and ask for the Attorney General's opinion within a reasonable time, but no later than ten business days after receiving the request. Tex. Gov't Code § 552.301(b),(d)(1)–(2). Within fifteen business days, the governmental body must submit to the Attorney General: the written request and evidence of the date it was received; a copy or representative sample(s) of the information requested; and written comments explaining why the stated exceptions apply. *Id.* at § 552.301(e)(1)(A)–(D).

12. The Attorney General must then "promptly render a decision" within 45 days that determines whether the requested information falls within one of the statute's exceptions. *Id.* § 552.306(a). If the Attorney General is unable to render its decision within 45 days, it may extend the deadline an additional ten business days by informing the governmental body and the requestor of the reason for the delay. *Id*. "[T]he [A]ttorney [G]eneral shall issue a written opinion of the determination and shall provide a copy of the opinion to the requestor." *Id.* § 552.306(b).

13. If a governmental body fails to make a timely request for an Attorney General opinion as provided by Subchapter G, the requested information is "presumed to be subject to required public disclosure and must be released unless there is a compelling reason to withhold the information." *Id.* § 552.302. If the governmental body refuses to supply the information, the requestor may "file suit for a writ of mandamus compelling [the] governmental body to make information available for public inspection . . . ." *Id.* § 552.321(a).

14. Finally, the requestor may "file suit for a writ of mandamus compelling [the] governmental body to make information available for public inspection" if the Attorney General has found that the information sought is not public record. *Id*.; *see also Tex. Dep't of Pub. Safety v. Gilbreath*, 842 S.W.2d 408, 411 (Tex. App.—Austin 1992, no pet.) ("The fact that the attorney general determined . . . information was not a public record [does] not preclude [the requestor] from seeking a trial court's determination as to whether the information sought was public information . . . .").

STATEMENT OF FACTS

I. The Knight Institute's Interest in the District's Records

15. The Knight Institute is a not-for-profit organization that aims to promote a system of free expression that fosters effective self-government. Defending and promoting the public's right to access information is a core part of this mission. The Knight Institute regularly relies on public records laws and the First Amendment to obtain information about government activity, and disseminates that information to the press and public through its website, social media accounts, press releases, blog posts, op-eds, and regular engagement with the press.

16. Relevant here, the Knight Institute's public records work has illuminated the scope and impact of surveillance by government and private corporations, enriching the public's understanding of the interplay between privacy and the freedoms of inquiry, speech, and association. Some of the Knight Institute's recent work has shed light on the digitization, retention, and surveillance of mail sent to people incarcerated in federal jails and prisons, and federal agencies' use of social media surveillance to conduct ideological screening of immigrants and visitors at the border. *See Knight Institute Seeks Federal Bureau of Prisons' Records Concerning Surveillance of Incarcerated People's Mail*, Knight First Amend. Inst. at Columbia Univ. (Aug. 4, 2021), https://perma.cc/Y2GB-PL6M; *Knight Institute v. DHS: A FOIA Lawsuit Seeking Records*

on Ideological Screening at the Border, Knight First Amend. Inst. at Columbia Univ. (last visited Dec. 17, 2024), https://perma.cc/Q26X-RYGC.

II. Use of A.I.-Powered Surveillance in Schools

17. As part of its ongoing work on free speech and surveillance, the Knight Institute seeks to learn more about how schools use A.I.-powered technology to restrict and monitor students' activity on school-issued devices and applications. Ellen Barry, *Spying on Student Devices, Schools Aim to Intercept Self-Harm Before It Happens*, The N.Y. Times (Dec. 11, 2024), https://perma.cc/ZDD7-GTSL. These systems, operated by private surveillance companies like GoGuardian, Gaggle, and Lightspeed, use artificial intelligence to scan student emails, documents, chats, and more against a list of keywords or phrases. Any content that suggests a student is engaging in behavior that poses a threat to themselves or others is flagged by the technology and reviewed by human content moderators, who then alert school administrators or law enforcement. *Id.* While the technology companies that offer these products use a standard list of keywords and phrases that will generate a flag, school administrators also have the ability to customize this list. Mark Keierleber, *Gaggle Surveils Millions of Kids in the Name of Safety. Targeted Families Argue it's 'Not That Smart'*, The 74 (Oct. 12, 2021), https://perma.cc/Q94H-T6TG.

18. There is widespread concern that school districts' use of these technologies causes serious privacy, expressive, associational, and equity harms. A recent report by the Center for Democracy & Technology found that the use of technology to screen or restrict access to certain material through content blocking and filtering stifles student learning and growth, making it difficult to complete school assignments and access information. CDT Report, *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI*, Ctr. for Democracy & Tech. (Sept. 2023), https://perma.cc/3QNP-6EVR. For example, students have been flagged by surveillance software for innocuous web searches related to the text of Genesis from Bible.com, classic literature like

Romeo and Juliet, and articles about Martin Luther King Jr. and the Civil Rights Movement. Dave Maass, Daly Barnett & Jason Kelley, *GoGuardian: A Red Flag Machine By Design*, Red Flag Mach. (last visited Mar. 7, 2025), https://perma.cc/Q966-5LU8. In other instances, monitoring of student activity has led to the disclosure of private information about students—including information about their sexuality. CDT Report, *supra* at 28.

19. The ability of school districts to customize lists of keywords and phrases they deem inappropriate—and keep those lists hidden from public view—has intensified these concerns. CDT's report on online surveillance found that some schools block, filter, or monitor LGBTQ+ and race-related content. *Id.* In another instance, in 2024, several high school journalism students convinced their Lawrence, Kansas school administrators to remove the journalism students' files from the purview of Gaggle's surveillance system based on the concern that the technology could invade the privacy of their reporting, which is sometimes critical of district staff and administration. Cuyler Dunn, *Lawrence Journalism Students Convince District to Reverse Course on AI Surveillance They Say Violates Freedom of Press*, The Lawrence Times (Apr. 18, 2024), https://perma.cc/J8PZ-N7J8.

III. The Knight Institute's Request, the District's Response, and the Attorney General's Rulings

i. Original Request

20. On March 29, 2023, the Knight Institute submitted a TPIA request to the Grapevine-Colleyville Independent School District for records related to the District's use of surveillance systems to monitor students' activity on school-issued devices and software, including:

a. Any information identifying the words or phrases the District has included, or plans to include, in its list(s) of blocked or monitored words;

b. Any information identifying the websites the District has included, or plans to include, in its list(s) of blocked or filtered websites;

c. Any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications between District employees, and communications between the District and the company supplying the District's digital surveillance system.

The Knight Institute also requested a fee waiver, which the Act permits "if a governmental body determines" that producing the information requested "is in the public interest" because it will "primarily benefit[] the general public." Tex. Gov't Code § 552.267(a). The request is attached hereto as **Exhibit A** (the "Original Request").

21. GCISD acknowledged receipt of the Original Request on April 5, 2023, and notified the Knight Institute that it intended to request an opinion of the Attorney General because it had determined that "some or all of [the] request is likely to fit within an exception to disclosure under Texas Government Code Section 552.139." GCISD also asked the Knight Institute to clarify the scope of part (c) of the Original Request, and to provide the District with search terms for part (c). GCISD's April 5, 2023 correspondence is attached hereto as **Exhibit B.**

22. On April 13, 2023, GCISD, through outside counsel, submitted a 10-day request to the Attorney General for a decision as to whether information responsive to parts (a) and (b) the Original Request is excepted from disclosure under Texas Government Code § 552.139, referred to here as the "computer network security exception."[1] Under this provision, information is excepted from the requirements of the TPIA if it "relates to computer network security, to

[1] In its April 13 10-day AG request, the District did not seek a decision as to whether information responsive to part (c) of the Original Request was excepted from disclosure because at the time it had asked the Knight Institute to clarify the scope of the request and develop a list of relevant search terms.

restricted information under Section 2059.055, or to the design, operation, or defense of a computer network." Tex. Gov't Code § 552.139(a).[2] GCISD's 10-day request for an Attorney General decision is attached hereto as **Exhibit C** ("April 13 10-day AG Request").

23. On April 20, 2023, GCISD submitted a 15-day request to the Attorney General for a decision as to whether information responsive to parts (a) and (b) of the Original Request is excepted from disclosure under TPIA's "computer network security exception." Specifically, GCISD claimed that the District has chosen to block or filter certain words and websites from its network "for the purpose of protecting the safety and security of District employees and students, as well as to protect the safety and security of the District's network by preventing computer security incidents." Those words and websites were chosen, GCISD claimed, "because of their propensity to expose the District's computers and network to malicious sites and other risks." For these reasons, GCISD concluded that the request sought "information directly arising from the [District's] routine efforts to prevent . . . a computer security incident," and is therefore excepted from disclosure under § 552.139(b)(4). GCISD's 15-day request for an Attorney General decision is attached hereto as **Exhibit D** ("April 20 15-day AG Request")

ii. Clarified Request I

24. On June 2, 2023, the Knight Institute submitted to GCISD a clarification of the Original Request, which narrowed the scope of the entire request to information related to the monitoring

[2] Under the statute, 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(b).

and filtering of LGBTQ+ and race-related content. In response to GCISD's request in its April 5, 2023, acknowledgement letter (*see* **Exhibit B**), the Knight Institute also clarified the scope of part (c) by: (1) stating its intent for the District to search every employee's email correspondence since January 1, 2020 and (2) providing a list of search terms for the District to use in that search. The Knight Institute also asked the District to confirm the name(s) of each vendor that it contracts with, or has previously contracted with, to provide online filtering and monitoring services. The clarified request is attached hereto as **Exhibit E** ("Clarified Request I"), while the list of search terms for part (c) is attached hereto as **Exhibit F** ("Search Terms").

25. On June 8, 2023, GCISD informed the Knight Institute that an initial search of the email correspondence requested in part (c) of Clarified Request I, using the Knight Institute's list of search terms, yielded over 2.4 million emails. GCISD estimated that it would cost $1.8 million to process them. GCISD's June 8, 2023 email is attached hereto as **Exhibit G** ("June 8 GCISD Correspondence"). GCISD also confirmed that it uses two systems to monitor students' digital activities: Lightspeed Systems and Gaggle.

iii. Clarified Request II

26. On June 14, 2023, the Knight Institute's counsel met with GCISD's counsel to discuss how the request for information responsive to part (c) of Clarified Request I could be further narrowed. That same the day, the Knight Institute memorialized the conversation in an email, requesting that the District (1) prioritize the production of analytics reports concerning the types of content the District's monitoring software has flagged; and (2) limit the email search results to: (a) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and (b) emails that include the terms "lightspeed" and "gaggle." The Knight Institute's email memorializing the June 14, 2023, discussion is hereto attached as **Exhibit H** ("Clarified Request II").

27. On June 16, 2023, the Attorney General issued Letter Ruling No. OR2023-20568 in response to the District's April 20 15-day Request regarding parts (a) and (b) of the Original Request, attached hereto as **Exhibit I** ("Attorney General Informal Letter Ruling on Original Request"). In the letter, the Attorney General determined that all but two of the requested records were excepted from disclosure under the Act's computer network security exception because they "relate[] to computer network security, and the design, operation, or defense of the district's computer network." *See* **Exhibit I**. The Attorney General's letter specified that the ruling was "limited to the particular information at issue in this request" and "must not be relied upon as a previous determination regarding any other information or any other circumstances."

28. On June 21, 2023, GCISD's counsel notified the Knight Institute that its search for information responsive to the second part of Clarified Request II yielded 824 potentially responsive emails. GCISD denied the Knight Institute's Initial Request for a fee waiver and estimated that it would cost $741.60 to process the records. GCISD noted that it was waiting for the Knight Institute to confirm that it accepted GCISD's estimated charges for the records responsive to Clarified Request II. GCISD also stated that it identified reports associated with Lightspeed and Gaggle in its search, but asserted that those reports are excepted from disclosure, and that it would seek an opinion from the Attorney General regarding the withholding of those reports. GCISD's June 21, 2023, email to the Knight Institute is attached hereto as **Exhibit J** ("June 21 GCISD Correspondence").

29. On June 28, 2023, GCISD submitted a request[3] for an Attorney General ruling that the first part of Clarified Request II was likewise excepted from disclosure under the computer network

[3] The District's request characterizes the first part of Clarified Request II as only requesting reports from Gaggle and Lightspeed Systems, which provide data to District personnel regarding flagged content. (*See* June 28 AG request). The Knight Institute, however, merely requested that the District *prioritize* this information in its search—not limit its search to these records. The Knight Institute is still entitled to all requested records.

security exception. GCISD's letter to the Attorney General is attached hereto as **Exhibit K** ("June 28 AG Request"). It argued that reports identifying words or subjects monitored by Gaggle and Lightspeed Systems are "'information directly arising from the [District's] routine efforts to prevent . . . a computer security incident.' Tex. Gov't Code § 552.139(b)(4)," and that "public disclosure of such words, website addresses, and other related information may expose the District to unnecessary security threats."

30. Notably, GCISD's June 28 AG Request did not seek a ruling with respect to the second part of Clarified Request II. GCISD's request for a ruling explicitly stated that, because it had not yet received a response from the Knight Institute regarding the cost estimate for responding to the second part of Clarified Request II, it "reserve[d] the right to seek a ruling from the Attorney General with respect to the information responsive to the second part of the Clarified Request should the requestor timely indicate that she intends to move forward with this portion of the request." *See* **Exhibit K, FN** 4.

31. On June 30, 2023, the Knight Institute asked GCISD to reconsider its decision to deny the Knight Institute's request for a fee waiver. On July 7, 2023, GCISD responded that it would continue to deny the Knight Institute's request for a fee waiver. On July 13, 2023, the Knight Institute confirmed that it planned to move forward with part (c) of the request and agreed to pay the estimated fees. The aforementioned exchange between GCISD and the Knight Institute is attached hereto as **Exhibit L** ("June 30 Fee Waiver Request").

32. Despite the Knight Institute's confirmation of its intent to move forward with the second part of Clarified Request II, the District did not then request an Attorney General ruling on the application of any disclosure exception to the second part of Clarified Request II.

33. On August 31, 2023, the Attorney General issued Letter Ruling No. OR2023-30020 in response to the District's June 28 Request regarding the first part of Clarified Request II, attached hereto as **Exhibit M** ("Attorney General Ruling, Clarified Request II"). In its ruling, the Attorney General determined that the requested information was excepted from disclosure under the TPIA's computer network security exception. *See* Tex. Gov't Code § 552.139. Again, the Attorney General's letter specified that the ruling was "limited to the particular information at issue in this request" and that the "ruling must not be relied upon as a previous determination regarding any other information or any other circumstances."

34. The Knight Institute mailed a check payment to GCISD for its processing of information responsive to the second part of Clarified Request II on September 28, 2023. On October 23, 2023, GCISD informed the Knight Institute that it had received the Knight Institute's payment and began processing the 824 responsive emails. GCISD's correspondence is attached hereto as **Exhibit N** ("October 23 Redaction Letter"). However, GCISD claimed that "almost all emails contain the very information the Texas Attorney General agreed must be withheld[,] . . . [including] information about subjects being searched, keywords being monitored, threat types, and why the communication was flagged for review by District personnel." Because that information would be redacted, GCISD claimed, the records would provide "very little information" to the Knight Institute. GCISD therefore offered to refund the Knight Institute's payment for the responsive information and close the request. If the Knight Institute did not close the request, GCISD indicated it would seek another opinion from the Attorney General regarding the second part of Clarified Request II.

35. On November 7, 2023, the Knight Institute sent a letter to GCISD requesting that it continue to process the 824 emails responsive to the second part of Clarified Request II. The letter

is attached hereto as **Exhibit O** ("November 7 KFAI Letter to GCISD re redactions"). The Knight Institute notified GCISD that a request for an Attorney General opinion regarding the second part of Clarified Request II would be untimely, as the TPIA requires that an agency request an opinion within ten business days of receiving a request or clarification of a request. *See* Tex. Gov't Code § 552.301(b). The Knight Institute had confirmed its intent to move forward with the second part of Clarified Request II on July 13, 2023. *See* **Exhibit L**.

36. On November 14, 2023, GCISD responded that it would continue to process the emails, but would redact them in accordance with "the Attorney General's ruling that certain information should be withheld as it relates to computer network security, and the design, operation, or defense of the District's computer network." GCISD's response is attached hereto as **Exhibit P** ("November 14 GCISD response re email redactions"). GCISD did not indicate which prior Attorney General ruling it purported to rely on, or why it believed it did not need to seek a new Attorney General opinion.

37. On November 16, 2023, the Knight Institute objected to GCISD's reliance on the previous Attorney General opinion(s) to redact the responsive emails, as both opinions made clear that the rulings were "limited to the particular information" presented for review and "must not be relied upon as a previous determination regarding any other information or any other circumstances." The Knight Institute's objection is attached hereto as **Exhibit Q** ("November 16 objection to email redactions"). GCISD's counsel never responded to this objection.

38. On November 17, 2023, GCISD disclosed the 824 responsive emails via its online public records portal. GCISD redacted virtually all information relevant to the second part of Clarified

Request II, including keywords and phrases that the District monitors.[4] Representative responsive emails disclosed by GCISD are attached hereto as **Exhibit R.**

39. Seventeen months later, on April 17, 2025, after the Knight Institute filed this lawsuit, GCISD sought an Attorney General opinion giving it retroactive authorization to withhold the public records requested in the second part of Clarified Request II. In its Request Letter, GCISD acknowledged that it should have sought an Attorney General opinion at the time the Knight Institute paid the fee to process the requested records. GCISD's Request Letter is attached hereto as **Exhibit S**.

40. To overcome the TPIA's presumption that the governmental body's failure to request a timely opinion requires public disclosure of the information, GCISD argued that the computer network security exception serves as a "compelling reason" to withhold the requested information because the it is "information directly arising from the [District's] routine efforts to prevent . . . a computer security incident." *See* **Exhibit S** (the request letter) (citing Tex. Gov't Code § 552.139(b)(4)).

41. In its response dated May 27, 2025, the Knight Institute asserted that GCISD failed to meet its burden to overcome the presumption of public disclosure. The Institute noted that GCISD improperly relied on the August 31, 2023 opinion, which pertained to materially different records, to withhold the information sought in the second part of Clarified Request II. Additionally, the Knight Institute argued that GCISD's year-and-a-half delay in seeking an Attorney General opinion demonstrates the continued withholding of the information is not "of such a pressing nature . . . that it outweighs the interests favoring public access[.]" The Knight Institute's Response Letter is attached hereto as **Exhibit T**. The Knight Institute maintained that the computer network security

[4] In some of the responsive emails disclosed by GCISD the relevant information was not fully redacted by the District. On information and belief, those emails were disclosed inadvertently. *See, e.g.*, **Exhibit R**, 1, 3.

exception does not *per se* constitute a compelling reason to withhold records to which a presumption of public disclosure has attached; nor should the exception be treated as compelling as applied to these records—particluarly in light of GCISD's admitted inaction in seeking to protect the records upon notice of the Knight Institute's interest in them nearly two years ago.

42. On June 26, 2025, the Attorney General issued Letter Ruling No. OR2025-022099, determining that the information designated as exempt from disclosure under § 552.139 served as a compelling reason to overcome the presumption of public disclosure, that the responsive records related to computer network security, and that the records could therefore be withheld. The Attorney General's Letter Ruling is attached hereto as **Exhibit U**.

ARGUMENT

43. GCISD's failure to disclose the information sought in the Knight Institute's Original Request and in Clarified Request II unlawfully deprives the Knight Institute of its right to that information. The information requested by the Knight Institute is public information and should be released because: (1) information pertaining to keywords and websites GCISD has blocked or monitored was produced in connection with official business; and (2) none of the information is excepted from disclosure under the computer network security exception.

44. The information requested in the Original and Clarified Requests is public information under the TPIA. *See* Tex. Gov't Code § 552.002(a). "Public information" is defined as "information that is written, produced, collected, assembled, or maintained . . . in connection with the transaction of official business" by or for a governmental body. *Id.* The requested information—information related to the words and websites GCISD blocks or monitors—was produced in the course of GCISD's official business operating school-issued devices and software.

45. The information requested is also "contracting information," because it involves "communications and other information sent between a governmental body and a vendor or

contractor related to the performance of a final contract with the governmental body or work performed on behalf of the governmental body." Tex. Gov't Code § 552.003(1-a)(E). The information requested is therefore entitled to a presumption of public release, "unless excepted from disclosure" under the Act. Tex. Gov't Code § 552.0222(a). The Knight Institute requested information pertaining to the performance of the contract between GCISD and their third party vendors—the key words the District directed its vendor to use to block, filter, or monitor content on school issued devices. These keywords represent the instructions and guidelines established by GCISD for their vendor to follow when providing the services outlined in their agreements. They establish a direct link between the requested records and the essential functions being carried out under the contract.

46. The information requested in the Original and Clarified Requests is not excepted from disclosure under the computer network security exception. *See* Tex. Gov't Code § 552.139. The District's disclosure of words and websites it monitors or blocks would not reveal information related to "computer network security" or the "design, operation, or defense of a computer network." *See id.* § 552.139(a). Nor would the disclosure of that information expose GCISD's network to a "computer security incident." *See id.* § 552.139(b)(4) (limiting confidential information to that which "directly "aris[es]" from "routine efforts" to address a "computer security incident"). GCISD has offered no basis for its claim that disclosing information related to the lists of words and websites it monitors or blocks would expose it to security threats.

47. Moreover, the information requested in the second part of Clarified Request II is presumptively public because GCISD did not timely request an opinion from the Attorney General that a TPIA exception applies to that information. *See* Tex. Gov't Code § 552.302 (providing that "information requested in writing is presumed to be subject to required public disclosure" if the

governmental body does not timely seek an Attorney General ruling); *Paxton v. City of Dall.*, 509 S.W.3d 247, 252 (Tex. 2017) ("if a request for decision is untimely, 'the information requested in writing is presumed to be subject to required public disclosure and must be released *unless there is a compelling reason to withhold the information.*'"). The Act requires that a governmental body seeking to withhold information request an Attorney General ruling within ten business days of receiving a request, or a clarification of a request. *See* Tex. Gov't Code § 552.301(b); *see also City of Dall. v. Abbott*, 304 S.W.3d 380, 387 (Tex. 2010) (holding that the ten-day period to request an attorney general ruling is measured from the date the request is clarified or narrowed when a governmental entity requests clarification or narrowing of an unclear or overbroad request for information). The Knight Institute confirmed its intent to move forward with the second part of Clarified Request II on July 13, 2023. Almost two years later and only after the filing of this lawsuit, GCISD finally requested an opinion from the Attorney General that a TPIA exception applies to the information requested in the second part of Clarified Request II on April 17, 2025.

48. The computer network security exception is neither a compelling justification *per se*, nor is it a compelling justification as applied to the records sought here. *See Paxton*, 509 S.W.3d at 259 ("[A] reason to withhold information will be 'compelling' only when it is of such a pressing nature (e.g., urgent, forceful, or demanding) that it outweighs the interests favoring public access to the information and overcomes section 552.302's presumption that disclosure is required."). *Compare* Tex. Gov't Code § 552.139(a) (allowing discretionary disclosure of responsive information) *with id.* § 552.139(b) (making certain categories of information confidential by law). GCISD cannot meet its burden to establish that it has a compelling reason to withhold the responsive records, and for that reason, the records responsive to Clarified Request II are subject to required public disclosure.

49. Finally, the Knight Institute is entitled to a fee waiver. The TPIA allows fees to be waived or reduced if the governmental body determines that providing a copy of the information primarily benefits the general public. Tex. Gov. Code § 552.267(a). Disclosure of the information sought here would primarily benefit the public interest, as it would inform the public about actual or alleged government activity. Moreover, disclosure would not further the Knight Institute's commercial interest. As indicated in our request, the Knight First Amendment Institute is a New York not-for-profit corporation based at Columbia University that works to preserve and expand the freedoms of speech and the press through strategic litigation, research, and public education. The Knight Institute will make any information disclosed available to the public at no cost. GCISD has offered no basis for its denial of the Knight Institute's fee waiver request, stating only that "the District does not determine that the standard in Tex. Gov't Code § 552.267(a) is met in this instance, and, therefore, will not waive or reduce the charges associated with the [] Institute's request." *See* **Exhibit L**.

PETITION FOR WRIT OF MANDAMUS

50. The Grapevine-Colleyville Independent School District is withholding information responsive to the Knight Institute's request in violation of the TPIA.

51. Pursuant to Section 552.321(a) of the TPIA, the Knight Institute is entitled to a writ of mandamus compelling the Grapevine-Colleyville Independent School District to disclose all responsive information.

ATTORNEY'S FEES

52. The Knight Institute requests all reasonable and necessary attorney's fees resulting from this litigation, pursuant to Tex. Gov't Code § 552.323.

PRAYER

53. Wherefore, Premises Considered, Plaintiff Knight First Amendment Institute at Columbia University respectfully prays the Court, upon final hearing:

A. Enter a writ of mandamus requiring GCISD to produce to the Knight Institute the requested information in the Original Request.

B. Alternatively, enter a writ of mandamus requiring GCISD to produce to the Knight Institute the requested information in Clarified Request I.

C. Alternatively, enter a writ of mandamus requiring GCISD to produce to the Knight Institute the requested information in Clarified Request II.

D. Order that the Knight Institute is entitled to a fee waiver for its Request, and that GCISD reimburse the Knight Institute for its previous payment for public information.

E. Order that GCISD reimburse the Knight Institute for the reasonable and necessary attorney's fees resulting from this litigation.

F. Order all such further relief to which the Knight Institute is justly entitled.

September 23, 2025

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*
Katie Fallow*
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

EXHIBIT A

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
info@knightcolumbia.org

March 29, 2023

Grapevine-Colleyville Independent School
District
Public Information Request
3051 Ira E. Woods Avenue
Grapevine, Texas 76051

Re: Texas Public Information Act Request

To whom it may concern,

This letter constitutes a request pursuant to the Texas Public Information Act ("TPIA"), Texas Government Code Ch. 552, for information related to the Grapevine-Colleyville Independent School District's ("District") use of surveillance systems to monitor students' activity on digital devices and accounts. This request is made for public and non-commercial purposes by the Knight First Amendment Institute at Columbia University ("Knight Institute" or "Institute").[1]

I. Background

As students across the country transitioned to remote learning in response to the COVID-19 pandemic, school administrators increasingly turned to surveillance companies to assist with monitoring students' activity on digital devices and school-issued Google and Microsoft accounts.[2] One of the most prevalent tools marketed by these companies is spy tech that uses artificial intelligence to track all student activity and communications on their digital devices and accounts. In practice,

[1] The Knight First Amendment Institute is a New York not-for-profit corporation based at Columbia University that works to preserve and expand the freedoms of speech and the press through strategic litigation, research, and public education.

[2] Mark Keierleber, *The spy tech that followed kids home for remote learning—and won't leave*, Fast Company (Sept. 20, 2021), https://www.fastcompany.com/90677509/the-spy-tech-that-followed-kids-home-for-remote-learning-and-wont-leave.

these systems typically work by restricting students' access to specific websites and/or applications, while scanning student emails, documents, chats, and more against a list of monitored words and phrases.[3] Any content that may indicate a student is engaging in "inappropriate behaviors" or poses "potential threats to self or others," including profanity, references to self-harm, violence, bullying, or drugs, is flagged by the tool and reviewed by human content moderators, who can pass the material to school administrators or law enforcement to take further action.[4] While surveillance companies typically have a standard list of keywords that will generate a flag, school administrators have the ability to customize this list to reflect local contexts.[5]

Surveillance companies claim that these systems protect student safety, but students, parents, and others have raised concerns that they actually cause serious harm, posing significant threats to students' privacy and free speech rights and contributing to a long legacy of policing and surveillance in public schools.[6] To learn more about how these systems are being deployed, this request seeks records related to the list of words, phrases, and websites that the District filters and/or monitors as part of its surveillance of students' digital activities.

II. Information requested

The Knight Institute requests the following information[7] related to the Grapevine-Colleyville Independent School District's use of surveillance systems to monitor student activity on digital devices and accounts, created on or after January 1, 2020:

a. Any information identifying the words or phrases the District has included, or plans to include, in its list(s) of blocked or monitored words;[8]

---

[3] Caroline Haskins, *Gaggle Knows Everything About Teens And Kids In School*, Buzzfeed News (Nov. 1, 2019, 3:48pm), https://perma.cc/7269-VTFS.

[4] *Id.*; Mark Keierleber, *Minneapolis Schools to Halt Controversial Student Surveillance Initiative*, The 74 (June 27, 2022), https://perma.cc/S6TA-6696.

[5] Mark Keierleber, *Gaggle Surveils Millions of Kids in the Name of Safety. Targeted Families Argue it's 'Not That Smart'*, The 74 (Oct. 12, 2021), https://perma.cc/Q94H-T6TG.

[6] Keierleber, *supra* note 4.

[7] For purposes of this request, "information" includes but is not limited to all records or communications preserved in written or electronic form, including but not limited to: correspondence, documents, data, videotapes, audio tapes, emails, faxes, files, guidance, guidelines, evaluations, instructions, analyses, memoranda, agreements, notes, orders, policies, procedures, protocols, reports, rules, training manuals, other manuals, or studies.

[8] For purposes of this request, "list of blocked or monitored words" means any specific word or phrase that may trigger an alert, flag, block, restriction,

b. Any information identifying the websites the District has included, or plans to include, in its list(s) of blocked or filtered websites;[9]

c. Any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications between District employees, and communications between the District and the company supplying the District's digital surveillance system.

III. Request for waiver or limitation of fees

The Knight Institute requests that you produce the information free of charge on the grounds that this request is made for public and non-commercial purposes and will benefit the general public. Tex. Gov't Code § 552.267. However, if you are unable to do so, the Institute will reimburse you for the reasonable costs associated with fulfilling this request if your office has a policy of requiring the payment of a copying charge for such information. **If you anticipate that the total costs associated with fulfilling this request will exceed $35, please contact me with an estimate of the likely cost before proceeding**.

IV. Information about the request

The Texas Public Information Act mandates that if you are unable to produce the requested information within 10 business days of this request, you certify that fact in writing and set a date within a reasonable time when the information will be available.

Should you elect to withhold or delete any information, please justify your decision by referencing specific exemptions under the Act. In doing so, we remind the District that Tex. Gov't Code § 552 establishes a strong presumption in favor of disclosure. *See* Open Records Decision 363 at 1 (1983) (explaining that records must be disclosed "unless they fall within one of the particular exceptions applicable"); Open Records

---

report, or notification by the District's digital monitoring system(s), whether that alert, flag, block, restriction, report, or notification is sent to the affected student, an employee or contractor of the surveillance provider, a District employee, or another individual. "List of blocked or monitored words" explicitly includes any "default" words or phrases suggested by the District's surveillance partner and adopted by the District, as well as any additional words or phrases added or requested by the District.

[9] For purposes of this request, "list of blocked or filtered websites" means any specific website, domain name, or keyword within a website name that is blocked, filtered, or otherwise restricted by the District, as well as any specific website, domain name, or keyword within a website name that may trigger an alert, flag, block, restriction, report, or notification by the District's digital monitoring system(s).

Decision 91 at 2 (1975) ("The Act makes all information public unless excepted."). These exemptions "should be construed narrowly." *Arlington Indep. Sch. Dist. v. Tex. Att'y Gen.*, 37 S.W.3d 152, 157 (Tex. App. 2001). If any exemption that you assert applies to only a portion of the information (as opposed to the entire record), please redact the portion you claim is exempt, provide copies of the remainder of the information, and detail your reasons for the modification.

We also ask that you provide responsive electronic information in its native file format. Alternatively, please provide the information electronically in a text-searchable, static-image format (e.g., PDF), in the best image quality in the District's possession, and in separate, Bates-stamped files.

We request that you produce responsive materials in their entirety, including all attachments, appendices, enclosures, and/or exhibits. To the extent that a response to this request would require you to provide multiple copies of identical material, the request is limited so that only one copy of identical material is requested.

* * *

Thank you for your attention to our request. We would be happy to discuss its terms with you over the phone or via email to clarify any aspect of it.

/s/ Jennifer Jones

Jennifer Jones
Stacy Livingston
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT B

Subject: [Records Center] Open Public Records Request :: P000953-033023
Date: Wednesday, April 5, 2023 at 6:50:50 PM Eastern Daylight Time
From: GCISD Support
To: Jennifer Jones

--- Please respond above this line ---

RE: PUBLIC RECORDS REQUEST of March 30, 2023, Reference # P000953-033023

Dear Jennifer Jones,

The Grapevine-Colleyville ISD ("District") received a Public Information Act Request from you on March 30, 2023. After reviewing your request for records, the District has determined that some or all of your request is likely to fit within an exception to disclosure under Texas Government Code Section 552.139. Therefore, the District is notifying you that it intends to request an opinion of the Texas Attorney General regarding your request. That determination from the Attorney General can take up to sixty or more days to receive.

This letter is also being sent to clarify some of the information that you are seeking from the District. The District is not able to conduct a search of its email system without search terms. Your request is for "any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications between District employees and communications between the District and the company supplying the District's digital surveillance system." Please identify the search terms that you are asking the District to search.

Additionally, do you intend for the District to search every employee's email correspondence since January 1, 2020, or are there individuals or positions whose email communication you would like us to search? The District has more than 1,750 employees and the search, as currently submitted, implies all employees. Depending on the search terms that you provide, this could result in a significant number of emails for the District to review for responsiveness and for confidential information. Certain confidential information may be redacted by the District but if there is a question about whether something in that communication is confidential, the District reserves its right to seek an Attorney General opinion regarding that information.

Once the District receives clarification from you on the items requested, the District will be able to prepare a cost estimate as required by Texas Government Code, Section 552. That estimate will include the costs for locating, compiling, reviewing and redacting all records, as needed.

If you would like for the District to proceed with your public information request, please provide the clarifications within sixty-one (61) days from today, April 5, 2023. Otherwise, the District will consider your request withdrawn.

You may provide a response to the District by any of the following methods:

1. by responding to this email/letter

2. by regular mail to Grapevine-Colleyville ISD, Attention: Alex Harlow, Grapevine-Colleyville ISD, 3051 Ira E Woods, Grapevine, TX 76051

3. in person at the Office of the Grapevine-Colleyville ISD, Alex Harlow, 3051 Ira E Woods, Grapevine, TX 76051

Upon receipt of your clarification, the Grapevine-Colleyville ISD will further respond to your Public Information Act Request as required by law, including providing you with an estimate of costs associated with producing the requested records.

Sincerely,

Paula Barbaroux

Chief Operations Officer

To monitor the progress or update this request please log into the Open Public Records Center



EXHIBIT C

Alexandra M. Williams
(817) 334-7292 (Direct Dial)
(817) 334-7290 (Direct Fax)
amwilliams@jw.com

April 13, 2023

Office of Attorney General
Open Records Section
P.O. Box 12548
Austin, Texas 78711-2548

Re: Open Records Request of Jennifer Jones, The Knight First Amendment Institute received on March 30, 2023; Internal Ref. No. P000953-033023

Dear Sir or Madam:

I am counsel to the Board of Trustees for Grapevine-Colleyville Independent School District (the "District") and provide this correspondence on the District's behalf. The District is requesting an opinion pursuant to Texas Government Code § 553.301 of the Texas Public Information Act ("Act") regarding whether certain information is subject to disclosure under the Act. The District received the enclosed public information request on March 30, 2023.[1]

The requestor made the following requests ("Request") to the District:

> *The Knight Institute requests the following information related to the Grapevine-Colleyville Independent School District's use of surveillance systems to monitor student activity on digital devices and accounts, created on or after January 1, 2020:*
>
> a. *Any information identifying the words or phrases the District has included, or plans to include, in its list(s) of blocked or monitored words;*
> b. *Any information identifying the websites the District has included, or plans to include, in its list(s) of blocked or filtered websites; and*
> c. *Any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications between District employees, and communications between the District and the company supplying the District's digital surveillance system.*

[1] A true and correct copy is attached as Exhibit 1.

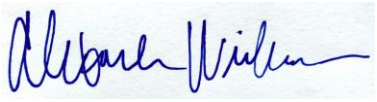
There are documents responsive to this Request. However, the District believes that the items responsive to this Request may be excepted from public disclosure under Texas Government Code § 552.139.

Pursuant to Texas Government Code § 552.301(e), the District will send within 15 business days of the receipt of the Request additional information supporting its request for an Attorney General decision. Such correspondence will include copies of the documents (or representative samples of such documents) containing the information that may be protected from disclosure under the Act, as well as the District's arguments for exception from disclosure and legal support.

By copy of this letter, the District is informing the requestor of its request for an Attorney General decision regarding whether the requested information is within an exception to the Act and of its intent to withhold the information until a decision is made pursuant to this request. Tex. Gov't Code § 552.301(d).

Should you have any questions, please do not hesitate to contact me.

Sincerely,



Alexandra M. Williams
Attorney

Enclosures as noted

cc: Requestor Jennifer Jones, The Knight First Amendment Institute, w/o enclosures (via email)

Paula Barbaroux, w/o enclosures (via email)

35906766v.1

EXHIBIT 1

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
info@knightcolumbia.org

March 29, 2023

Grapevine-Colleyville Independent School
District
Public Information Request
3051 Ira E. Woods Avenue
Grapevine, Texas 76051

Re: Texas Public Information Act Request

To whom it may concern,

This letter constitutes a request pursuant to the Texas Public Information Act ("TPIA"), Texas Government Code Ch. 552, for information related to the Grapevine-Colleyville Independent School District's ("District") use of surveillance systems to monitor students' activity on digital devices and accounts. This request is made for public and non-commercial purposes by the Knight First Amendment Institute at Columbia University ("Knight Institute" or "Institute").[1]

I. Background

As students across the country transitioned to remote learning in response to the COVID-19 pandemic, school administrators increasingly turned to surveillance companies to assist with monitoring students' activity on digital devices and school-issued Google and Microsoft accounts.[2] One of the most prevalent tools marketed by these companies is spy tech that uses artificial intelligence to track all student activity and communications on their digital devices and accounts. In practice,

[1] The Knight First Amendment Institute is a New York not-for-profit corporation based at Columbia University that works to preserve and expand the freedoms of speech and the press through strategic litigation, research, and public education.

[2] Mark Keierleber, *The spy tech that followed kids home for remote learning—and won't leave*, Fast Company (Sept. 20, 2021), https://www.fastcompany.com/90677509/the-spy-tech-that-followed-kids-home-for-remote-learning-and-wont-leave.

these systems typically work by restricting students' access to specific websites and/or applications, while scanning student emails, documents, chats, and more against a list of monitored words and phrases.[3] Any content that may indicate a student is engaging in "inappropriate behaviors" or poses "potential threats to self or others," including profanity, references to self-harm, violence, bullying, or drugs, is flagged by the tool and reviewed by human content moderators, who can pass the material to school administrators or law enforcement to take further action.[4] While surveillance companies typically have a standard list of keywords that will generate a flag, school administrators have the ability to customize this list to reflect local contexts.[5]

Surveillance companies claim that these systems protect student safety, but students, parents, and others have raised concerns that they actually cause serious harm, posing significant threats to students' privacy and free speech rights and contributing to a long legacy of policing and surveillance in public schools.[6] To learn more about how these systems are being deployed, this request seeks records related to the list of words, phrases, and websites that the District filters and/or monitors as part of its surveillance of students' digital activities.

II. Information requested

The Knight Institute requests the following information[7] related to the Grapevine-Colleyville Independent School District's use of surveillance systems to monitor student activity on digital devices and accounts, created on or after January 1, 2020:

a. Any information identifying the words or phrases the District has included, or plans to include, in its list(s) of blocked or monitored words;[8]

---

[3] Caroline Haskins, *Gaggle Knows Everything About Teens And Kids In School*, Buzzfeed News (Nov. 1, 2019, 3:48pm), https://perma.cc/7269-VTFS.

[4] *Id.*; Mark Keierleber, *Minneapolis Schools to Halt Controversial Student Surveillance Initiative*, The 74 (June 27, 2022), https://perma.cc/S6TA-6696.

[5] Mark Keierleber, *Gaggle Surveils Millions of Kids in the Name of Safety. Targeted Families Argue it's 'Not That Smart'*, The 74 (Oct. 12, 2021), https://perma.cc/Q94H-T6TG.

[6] Keierleber, *supra* note 4.

[7] For purposes of this request, "information" includes but is not limited to all records or communications preserved in written or electronic form, including but not limited to: correspondence, documents, data, videotapes, audio tapes, emails, faxes, files, guidance, guidelines, evaluations, instructions, analyses, memoranda, agreements, notes, orders, policies, procedures, protocols, reports, rules, training manuals, other manuals, or studies.

[8] For purposes of this request, "list of blocked or monitored words" means any specific word or phrase that may trigger an alert, flag, block, restriction,

b. Any information identifying the websites the District has included, or plans to include, in its list(s) of blocked or filtered websites;[9]

c. Any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications between District employees, and communications between the District and the company supplying the District's digital surveillance system.

III. Request for waiver or limitation of fees

The Knight Institute requests that you produce the information free of charge on the grounds that this request is made for public and non-commercial purposes and will benefit the general public. Tex. Gov't Code § 552.267. However, if you are unable to do so, the Institute will reimburse you for the reasonable costs associated with fulfilling this request if your office has a policy of requiring the payment of a copying charge for such information. **If you anticipate that the total costs associated with fulfilling this request will exceed $35, please contact me with an estimate of the likely cost before proceeding**.

IV. Information about the request

The Texas Public Information Act mandates that if you are unable to produce the requested information within 10 business days of this request, you certify that fact in writing and set a date within a reasonable time when the information will be available.

Should you elect to withhold or delete any information, please justify your decision by referencing specific exemptions under the Act. In doing so, we remind the District that Tex. Gov't Code § 552 establishes a strong presumption in favor of disclosure. *See* Open Records Decision 363 at 1 (1983) (explaining that records must be disclosed "unless they fall within one of the particular exceptions applicable"); Open Records

---

report, or notification by the District's digital monitoring system(s), whether that alert, flag, block, restriction, report, or notification is sent to the affected student, an employee or contractor of the surveillance provider, a District employee, or another individual. "List of blocked or monitored words" explicitly includes any "default" words or phrases suggested by the District's surveillance partner and adopted by the District, as well as any additional words or phrases added or requested by the District.

[9] For purposes of this request, "list of blocked or filtered websites" means any specific website, domain name, or keyword within a website name that is blocked, filtered, or otherwise restricted by the District, as well as any specific website, domain name, or keyword within a website name that may trigger an alert, flag, block, restriction, report, or notification by the District's digital monitoring system(s).

Decision 91 at 2 (1975) ("The Act makes all information public unless excepted."). These exemptions "should be construed narrowly." *Arlington Indep. Sch. Dist. v. Tex. Att'y Gen.*, 37 S.W.3d 152, 157 (Tex. App. 2001). If any exemption that you assert applies to only a portion of the information (as opposed to the entire record), please redact the portion you claim is exempt, provide copies of the remainder of the information, and detail your reasons for the modification.

We also ask that you provide responsive electronic information in its native file format. Alternatively, please provide the information electronically in a text-searchable, static-image format (e.g., PDF), in the best image quality in the District's possession, and in separate, Bates-stamped files.

We request that you produce responsive materials in their entirety, including all attachments, appendices, enclosures, and/or exhibits. To the extent that a response to this request would require you to provide multiple copies of identical material, the request is limited so that only one copy of identical material is requested.

* * *

Thank you for your attention to our request. We would be happy to discuss its terms with you over the phone or via email to clarify any aspect of it.

/s/ Jennifer Jones

Jennifer Jones
Stacy Livingston
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT D

Alexandra M. Williams
(817) 334-7292 (Direct Dial)
(817) 334-7290 (Direct Fax)
amwilliams@jw.com

April 20, 2023

VIA ONLINE SUBMISSION

The Honorable Ken Paxton
Attorney General, State of Texas
Open Records Section
P.O. Box 12548
Austin, Texas 78711-2548

Re: Open Records Request of Jennifer Jones of the Knight First Amendment Institute received on March 30, 2023
Internal Ref: P000953-033023

Dear Attorney General Paxton:

I am counsel to the Board of Trustees for Grapevine-Colleyville Independent School District (the "District"). The District received the public information request attached as Exhibit 1 on March 30, 2023 ("Request"). This firm, on behalf of the District, previously submitted a timely 10-day letter with respect to the Request. A copy of the District's 10-day letter is attached as Exhibit 2. The District now requests an opinion on certain documents attached as Exhibit 3.

This correspondence constitutes the District's submission required under Texas Government Code § 552.301(e). By copy of this letter, the District is informing the requestor of its submission of written comments to the Attorney General under Section 552.301(e). Tex. Gov't Code § 552.301(e-1).

The requestor made the following requests to the District:[1]

> *The Knight Institute requests the following information related to the Grapevine-Colleyville Independent School District's use of surveillance systems to monitor student activity on digital devices and accounts, created on or after January 1, 2020:*
>
> *a. Any information identifying the words or phrases the District has included, or plans to include, in its list(s) of blocked or monitored words;*

[1] *See* Exhibit 1.

b. *Any information identifying the websites the District has included, or plans to include, in its list(s) of blocked or filtered websites; and*
c. *Any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications between District employees, and communications between the District and the company supplying the District's digital surveillance system.*[2]

The Request seeks information the District contends is excepted from disclosure under the Act for reasons discussed with greater specificity, below.

Please find attached in Exhibit 3 the documents that the District contends are not subject to mandatory disclosure. The District believes these documents fall within the following applicable exception:

TEX. GOV'T CODE § 552.139 – Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers

Exhibit 3 contains the responsive information the District maintains is not subject to disclosure. Exhibit 3 shows certain information (*i.e.*, words, website addresses) the District has chosen to block or filter from its network for the purpose of protecting the safety and security of District employees and students, as well as to protect the safety and security of the District's network by preventing computer security incidents.

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. In other words, 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). The public disclosure of such words, website addresses, and other related information may expose the District to unnecessary security threats. As such, the District requests that Attorney General permit the District to withhold all information responsive to the Request (*i.e.*, the entirety of Exhibit 3).[3]

[2] The District sent a request for clarification to the requestor with respect to subsection (c) of the Request on April 5, 2023, inquiring whether the requestor intended for the District to search the e-mail accounts of each and every District employee and requesting whether requestor could identify search terms to be used in such a search. See Tex. Gov't Code § 552.222. The District has not received any response from the requestor. As such, this correspondence pertains only to subsections (a) and (b) of the Request.

[3] *See* Tex. Att'y Gen. Op. No. OR2019-01233 (finding that a school district must withhold information in response to a similar request for "all urls and keywords that are blocked on school and or district WiFi networks" as such information "relates to computer network security, and the design, operation, or defense of the district's computer network").

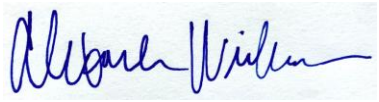
Conclusion

The District believes that the responsive documents contained in Exhibit 3 should be excepted from disclosure under the Act. This This correspondence constitutes the District's request to the Attorney General required under Texas Government Code § 552.301(e). The Attorney General has not made a previous determination regarding the specific information contained in Exhibit 3.

By copy of this letter, the District is informing the requestor of its request to the Attorney General, contained herein, for a decision regarding whether the information is within an exception and of its intent to withhold the requested information until a decision is made by your office pursuant to this request. Tex. Gov't Code § 552.301(e-1).

Should you have any questions, please do not hesitate to contact me.

Sincerely,



Alexandra M. Williams
Attorney

Enclosures as noted

cc: Requestor Jennifer Jones, The Knight First Amendment Institute, w/o enclosures (via email)

Paula Barbaroux, w/o enclosures (via email)

35902656v.1

EXHIBIT E

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
info@knightcolumbia.org

June 2, 2023

Alex Harlow
Grapevine-Colleyville Independent School
District
3051 Ira E. Woods
Grapevine, TX 76051

Re: Public Information Act Request No. P000953-033023

Dear Alex Harlow,

Thank you for your response to the Public Information Act request submitted by the Knight First Amendment Institute at Columbia University ("Institute") on March 29, 2023, Reference No. P000953-033023. We write in response to your email correspondence dated April 5, 2023.

First, you indicated that the Grapevine-Colleyville Independent School District ("District") has determined that some or all of the Institute's request is likely to fit within an exception to disclosure under Texas Government Code Section 552.139 and notified us of your intent to request an opinion of the Texas Attorney General regarding our request.[1] Second, you asked for clarity regarding the information the Institute seeks from the District. Specifically, you asked that the Institute identify search terms for the District to use in its search for responsive information. Finally, you asked whether we intend for the District to search every employee's email correspondence since January 1, 2020, or if there are specific individuals or positions whose email communications we would like you to search.

We address each of these items below.

[1] Since then, the Institute has received copies of the correspondence sent by Counsel to the Board of Trustees for Grapevine-Colleyville Independent School District to the Texas Attorney General on April 13, 2023, and April 20, 2023.

I. Proposed narrowing of the Request

To address the District's stated concerns that disclosing the information responsive to subsections (a) and (b) of our Request may jeopardize the safety and security of District employees and students and may expose the District to cybersecurity threats, we would like to narrow the entire Request, inclusive of subsections (a), (b), and (c), as follows[2]:

First, the Institute asks that the District limit its search to information related to the following:

i. monitoring and/or filtering teacher and student engagement[3] with current or historical events, political and social movements, and/or analysis of race, gender, and sexuality;
ii. compliance with Senate Bill 3[4]
iii. compliance with House Bill 3979,[5] or
iv. compliance with GCISD Board Policy EMB (LOCAL), EFA (LOCAL), EFB (LOCAL), and AIB (LOCAL)[6]

---

[2] Subsection (a) of our Request seeks "Any information identifying the words or phrases the District has included, or plans to include, in its list(s) of blocked or monitored words." Subsection (b) of our Request seeks "Any information identifying the websites the District has included, or plans to include, in its list(s) of blocked or filtered websites."

[3] For purposes of this Request, "engagement" includes but is not limited to classroom discussion, interpersonal communications, research, and writing.

[4] S.B. 3: Relating to civics training programs for certain public school social studies teachers and principals, parental access to certain learning management systems, and certain curriculum in public schools, including certain instructional requirements and prohibitions. S.B. 3, 87th Leg., Reg, Sess. (Tex. 2021), https://perma.cc/RB3Q-SDM4.

[5] H.B. 3979: Relating to civics instruction public school students and instruction policies in public schools. H.B. 3979, 87th Leg., Prior Sess. (Tex. 2021), https://perma.cc/9RH9-98WA.

[6] Grapevine-Colleyville Independent School District, *EMB – Miscellaneous Instructional Policies: Teaching About Controversial Issues*, Board Policy Manual (June 30, 2022), https://perma.cc/8JX7-ZP4W; Grapevine-Colleyville Independent School District, *EFA – Instructional Resources: Instructional Materials*, Board Policy Manual (Aug. 22, 2022), https://perma.cc/D47G-HU2V; Grapevine-Colleyville Independent School District, *EFB – Instructional Resources: Library Materials*, Board Policy Manual (Aug. 22, 2022), https://perma.cc/QN7E-HYFV; Grapevine-Colleyville Independent School District, *AIB – Accountability: Performance Reporting*, Board Policy Manual (Aug. 22, 2022), https://perma.cc/9BY3-9EZR.

Second, the Institute asks that the District exclude or redact any information from its search results that identifies words, phrases, or websites that could potentially identify methods of hacking or damaging the District's wireless or wired networks, databases, or computers. By excluding or redacting this specific information, the District can provide access to the government information requested by the Institute while avoiding public disclosure of information that may expose the District to security threats and/or threaten the safety and security of District employees and students.

II. Search terms and scope of subsection (c)

The Institute has identified search terms to clarify the information we seek related to subsection (c), which asks for "any correspondence regarding the list(s) of blocked, monitored, or filtered words and/or websites, including but not limited to internal communications between District employees and communications between the District and the company supplying the District's digital surveillance system." We have attached to this correspondence a spreadsheet identifying search terms. We also would like to clarify that we intend for the District to search every employee's email correspondence since January 1, 2020.

III. Additional information regarding our request

Finally, the District did not provide any information responsive to our request in the email dated April 5, 2023, including the names of the vendors the District contracts with to filter students' internet searches and/or monitor student activity on digital devices and accounts. We ask that the District confirm the name(s) of each vendor that it contracts with, or has previously contracted with, to provide these services since January 1, 2020.

* * *

Thank you for your attention to this matter. Please contact us directly if you have any questions.

/s/ Jennifer Jones
Jennifer Jones
Stacy Livingston
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
Jennifer.jones@knightcolumbia.org

EXHIBIT F

"CRT"
"anti-CRT"
"critical race theory"
"culturally responsive teaching"
"gender fluidity"
"non-binary" or "nonbinary"
"1619 Project"
"social construct"
"hormone therapy"
"gender reassignment"
"gender dysmorphia"
"gender expression"
"systemic racism"
"enslaved"
"slavery"
"feminism"
"white guilt"
"BLM"
"Black Lives Matter"
"intersex"
"pronouns"
"trans rights" or "transgender rights"
"transgender"
"TERF"
"AIDs"
"planned parenthood"
"ACLU"
"implicit racism"
"implicit bias"
"IAT" or "implicit association test"
"reparations"
"oppression" or "oppressed" or "oppress"
"eugenics"
"discrimination" or "discriminate" or "discriminatory"
"misogyny" or "misogynist"
"sexism" or "sexist"
"true founding"
"redlining" or "red-lining"
"police brutality"
"overpolicing"
"inequality"
"racial wealth gap"
"lynching"
"equity" or "equitable"
"diversity, equity, and inclusion" or "DEI"

"woke"
"marxism" or "marxist"
"communism" or "communist"
"socialism" or "socialist"
"same-sex"
"homosexuality" or "homosexual"
"heterosexuality" or "heterosexual"
"cisgender" or "cis"
"cultural appropriation"
"cultural competence" or "multicultural competence"
"institutional racism"
"colonialism" or "neo-colonialism" or "colonize" or "decolonize"
"cultural intelligence"
"anti-racism" or "anti-racist" or "antiracism" or "antiracist"
"social justice"
"restorative justice"
"internalized bias"
"bisexual" or "bisexuality"
"normative" or "heteronormative"
"disparate outcomes" or "disparate impact"
"inequity"
"power structure"
"racial hierarchy"
"caste"
"afrocentric" or "afrocentrism" or "eurocentric" or "eurocentrism"
"neoliberal"
"ethnocentric"
"microagression"
"people of color" or "POC" or "BIPOC"
"white privilege"
"underprivileged"
"marginalize"
"minority"
"whiteness"
"blackness"
"social emotional learning"
"Stamped"
"gender theory"
"racial profiling"
"colorblind"
"abortion"
"pregnant" or "pregnancy"
"mifepristone"
“transgenderism”
"gender transitioning"

"gender-affirming"
"hormone replacement therapy" or "HRT"
"sexual orientation"
"drag"
"say their names"
"S.B. 3" or "SB3" or "SB-3" or "senate bill 3"
"H.B. 3987" or "HB3987" or "house bill 3987"
"New York Times" or "NYT"
"Nikole Hannah-Jones" or "Nikole Hannah Jones"
"queer"

EXHIBIT G

Subject: [Records Center] Open Public Records Request :: P000953-033023
Date: Thursday, June 8, 2023 at 11:52:28 AM Eastern Daylight Time
From: GCISD Support
To: Jennifer Jones

--- Please respond above this line ---

GRAPEVINE COLLEYVILLE INDEPENDENT SCHOOL DISTR CT

RE: PUBLIC RECORDS REQUEST of March 30, 2023, Reference # P000953-033023

Dear Ms. Jones,

The Grapevine-Colleyville ISD ("District") received your response to the District's request for clarification on June 2, 2023.

First, in regard to Section II of your response, the District ran an initial search of all current and former employees' emails for the time period of January 1, 2020, to March 30, 2023, using the 140 search terms that you submitted. This resulted in an email count of 2,400,179 potentially responsive emails of varying quantities of pages. The District uses Google Mail for its email system. Google does not deduplicate, therefore, the above number of emails will likely include duplicates. The above count also does not indicate the number of attachments that those emails might include. As required by Texas Government Code, Section 552.2615, the District is providing a cost estimate for this part of your records request. The District does not waive its right to charge fees as allowed by law. The estimate includes the time to review each potentially responsive email and its attachments and to redact any information as allowed by law. An example is information identifying a student. The District also reserves its right to submit other information that it finds in the records to the Texas Attorney General's Office for a determination about its withholding. An example is attorney-client communication.

The cost estimate for your clarified request as provided in your June 2, 2023 correspondence is as follows:

Compiling, reviewing, and redacting potentially responsive emails: 2,400,179 x 3 minutes = 120,008.95 hours at $15.00 per hour = $1,800,134.25

Overhead fee at 20% = $360,026.85

Total charges = $2,160,161.10

Please note that this is an estimate and the actual cost could be higher.

This cost estimate is being provided in accordance with Texas Government Code § 552.2615. Your clarified request will be considered automatically withdrawn if you do not respond in writing within ten business days that you (a) accept the estimated charges, (b) are modifying the request in response to this cost estimate, or (c) have sent a complaint regarding these estimated charges to the attorney general.

I hope the Institute is willing to narrow its search.

In regard to Section I. of your response letter, I appreciate the attempt to narrow the records request to those statements in items i. through iv. Unfortunately, the District's search does not include the ability to narrow a search of emails to those items. The system cannot perform such a task and therefore, an employee or contractor would have to review each email for such items. I note that some of the items in i. through iv. were included in the search terms referenced above but not all. The District will wait for the determination from the Texas Attorney General's office before proceeding with any response or cost estimate related to this part of the request.

Section III. of your response letter asks the District to confirm the names of each vendor that it contracts with, although such a request was not included in your initial public information request received on March 30, 2023. This request in Section III of your response is not a request for records and is therefore not a proper request under the Public Information Act. See, See Open Records Decision No. 555 at 1–2 (1990) (considering request for answers to fact questions). However, in the spirit of cooperation and transparency, the District states in response to your inquiry that it contracts with Lightspeed and Gaggle.

In your original request, dated March 29, 2023, received on March 30, 2023, you stated that the District is to request the following from all of its employees: correspondence, documents, data, videotapes, audio tapes, faxes, files, guidance, evaluations, instructions, analyses, memoranda, agreements, notes, orders, policies, procedures, protocols, reports, rules, training materials, other manuals, or studies related to the District's use of surveillance systems to monitor student activity with respect to all of the subparts of your request. (See Footnote 7 of your original request). Now that you have clarified that your request pertains to all of the District's employees (and former employees who were employed from January 2020 through the date of your request), we determine the number of potentially responsive records to be reviewed at approximately 1,000. Your response arrived several days after the conclusion of the GCISD academic year. Therefore, most of the faculty are now off contract and will have to be contacted upon their return for the new school year. The cost estimate for

this part of your request is as follows:

Compiling, reviewing, and redacting potentially responsive records: 1,000 x 3 minutes = 50 hours at $15.00 per hour = $750.

Overhead fee at 20% = $150

Total charges = $900.00

Again, please note that this is an estimate and the actual cost could be higher.

This cost estimate is being provided in accordance with Texas Government Code § 552.2615. Your clarified request will be considered automatically withdrawn if you do not respond in writing within ten business days that you (a) accept the estimated charges, (b) are modifying the request in response to this cost estimate, or (c) have sent a complaint regarding these estimated charges to the attorney general.

If you would like to proceed with this request, please submit a check in the amount of $445.00 (a deposit) made out to Grapevine-Colleyville ISD., Attention: Communications Department, 3051 Ira E. Woods Avenue, Grapevine, Texas 76501. Please mark the check with Reference # P000953-03323. This payment must be received within 10 business days of the date of this statement. Upon receipt of payment, the Grapevine-Colleyville ISD will proceed.

You may provide a response to the District by any of the following methods:

1. by responding to this email
2. by regular mail to Grapevine-Colleyville ISD, Attention: Alex Harlow, Public Information Specialist, 3051 Ira E Woods, Grapevine, TX 76051
3. in person at the Office of the Grapevine-Colleyville ISD, Attention: Alex Harlow, 3051 Ira E Woods, Grapevine, TX 76051

Finally, the District must notify you if there is a less costly method of viewing the records that you have requested. In this case, the District does not have a less costly way of allowing you to view the records.

Sincerely,

Paula Barbaroux

Chief Operations Officer

To monitor the progress or update this request please log into the Open Public Records Center

Powered by GovQA

EXHIBIT H

Subject: Knight First Amendment Institute information request, Reference #P000953-033023
Date: Wednesday, June 14, 2023 at 6:51:57 PM Eastern Daylight Time
From: Jennifer Jones
To: Williams, Ali

Dear Ali,

Thank you again for speaking with us yesterday regarding the Knight First Amendment Institute's public information request, Reference #P000953-033023. As we discussed, it would be helpful if the District could address the following questions as we work to further clarify our request in response to its correspondence dated June 8, 2023.

First, it is our understanding that the Gaggle and Lightspeed Systems services the District uses to monitor students' digital activities provide a user interface, sometimes called a "dashboard," and that the dashboard generates analytics reports. These reports provide school district administrators with data about the types of content the monitoring software has flagged. See, for example, Lightspeed's Filter Reports and Gaggle's Dashboard Reports. These reports could potentially give us insight into how the District uses the Lightspeed and Gaggle systems, which could potentially aid us in narrowing the scope of our request. Can the District confirm whether it has possession of this information? If so, would it be willing to prioritize production of this information to the Institute?

Second, the District indicated in its correspondence dated June 8, 2023 that its search of all current and former employees' emails for the time period of January 1, 2020, to March 30, 2023, using the 140 search terms that we submitted, resulted in an email count of 2,400,179 potentially responsive emails. We'd like to know if the District is able to further limit these email search results to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle."

Please let me know if you have any questions.

Thank you,
Jennifer

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT I

Tex. Atty. Gen. Op. OR2023-20568 (Tex.A.G.), Tex. Atty. Gen. Op. 2023-20568, 2023 WL 4332799

Office of the Attorney General

State of Texas
Informal Letter Ruling No. OR2023-20568
June 16, 2023

***1** Ms. Alexandra M. Williams
Counsel for Grapevine-Colleyville Independent School District
Jackson Walker, L.L.P.
777 Main Street, Suite 2100
Fort Worth, Texas 76102

Dear Ms. Williams:
You ask whether certain information is subject to required public disclosure under the Public Information Act (the "Act"), chapter 552 of the Government Code. Your request was assigned ID# 062638 (Internal Ref: P000953-033023).

The Grapevine-Colleyville Independent School District (the "district"), which you represent, received a request for information, including communications, regarding the district's digital surveillance system. You claim the submitted information is excepted from disclosure under section 552.139 of the Government Code. We have considered the exception you claim and reviewed the submitted information.

Section 552.139 of the Government Code provides, in relevant part:
(a) Information is excepted from [required public disclosure] if it is information that relates to computer network security, to restricted information under Section 2059.055 [of the Government Code], or to the design, operation, or defense of a computer network.

(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; [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.

Id. § 552.139(a), (b)(1)-(2), (4). Section 2059.055 of the Government Code provides, in pertinent part:
(b) Network security information is confidential under this section if the information is:
(1) related to passwords, personal identification numbers, access codes, encryption, or other components of the security system of a governmental entity;

(2) collected, assembled, or maintained by or for a governmental entity to prevent, detect, or investigate criminal activity; or

 © 2023 Thomson Reuters. No claim to original U.S. Government Works.

(3) related to an assessment, made by or for a governmental entity or maintained by a governmental entity, of the vulnerability of a network to criminal activity.

Id. § 2059.055(b). You state the submitted information reveals "certain words and website addresses which the [d]istrict has chosen to block or filter ... because of their propensity to expose the [district's computers and networks to malicious sites and other risks." You state the information at issue, if released, "may expose the [d]istrict to unnecessary security threats." Based on these arguments and our review of the information, we find the information we marked relates to computer network security, and the design, operation, or defense of the district's computer network. Accordingly, the district must withhold the information we marked under section 552.139 of the Government Code. However, we find you have not demonstrated the remaining information is subject to section 552.139. Accordingly, the district may not withhold any of the remaining information under section 552.139 of the Government Code. The district must release the remaining information.

***2** This letter ruling is limited to the particular information at issue in this request and limited to the facts as presented to us; therefore, this ruling must not be relied upon as a previous determination regarding any other information or any other circumstances.

This ruling triggers important deadlines regarding the rights and responsibilities of the governmental body and of the requestor. For more information concerning those rights and responsibilities, please visit our website at https://www.texasattorneygeneral.gov/open-government/members-public/what-expect-after-ruling-issued or call the OAG's Open Government Hotline, toll free, at (877) 673-6839. Questions concerning the allowable charges for providing public information under the Public Information Act may be directed to the Cost Rules Administrator of the OAG, toll free, at (888) 672-6787.
Sincerely,

D. Michelle Case
Assistant Attorney General
Open Records Division

Tex. Atty. Gen. Op. OR2023-20568 (Tex.A.G.), Tex. Atty. Gen. Op. 2023-20568, 2023 WL 4332799

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

EXHIBIT J

Subject: RE: Knight First Amendment Institute information request, Reference #P000953-033023
Date: Wednesday, June 21, 2023 at 4:27:11 PM Eastern Daylight Time
From: Williams, Ali
To: Jennifer Jones
Attachments: image001.png

Good afternoon, Jennifer:

I have communicated with Grapevine-Colleyville ISD ("GCISD") regarding your email below, which GCISD construes to be a clarification of your clarified request provided in your correspondence to GCISD dated June 2, 2023.

With regard to your first clarification, GCISD has identified reports associated with Lightspeed and/or Gaggle. However, GCISD does not believe such reports are subject to disclosure and will be seeking an opinion from the Attorney General regarding the withholding of such reports.

With regard to your second clarification, pertaining to further limiting the email search results to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle," GCISD has further limited such search. 824 responsive emails have been identified. As required by Texas Gov't Code Sec. 552.2615, GCISD is providing a cost estimate for this part of your records request. GCISD is not waiving its right to charge fees as allowed by law. The estimate includes the time to review each potentially responsive email and its attachments and to redact any information as allowed by law, including but not limited to personally identifiable information of students. GCISD reserves the right to submit other information it finds in these emails to the Attorney General's Office for a determination about its withholding. The cost estimate for your clarified request as provided in your email correspondence below dated June 14, 2023 is as follows:

- Compiling, reviewing, and redacting potentially responsive emails: 824 x 3 minutes = 41.2 hours at $15.00 per hour = $618
- Overhead fee at 20% = $123.6
- Total charges = $741.60

Please note that this is an estimate and the actual cost could be higher.

This cost estimate is being provided in accordance with Texas Gov't Code Sec. 552.2615. Your clarified request will be considered automatically withdrawn if you do not respond in writing within ten business days that you (a) accept the estimated charges, (b) are modifying the request in response to this cost estimate, or (c) have sent a complaint regarding these estimated charges to the attorney general. Your response may be sent by e-mail correspondence or regular mail to me as counsel for GCISD as well as by regular mail, in person, or through communication utilizing GCISD's PIA portal.

Additionally, GCISD, through counsel, received yesterday a ruling made by the Attorney General regarding the correspondence submitted by GCISD, through counsel, on April 13, 2023 and April 20, 2023 regarding your public information request #P000953-033023. The Attorney General ruled that some information shall be released to you and some information shall be withheld. GCISD personnel will release to you the information not subject to be withheld within the required time period.

Regards,
Ali

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com

Jackson Walker LLP

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Wednesday, June 14, 2023 5:52 PM
To: Williams, Ali <amwilliams@jw.com>
Subject: Knight First Amendment Institute information request, Reference #P000953-033023

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Dear Ali,

Thank you again for speaking with us yesterday regarding the Knight First Amendment Institute's public information request, Reference #P000953-033023. As we discussed, it would be helpful if the District could address the following questions as we work to further clarify our request in response to its correspondence dated June 8, 2023.

First, it is our understanding that the Gaggle and Lightspeed Systems services the District uses to monitor students' digital activities provide a user interface, sometimes called a "dashboard," and that the dashboard generates analytics reports. These reports provide school district administrators with data about the types of content the monitoring software has flagged. See, for example, Lightspeed's Filter Reports and Gaggle's Dashboard Reports. These reports could potentially give us insight into how the District uses the Lightspeed and Gaggle systems, which could potentially aid us in narrowing the scope of our request. Can the District confirm whether it has possession of this information? If so, would it be willing to prioritize production of this information to the Institute?

Second, the District indicated in its correspondence dated June 8, 2023 that its search of all current and former employees' emails for the time period of January 1, 2020, to March 30, 2023, using the 140 search terms that we submitted, resulted in an email count of 2,400,179 potentially responsive emails. We'd like to know if the District is able to further limit these email search results to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle."

Please let me know if you have any questions.

Thank you,
Jennifer

Jennifer Jones (she/her)
Staff Attorney

Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT K

Alexandra M. Williams
(817) 334-7292 (Direct Dial)
(817) 334-7290 (Direct Fax)
amwilliams@jw.com

June 28, 2023

VIA ONLINE SUBMISSION

The Honorable Ken Paxton
Attorney General, State of Texas
Open Records Section
P.O. Box 12548
Austin, Texas 78711-2548

Re: Clarified Open Records Request of Jennifer Jones of the Knight First Amendment Institute received on June 14, 2023
Internal Ref: P000953-033023

Dear Attorney General Paxton:

I am counsel to the Board of Trustees for Grapevine-Colleyville Independent School District (the "District"). The District received the public information request attached as Exhibit 1[1] on March 30, 2023 ("Original Request"). The District timely requested and obtained a ruling from the Attorney General regarding part of the Original Request.[2] The requestor responded to the District's request for clarification of the remainder of the Original Request on June 14, 2023 ("Clarified Request"), which is attached as Exhibit 2.[3]

In response to the Clarified Request, the District informed the requestor it intended to seek a ruling from the Attorney General with respect to the first part of the Clarified Request and provided a cost estimate pursuant to Texas Government Code § 552.2615 with respect to the second part of the Clarified Request.[4]

[1] Exhibit 1 also contains the District's correspondence to the Attorney General regarding the Original Request as well as the Attorney General's ruling pertaining to same.

[2] Following the receipt of the Attorney General's ruling on part of the Original Request, the District timely produced the documents identified by the Attorney General as not subject to withholding. The Attorney General assigned the District's request pertaining to the Original Request ID# 062638.

[3] The requestor's correspondence containing the clarification followed a telephone call with undersigned counsel regarding the substance of the request, and such correspondence was sent directly to counsel for the District, to be received on behalf of the District.

[4] As of the date of this correspondence, the District has not yet received a response from the requestor regarding the cost estimate. The District reserves the right to seek a ruling from the Attorney General with respect to the information responsive to the second part of the Clarified Request should the requestor timely indicate that she intends to move forward with this portion of the request.

As such, the District now requests an opinion on certain documents attached as Exhibit 3, which are responsive to the first part of the Clarified Request. The first part of the Clarified Request seeks reports from Gaggle and Lightspeed Systems which provide data to District personnel regarding content flagged by Gaggle and Lightspeed Systems during students' and employees' use of District technology.[5]

This correspondence constitutes the District's submission required under Texas Government Code § 552.301(b) and (e) with respect to the Clarified Request. By copy of this letter, the District is informing the requestor of its submission of written comments to the Attorney General regarding the Clarified Request under Section 552.301(b) and (e). Tex. Gov't Code § 552.301(d), (e-1).

TEX. GOV'T CODE § 552.139 – Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers

Exhibit 3 contains the responsive information the District maintains is not subject to disclosure. Exhibit 3 contains a report generated by Gaggle which identifies words and/or subjects monitored by Gaggle and shows the number of instances in which such word and/or subject is flagged by the Gaggle program within the District's technology systems. The District has engaged the services of Gaggle for the purpose of protecting the safety and security of District employees and students, as well as to protect the safety and security of the District's network by preventing computer security incidents.

Certain words, subjects, and/or 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. In other words, 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). The public disclosure of such words, website addresses, and other related information may expose the District to unnecessary security threats. As such, the District requests that Attorney General permit the District to withhold all information responsive to the Request (*i.e.*, the entirety of Exhibit 3).[6]

Conclusion

The District believes that the responsive documents contained in Exhibit 3 should be excepted from disclosure under the Act. The Attorney General has not made a previous determination regarding the specific information contained in Exhibit 3.

By copy of this letter, the District is informing the requestor of its request to the Attorney General, contained herein, for a decision regarding whether the information is within an exception and of

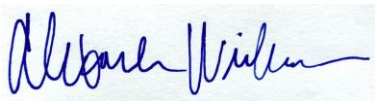
[5] *See* Exhibit 2.

[6] *See* Tex. Att'y Gen. Op. No. OR2019-01233 (finding that a school district must withhold information in response to a similar request for "all urls and keywords that are blocked on school and or district WiFi networks" as such information "relates to computer network security, and the design, operation, or defense of the district's computer network").

its intent to withhold the requested information until a decision is made by your office pursuant to this request. Tex. Gov't Code § 552.301(d), (e-1).

Should you have any questions, please do not hesitate to contact me.

Sincerely,



Alexandra M. Williams
Attorney

Enclosures as noted

cc: Requestor Jennifer Jones, The Knight First Amendment Institute, w/o enclosures (via email)

Paula Barbaroux, Gema Padgett, Alex Harlow w/o enclosures (via email)

EXHIBIT L

Subject: RE: Knight First Amendment Institute information request, Reference #P000953-033023
Date: Thursday, July 20, 2023 at 10:47:23 AM Eastern Daylight Time
From: Williams, Ali
To: Jennifer Jones
CC: Stacy Livingston, Alexander A Abdo
Attachments: image001.png

Jennifer,

I checked with the District regarding payment method, and the District cannot accept a credit card payment. Once the District receives the Institute's payment, it can begin to review the responsive records.

Given the volume of the records and the need to review for FERPA-protected information as well as information that should be presented to the Attorney General for a determination for withholding under the Public Information Act, as well as the other duties of the District employee assisting with this request given that the school year will soon be starting, the District will not be able to provide the responsive documents to the Institute within 10 business days after receiving payment. The District estimates needing 25 business days to review the records and provide responsive documents to the Institute.

Additionally, as noted in my e-mail correspondence to you on June 21, 2023 including the cost estimate, the cost estimate is just an estimate and could be higher. This will not be able to be precisely determined until the conclusion of the District's work in compiling and providing the responsive records is complete. If the District determines before it makes the records available to the Institute that the estimated charges will exceed the charges detailed in the previous written itemized statement (in my June 21, 2023 email) by 20 percent or more, the District will send to the Institute a written updated itemized statement that details all estimated charges that will be imposed, including any allowable charges for labor or personnel costs. If the Institute does not respond in writing to this updated estimate in the time and manner described by Tex. Gov't Code 552.2615(b), the request will be considered to have been withdrawn by the Institute.

Finally, your email below states that the Institute will pay the fees for the request, conditional on the Institute's right to seek judicial review of the denial of the request for a fee waiver. The determination made with regard to the requested fee waiver pursuant to Tex. Gov't Code 552.267(a) lies solely with the District. As stated herein, the District requires the Institute's payment to begin work on this request. Such payment is not conditional.

Please let me know if there is specific information you need in order to provide payment to the District for this request.

Ali

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com

Jackson Walker LLP

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Thursday, July 13, 2023 3:02 PM
To: Williams, Ali <amwilliams@jw.com>
Cc: Stacy Livingston <stacy.livingston@knightcolumbia.org>; Alexander A Abdo <alex.abdo@knightcolumbia.org>
Subject: Re: Knight First Amendment Institute information request, Reference #P000953-033023

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Dear Ali,
Thank you for your response. The Institute will pay for the fees associated with request #P000953-033023, conditional on our right to seek judicial review of the denial of our request for a fee waiver. Please let us know how we can remit payment for information responsive to this request. In the interest of obtaining the information as soon as possible, the Institute would prefer to pay via credit card. Please note that if the District requires payment via check, the Institute would need at least 3 weeks to process the check in accordance with Columbia University's payment processing timeline.
Thank you,

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

From: Williams, Ali <amwilliams@jw.com>
Date: Friday, July 7, 2023 at 10:46 AM
To: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Cc: Stacy Livingston <stacy.livingston@knightcolumbia.org>, Alexander A Abdo <alex.abdo@knightcolumbia.org>
Subject: RE: Knight First Amendment Institute information request, Reference #P000953-033023

Jennifer,

The District does not determine that the standard in Tex. Gov't Code Sec. 552.267(a) is met in this instance, and, therefore, will not waive or reduce the charges associated with the Knight First Amendment Institute's request.

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com

Jackson Walker LLP

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Friday, June 30, 2023 1:10 PM
To: Williams, Ali <amwilliams@jw.com>
Cc: Stacy Livingston <stacy.livingston@knightcolumbia.org>; Alexander A Abdo <alex.abdo@knightcolumbia.org>
Subject: Re: Knight First Amendment Institute information request, Reference #P000953-033023

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Dear Ali,

Thank you for your response. We write to ask that the District reconsider its decision regarding the Institute's request for a fee waiver, which was included in its public information request #P000953-033023. The Texas Public Information Act allows fees to be waived or reduced if the governmental body determines that providing a copy of the information primarily benefits the general public. Tex. Gov. Code § 552.267(a). Disclosure of the information sought here would primarily benefit the public interest, as it would inform the public about actual or alleged government activity. Specifically, the requested information is necessary to the public's understanding of how schools enforce rules concerning classroom discussions about sexuality, gender, and race. *See, e.g.*, Mark Keierleber, *The risks of student surveillance amid abortion bans and LGBTQ restrictions*, THE GUARDIAN (Sep. 8, 2022, 6:00 PM), https://www.theguardian.com/education/2022/sep/08/abortion-bans-school-surveillance-lgbtq-restrictions; Brian Lopez, *Republican bill that limits how race, slavery and history are taught in Texas schools becomes law*, THE TEXAS TRIBUNE (Dec. 2, 2021, 6:00 PM), https://www.texastribune.org/2021/12/02/texas-critical-race-theory-law/#:~:text=Republican%20bill%20that%20limits%20how,public%20policy%20or%20social%20affairs.%E2%80%9D. Moreover, disclosure would not further the Knight Institute's commercial interest. As indicated in our request, The Knight First Amendment Institute is a New York not-for-profit corporation based at Columbia University that works to preserve and expand the freedoms of speech and the press through strategic litigation, research, and public education. The Institute will make any information disclosed available to the public at no cost.

In light of the above, we ask that the District waive or reduce the $741.60 fee estimate it provided in its correspondence below, dated June 21, 2023. Thank you for considering our request.

Regards,
Jennifer

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

From: Williams, Ali <amwilliams@jw.com>
Date: Wednesday, June 21, 2023 at 4:27 PM
To: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Subject: RE: Knight First Amendment Institute information request, Reference #P000953-033023

Good afternoon, Jennifer:

I have communicated with Grapevine-Colleyville ISD ("GCISD") regarding your email below, which GCISD construes to be a clarification of your clarified request provided in your correspondence to GCISD dated June 2, 2023.

With regard to your first clarification, GCISD has identified reports associated with Lightspeed and/or Gaggle. However, GCISD does not believe such reports are subject to disclosure and will be seeking an opinion from the Attorney General regarding the withholding of such reports.

With regard to your second clarification, pertaining to further limiting the email search results to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle," GCISD has further limited such search. 824 responsive emails have been identified. As required by Texas Gov't Code Sec. 552.2615, GCISD is providing a cost estimate for this part of your records request. GCISD is not waiving its right to charge fees as allowed by law. The estimate includes the time to review each potentially responsive email and its attachments and to redact any information as allowed by law, including but not limited to personally identifiable information of students. GCISD reserves the right to submit other information it finds in these emails to the Attorney General's Office for a determination about its withholding. The cost estimate for your clarified request as provided in your email correspondence below dated June 14, 2023 is as follows:

- Compiling, reviewing, and redacting potentially responsive emails: 824 x 3 minutes = 41.2 hours at $15.00 per hour = $618
- Overhead fee at 20% = $123.6
- Total charges = $741.60

Please note that this is an estimate and the actual cost could be higher.

This cost estimate is being provided in accordance with Texas Gov't Code Sec. 552.2615. Your clarified request will be considered automatically withdrawn if you do not respond in writing within ten business days that you (a) accept the estimated charges, (b) are modifying the request in response to this cost estimate, or (c) have sent a complaint regarding these estimated charges to the attorney general. Your response may be sent by e-mail correspondence or regular mail to me as counsel for GCISD as well as by regular mail, in person, or through communication utilizing GCISD's PIA portal.

Additionally, GCISD, through counsel, received yesterday a ruling made by the Attorney General regarding the correspondence submitted by GCISD, through counsel, on April 13, 2023 and April 20, 2023 regarding your public information request #P000953-033023. The Attorney General ruled that some information shall be released to you and some information shall be withheld. GCISD personnel will release to you the information not subject to be withheld within the required time period.

Regards,
Ali

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com



From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Wednesday, June 14, 2023 5:52 PM
To: Williams, Ali <amwilliams@jw.com>
Subject: Knight First Amendment Institute information request, Reference #P000953-033023

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Dear Ali,

Thank you again for speaking with us yesterday regarding the Knight First Amendment Institute's public information request, Reference #P000953-033023. As we discussed, it would be helpful if the District could address the following questions as we work to further clarify our request in response to its correspondence dated June 8, 2023.

First, it is our understanding that the Gaggle and Lightspeed Systems services the District uses to monitor students' digital activities provide a user interface, sometimes called a "dashboard," and that the dashboard generates analytics reports. These reports provide school district administrators with data about the types of content the monitoring software has flagged. See, for example, Lightspeed's Filter Reports and Gaggle's Dashboard Reports. These reports could potentially give us insight into how the District uses the Lightspeed and Gaggle systems, which could potentially aid us in narrowing the scope of our request. Can the District confirm whether it has possession of this information? If so, would it be willing to prioritize production of this information to the Institute?

Second, the District indicated in its correspondence dated June 8, 2023 that its search of all current and former employees' emails for the time period of January 1, 2020, to March 30, 2023, using the 140 search terms that we submitted, resulted in an email count of 2,400,179 potentially responsive emails. We'd like to know if the District is able to further limit these email search results to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle."

Please let me know if you have any questions.

Thank you,
Jennifer

Jennifer Jones (she/her)
Staff Attorney

Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT M

Tex. Atty. Gen. Op. OR2023-30020 (Tex.A.G.), Tex. Atty. Gen. Op. 2023-30020, 2023 WL 6369986

Office of the Attorney General

State of Texas
Informal Letter Ruling No. OR2023-30020
August 31, 2023

***1** Ms. Alexandra M. Williams
Counsel for Grapevine-Colleyville Independent School District
Jackson Walker, L.L.P.
777 Main Street, Suite 2100
Fort Worth, Texas 76102

Dear Ms. Williams:
You ask whether certain information is subject to required public disclosure under the Public Information Act (the "Act"), chapter 552 of the Government Code. Your request was assigned ID# 077074 (Internal Ref: P000953-033023).

The Grapevine-Colleyville Independent School District (the "district"), which you represent, received a request for information, including a report regarding the district's digital surveillance system. [1] You claim the submitted information is excepted from disclosure under section 552.139 of the Government Code. We have considered the exception you claim and reviewed the submitted information.

Section 552.139 of the Government Code provides, in relevant part:
(a) Information is excepted from [required public disclosure] if it is information that relates to computer network security, to restricted information under Section 2059.055 [of the Government Code], or to the design, operation, or defense of a computer network.

(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; [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.

Id. § 552.139(a), (b)(1)-(2), (4). You state the submitted information consists of a report generated by the district's digital surveillance system that reveals the words and subjects that are being monitored by the system and the number of instances they are flagged by the program. You explain that the district has engaged these services to protect the safety and security of

 © 2025 Thomson Reuters. No claim to original U.S. Government Works.

district students and employees and the safety and security of the district's network by preventing computer security incidents. Based on these arguments and our review of the information, we agree the information you marked relates to computer network security, and the design, operation, or defense of the district's computer network. Accordingly, the district must withhold the information you marked under section 552.139 of the Government Code.

***2** This letter ruling is limited to the particular information at issue in this request and limited to the facts as presented to us; therefore, this ruling must not be relied upon as a previous determination regarding any other information or any other circumstances.

This ruling triggers important deadlines regarding the rights and responsibilities of the governmental body and of the requestor. For more information concerning those rights and responsibilities, please visit our website at https://www.texasattorneygeneral.gov/open-government/members-public/what-expect-after-ruling-issued or call the OAG's Open Government Hotline, toll free, at (877) 673-6839. Questions concerning the allowable charges for providing public information under the Public Information Act may be directed to the Cost Rules Administrator of the OAG, toll free, at (888) 672-6787.

Sincerely,

Michelle Garza
Assistant Attorney General
Open Records Division

Footnotes

1 You state the district sought and received clarification of the information requested. *See* Gov't Code § 552.222 (providing if request for information is unclear, governmental body may ask requestor to clarify request); *see also City of Dallas v. Abbott*, 304 S.W.3d 380, 387 (Tex. 2010) (holding that when a governmental entity, acting in good faith, requests clarification or narrowing of an unclear or overbroad request for information, the ten-day period to request an attorney general ruling is measured from the date the request is clarified or narrowed).

Tex. Atty. Gen. Op. OR2023-30020 (Tex.A.G.), Tex. Atty. Gen. Op. 2023-30020, 2023 WL 6369986

End of Document

© 2025 Thomson Reuters. No claim to original U.S. Government Works.

EXHIBIT N

Subject: [Records Center] Open Public Records Request :: P000953-033023
Date: Monday, October 23, 2023 at 10:17:06 AM Eastern Daylight Time
From: GCISD Support
To: Jennifer Jones

--- Please respond above this line ---

GRAPEVINE COLLEYVILLE INDEPENDENT SCHOOL DISTR CT

RE: PUBLIC RECORDS REQUEST of March 30, 2023, Reference # P000953-033023

Dear Ms. Jones,

Upon receipt of your payment, the District downloaded the 824 responsive emails and began its review for the purposes of redacting confidential information. In doing so, we discovered that almost all emails contain the very information the Texas Attorney General agreed must be withheld. The emails contain information about subjects being searched, keywords being monitored, threat types, and why the communication was flagged for review by District personnel. All of that information would be redacted and the result would be emails with very little information. We have attached a sample of a redacted email to illustrate the point.

If you agree that once redacted the information is of no use, the District is willing to refund the payment and close this request. If not, the District will once again seek an opinion of the Attorney General's office. I have attached a copy of the previous Attorney General's ruling.

Please let me know how you would like to proceed.

Sincerely,

Paula Barbaroux

Chief Operations Officer

To monitor the progress or update this request please log into the Open Public Records Center

Powered by GovQA

EXHIBIT O

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
info@knightcolumbia.org

November 7, 2023

Ali Williams
Jackson Walker LLP
777 Main Street Suite 2100
Fort Worth, TX 76102
amwilliams@jw.com

Re: Public Information Act request, Reference # P000953-033023

Counsel,

The Knight First Amendment Institute at Columbia University received an email from Grapevine-Colleyville Independent School District dated October 23, 2023 offering to refund our payment for the processing of 824 emails responsive to subsection (c) of our information request because, according to the District, most of the information in those emails would be redacted. The District also stated that, if the Institute nonetheless insisted on the processing and production of those emails, the District would seek an opinion from the Attorney General's office. We would like the District to continue to process and disclose the 824 emails it has identified as responsive to our request.

Moreover, we do not agree with the District that the information it intends to redact from the emails falls within any disclosure exception. On June 2, 2023 the Institute identified search terms to clarify the information we seek related to subsection (c) of our original request, and on June 14, 2023, we sent an email further narrowing the scope of information requested in subsection (c) to (1) emails to and from the "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle." The search terms that we provided specifically relate to concepts and terminology associated with social and political issues and identities such as race, gender, and sexual orientation. Neither these terms nor their presence in the emails at issue would reveal information related to the "design, operation, or defense of a computer network." Tex. Gov't Code § 552.139(a). Previously, you indicated that the District had blocked or

filtered from its network "[c]ertain words and website addresses" because of their propensity to expose the District's network to "malicious sites." But the search terms we've provided are not the kind of terms that could expose the District's network to a "computer security incident." *See* Tex. Gov't Code § 552.139(b)(4) (limiting excepted information to that which "directly "aris[es]" from "routine efforts" to address a "*computer* security incident") (emphasis added). At most, they would reveal that the District monitors its students' reading of material related to certain political and social topics, but that is no basis for redacting the search terms.

Finally, while we understand that you intend to seek an opinion from the Attorney General, we believe that such a request would be untimely. We sent (and the District received) our final clarification of the request on June 14, 2023. If the District wished to withhold any requested information, it was required to ask for an Attorney General opinion within ten days of receiving the clarified request. Tex Gov't Code § 552.301(b); *see also City of Dallas v. Abbott*, 304 S.W.3d 380, 387 (Tex. 2010) (when a governmental entity requests a good-faith clarification of a request, the ten-day period to request an attorney general ruling is measured from the date of clarification). In your June 21 correspondence to us and in your June 28 request to the Attorney General, you indicated that the District "reserves the right to submit other information it finds in these emails to the Attorney General's Office for a determination about its withholding." But the Public Information Act is clear that the ten-day clock to request an Attorney General opinion runs from the day the request is received or clarified. *See Dallas Area Rapid Transit v. Dallas Morning News,* 4 S.W.3d 469, 475 (Tex. App. 1999) (finding that the ten-day clock for requesting Attorney General opinion ran from the date of the request where the government agency was capable of perceiving the connection between requested information and an exemption that could apply in the future). As such, the information at issue is presumptively subject to disclosure. Tex. Gov't Code § 552.302; *Simmons v. Kuzmich*, 166 S.W.3d 342, 350 (Tex. App. 2005).

* * *

Accordingly, we ask that the District complete its processing and disclosure of the 824 emails responsive to our June 14 clarified request. Please let me know if you have any questions. Thank you.

/s/ Jennifer Jones
Jennifer Jones
Knight First Amendment Institute
at Columbia University

475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT P

Subject: RE: Knight Institute Public Information Act request, Reference # P000953-033023.
Date: Tuesday, November 14, 2023 at 5:38:20 PM Eastern Standard Time
From: Williams, Ali
To: Jennifer Jones
CC: Alexander A Abdo, Hannah Vester
Attachments: image001.png

Jennifer,

Pursuant to the request in your correspondence, the District will continue to process for production the emails it has identified as responsive to KFAI's request, as clarified, noting it has KFAI's payment on file. The District estimates it will be able to complete the review of such emails for production by end of the week, and production will be made to KFAI through the PIA portal utilized by the District (through which KFAI has received other correspondence from the District). The District's continued review will be for the purpose of making redactions in accordance with the Family Educational Rights and Privacy Act (FERPA) and with the Attorney General's ruling that certain information should be withheld as it relates to computer network security, and the design, operation, or defense of the District's computer network.

Best,
Ali

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com

JW | Jackson Walker LLP

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Tuesday, November 7, 2023 3:28 PM
To: Williams, Ali <amwilliams@jw.com>
Cc: Alexander A Abdo <alex.abdo@knightcolumbia.org>; Hannah Vester <hannah.vester@knightcolumbia.org>
Subject: Knight Institute Public Information Act request, Reference # P000953-033023.

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Ali,

Please see the attached correspondence regarding the Knight First Amendment Institute's Public Information Act request, Reference # P000953-033023.

Please let me know if you have any questions.

Thank you,
Jennifer

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT Q

Subject: Re: Knight Institute Public Information Act request, Reference # P000953-033023.
Date: Thursday, November 16, 2023 at 4:38:35 PM Eastern Standard Time
From: Jennifer Jones
To: Williams, Ali
CC: Alexander A Abdo, Hannah Vester
Attachments: image001.png

Ali,

We appreciate your update that the District will continue to process the emails responsive to the Institute's request. However, we object to the District's reliance on the previous Attorney General opinions dated June 16 and August 31, 2023 to redact information in the emails under section 552.139 of the Government Code. Those opinions made clear that the Attorney General's rulings are "limited to the particular information" presented for review and "must not be relied upon as a previous determination regarding any other information or any other circumstances." Tex. Atty. Gen. Op. 2023-20568 (June 16, 2023); Tex. Atty. Gen. Op. 2023-30020 (Aug. 31, 2023).

Accordingly, the previous opinions do not authorize redactions made in response to the second part of our clarified request, which the District expressly excluded from its June 28 submission to the Attorney General.

As we explained in our correspondence dated November 7, if the District contends that information responsive to part two of the Institute's clarified request is excludable, it was required to request an additional opinion within ten days of receiving that clarification on June 14. Because the District missed this deadline and is not permitted to rely on previous Attorney General opinions, it is not permitted to redact any information responsive to our clarified request under section 552.139.

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

From: Williams, Ali <amwilliams@jw.com>
Date: Tuesday, November 14, 2023 at 5:38 PM
To: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Cc: Alexander A Abdo <alex.abdo@knightcolumbia.org>, Hannah Vester <hannah.vester@knightcolumbia.org>
Subject: RE: Knight Institute Public Information Act request, Reference # P000953-033023.

Jennifer,

Pursuant to the request in your correspondence, the District will continue to process for production the

emails it has identified as responsive to KFAI's request, as clarified, noting it has KFAI's payment on file. The District estimates it will be able to complete the review of such emails for production by end of the week, and production will be made to KFAI through the PIA portal utilized by the District (through which KFAI has received other correspondence from the District). The District's continued review will be for the purpose of making redactions in accordance with the Family Educational Rights and Privacy Act (FERPA) and with the Attorney General's ruling that certain information should be withheld as it relates to computer network security, and the design, operation, or defense of the District's computer network.

Best,
Ali

Ali Williams | Attorney
777 Main Street Suite 2100 | Fort Worth, TX | 76102
V: (817) 334-7292 | F: (817) 334-7290 | amwilliams@jw.com

JW | Jackson Walker LLP

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Tuesday, November 7, 2023 3:28 PM
To: Williams, Ali <amwilliams@jw.com>
Cc: Alexander A Abdo <alex.abdo@knightcolumbia.org>; Hannah Vester <hannah.vester@knightcolumbia.org>
Subject: Knight Institute Public Information Act request, Reference # P000953-033023.

****RECEIVED FROM EXTERNAL SENDER – USE CAUTION****

Ali,

Please see the attached correspondence regarding the Knight First Amendment Institute's Public Information Act request, Reference # P000953-033023.

Please let me know if you have any questions.

Thank you,
Jennifer

Jennifer Jones (she/her)
Staff Attorney
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302 | New York, NY 10115
(646) 745-8500
jennifer.jones@knightcolumbia.org

EXHIBIT R

From: **Lightspeed Systems** do_not_reply@lightspeedsystems.com
Subject: [EXTERNAL] Lightspeed Systems Notification for [redacted]: Self-Harm
Date: August 24, 2022 at 6:08 PM
To:

LS

Lightspeed Systems®

Incident: Self-Harm

[redacted]

06:07:53 PM

Search: can you die from abortion

https://www.google.com/search

View Student Activity

Lightspeed Systems

2500 Bee Cave Road | Building One, Suite 350 | Austin, TX 78746

Notification Settings.

From: **Lightspeed Systems** do_not_reply@lightspeedsystems.com
Subject: [EXTERNAL] Lightspeed Systems Notification for [redacted]: Self-Harm
Date: October 24, 2022 at 11:12 PM
To:

LS

Lightspeed Systems®

Incident: Self-Harm

[redacted]

[redacted]

11:12:08 PM

Search: can you die from bedbug bites

https://www.google.com/search

View Student Activity

Lightspeed Systems

2500 Bee Cave Road | Building One, Suite 350 | Austin, TX 78746

Notification Settings.

EXHIBIT S

Alexandra M. Williams
(817) 334-7292 (Direct Dial)
(817) 334-7290 (Direct Fax)
amwilliams@jw.com

April 17, 2025

VIA ONLINE SUBMISSION

The Honorable Ken Paxton
Attorney General, State of Texas
Open Records Section
P.O. Box 12548
Austin, Texas 78711-2548

Re: Clarified Open Records Request of Jennifer Jones of the Knight First Amendment Institute received on June 14, 2023
Internal Ref: P000953-033023

Dear Attorney General Paxton:

I am counsel to the Board of Trustees for Grapevine-Colleyville Independent School District (the "District"). The District received the public information request attached as Exhibit 1[1] on March 30, 2023 ("Original Request"). The District requested and obtained a ruling from the Attorney General regarding part of the Original Request.[2] The requestor responded to the District's request for clarification of the remainder of the Original Request on June 14, 2023 ("Clarified Request"), which is attached as Exhibit 2.[3]

The requestor divided the Clarified Request into two separate but related portions. The first portion pertained to analytics reports generated by Lightspeed and Gaggle, which was the subject of correspondence to the Attorney General submitted by this office on June 28, 2023, on which the Attorney General made a determination on August 31, 2023.[4] The Attorney General determined that the District must withhold the information submitted under Section 552.139 as the information related to computer network security, and the design, operation, or defense of the District's

[1] Exhibit 1 also contains the District's 10-day and 15-day correspondence to the Attorney General regarding the Original Request and documents sought to be withheld in response to the Original Request as well as the Attorney General's ruling pertaining to same.

[2] Following the receipt of the Attorney General's ruling on part of the Original Request, the District timely produced the documents identified by the Attorney General as not subject to withholding.

[3] The requestor's correspondence containing the clarification followed a telephone call with undersigned counsel regarding the substance of the request, and such correspondence was sent directly to counsel for the District, to be received on behalf of the District.

[4] This June 28, 2023 correspondence to the Attorney General and August 31, 2023 correspondence from the Attorney General are attached together as Exhibit 3.

computer network.[5] The documents were withheld accordingly. The Attorney General directly provided the requestor with a copy of the Attorney General's determination and ruling.

The second part of the Clarified Request sought a narrowing of 2,400,179 potentially responsive e-mails of current and former District employees using 140 search terms provided by the requestor by limiting these communications to (1) e-mails to and from "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle." The clarification narrowed the number of responsive records to 824 e-mails. The District sent a cost estimate to the requestor pursuant to Texas Government Code § 552.2615 regarding these 824 e-mails responsive to the clarified version of the second part of the Clarified Request. The requestor paid the amount sent in the cost estimate for the processing and production of these communications. The 824 e-mails included keywords that corresponded to the information the Attorney General determined must be withheld in its August 31, 2023 correspondence. As such, the District redacted that information previously determined to be required to be withheld pursuant to Section 552.139 when producing the 824 e-mails to the requestor.

The requestor has contested the District's redaction of those terms despite the Attorney General's determination that such information must be withheld.[6] As such, the District now specifically requests an opinion on certain documents attached as Exhibit 4, which is a representative sample of documents responsive to the clarified second part of the Clarified Request.[7]

This correspondence constitutes the District's submission required under Texas Government Code § 552.301(b) and (e) with respect to the Clarified Request. By copy of this letter, the District is informing the requestor of its submission of written comments to the Attorney General regarding the Clarified Request under Section 552.301(b) and (e). Tex. Gov't Code § 552.301(d), (e-1).

TEX. GOV'T CODE § 552.139 – Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers

Exhibit 4 contains a representative sample of the responsive information the District maintains is not subject to disclosure.[8] The records in the representative sample are e-mails either to and from "lightspeedsystems.com" and "gaggle.net" email domains and/or (2) emails that include the terms "lightspeed" and "gaggle." These e-mails contain keywords, a notation about "threat type" and a note about why the incident was flagged, which is information that corresponds to the analytics reports responsive to the first part of the Clarified Request, which the Attorney General determined must be withheld pursuant to Section 552.139. The District has engaged the services of Gaggle for the purpose of protecting the safety and security of District employees and students, as well as to

[5] *See* Exhibit 3.

[6] The requestor has filed suit against the District regarding this redacted information. This litigation, *Knight First Amendment Institute at Columbia University v. Grapevine-Colleyville Independent School District*, Cause No. 348-362718-25, is currently pending in the 348th District Court, Tarrant County, Texas.

[7] The documents in Exhibit 4 are a representative sample of the 824 e-mails as referenced herein.

[8] The records in Exhibit 4 have been marked to indicate the portions the District is requesting to redact before production. Additionally, FERPA information has already been redacted on the records in Exhibit 4.

protect the safety and security of the District's network by preventing computer security incidents. These e-mails demonstrate the services provided by Gaggle in order to provide that safety and security to the District's network.

Certain words, subjects, and/or website addresses have been chosen by Gaggle and/or Lightspeed because of their propensity to expose the District's computers and network to malicious sites and other risks.[9] In other words, 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). The public disclosure of the keywords, threat types, and other related information may expose the District to unnecessary security threats. As such, the District requests that Attorney General permit the District to withhold the marked information in Exhibit 4.[10]

Finally, the District is aware that more than 10 business days have passed since receiving the Request. The Act provides that an untimely request for an Attorney General decision causes the information to be presumed to be subject to required public disclosure "unless there is a compelling reason to withhold the information." Tex. Gov't Code § 552.302. However, the Attorney General has routinely determined that Section 552.139 provides a compelling reason to overcome the presumption of openness and will evaluate the applicability of that section to information submitted by a governmental body past the 10-day deadline. *See* Tex. Atty. Gen. Op. OR2020-15920, 2020 WL 3120750; Tex. Atty. Gen. Op. OR2018-02510, 2018 WL 871288. As such, the District requests the Attorney General consider the applicability of Section 552.139 to the representative sample of responsive records contained in Exhibit 4.

Conclusion

The District believes that the representative sample of responsive documents contained in Exhibit 4 should be excepted from disclosure under the Act. The District maintains that the Attorney General has made a previous determination regarding this information in its determination dated August 31, 2023 in opining that the related information in the analytics reports must be withheld, but now submits this separate request for ruling so as to obtain the Attorney General's determination regarding these specific records.

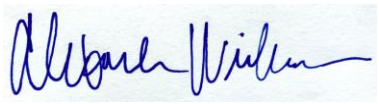
By copy of this letter, the District is informing the requestor of its request to the Attorney General, contained herein, for a decision regarding whether the information is within an exception and of its intent to withhold the requested information until a decision is made by your office pursuant to this request. Tex. Gov't Code § 552.301(d), (e-1).

[9] The District uses the products provided by Gaggle and Lightspeed, including the words, subjects, and website addresses to be caught by the products' filters, as provided and without further customization by the District.

[10] *See* Tex. Att'y Gen. Op. No. OR2019-01233 (finding that a school district must withhold information in response to a similar request for "all urls and keywords that are blocked on school and or district WiFi networks" as such information "relates to computer network security, and the design, operation, or defense of the district's computer network").

Should you have any questions, please do not hesitate to contact me.

Sincerely,



Alexandra M. Williams
Attorney

Enclosures as noted

cc: Requestor Jennifer Jones, The Knight First Amendment Institute, w/o enclosures (via email)

Paula Barbaroux, Alex Harlow (via email)

Charles Crawford, Lucas Henry (via email)

EXHIBIT T

May 27, 2025

Honorable Ken Paxton
Texas Attorney General
Open Records Division
P.O. Box 12548
Austin, Texas 78711-2548

Via: PIA Electronic Filing System

Re: Public Records Request of Knight First Amendment Institute at Columbia University to Grapevine-Colleyville Independent School District (No. P000953-033023).

Dear General Paxton,

We represent the Knight First Amendment Institute at Columbia University ("Knight Institute"), the requestor of the public information at issue in the above-referenced matter. On April 17, 2025, Grapevine-Colleyville Independent School District ("District") submitted an untimely request for an opinion from your office, seeking retroactive authorization to withhold public records sought by the Knight Institute nearly two years ago that are now the subject of active litigation. *See* Plaintiff's Original Petition and Request for Writ of Mandamus, *Knight First Amend. Inst. at Colum. Univ. v. Grapevine-Colleyville Indep. Sch. Dist.*, No. 348-362718-25 (348th Dist. Ct., Tarrant Cnty., Mar. 12, 2025) (attached as Exhibit A).

As the District acknowledges in its Request Letter, it should have sought an opinion from your office at the time the Knight Institute paid the fees to process the records it requested in the second part of its Clarified Request No. 2. *See* Request Letter at 3. Its failure to do so requires the District to show a "compelling" reason to withhold the responsive records to overcome the presumption that those records are now "subject to required public disclosure[.]" Gov't Code § 552.302. Whether or not the District can establish a "compelling" reason is a question now before the district court and, therefore, a question your office should decline to consider. *See* Ex. A ¶¶ 26-38, 43; *Kallinen v. City of Houston*, 462 S.W.3d 25, 28 (Tex. 2015) (Attorney General "does not claim exclusive jurisdiction to decide open records issues"); *cf.* Tex. Atty. Gen. Op. No. KP-0304 at 1, n.3 (2020) (noting Attorney General's "long-standing policy of generally refraining from addressing issues involved in pending litigation").

Abstention is particularly appropriate here because factual issues that cannot be resolved by your office affect the District's ability to establish a "compelling" justification for withholding. *See Paxton v. City of Dallas*, 509 S.W.3d 247, 259 (Tex. 2017) ("[A] reason to withhold information will be 'compelling' only when it is of such a pressing nature (e.g., urgent, forceful, or demanding)

that it outweighs the interests favoring public access to the information and overcomes section 552.302's presumption that disclosure is required.");[1] Open Records Decision No. 592 at 2 (1991) (Attorney General cannot resolve factual disputes in the opinion process). Indeed, the District originally informed the Knight Institute of its intent to seek an untimely Attorney General decision a year-and-a-half ago, on October 23, 2023, after being instructed by the Knight Institute to proceed with processing the records at issue in the second part of Clarified Request No. 2. Ex. A ¶¶ 34-35. But the District chose not to act until after the Knight Institute filed suit in March of this year. The District's lack of urgency in protecting the responsive records severely undercuts its position that the computer network security exception, Gov't Code § 552.139, if it even applies to these records,[2] is alone a compelling reason to withhold them.

Alternatively, if you do address the question of whether the District has met its burden to establish a compelling justification for continued withholding, you should find that the District has not. On the record before it, your office can (and should) find that:

1) The District was informed by your office in its August 31, 2023 opinion that the ruling "must not be relied upon as a previous determination regarding any other information or any other circumstances[,]" Atty. Gen. Op. OR2023-30020, 2023 WL 6369986, at *2 (Aug. 31, 2023);
2) The District was aware of this when it processed the second part of the Knight Institute's Clarified Request No. 2, which sought records materially different from the part of Clarified Request No. 2 for which the District requested an opinion, *see* Opinion Request Letter at 1-2 (describing its reliance on the Aug. 31, 2023 opinion in handling the second part of Clarified Request No. 2);
3) The District's reliance on the Aug. 31, 2023 opinion to withhold the responsive records at issue in the second part of Clarified Request No. 2 was improper given your office's admonishment not to use the Aug. 31, 2023 opinion as a previous determination;
4) By waiting a year-and-a-half to seek an Attorney General opinion—opting only to do so after the filing of litigation seeking disclosure of the responsive records—the District declined to act with the kind of urgency needed to show that continued withholding is "of such a pressing nature … that it outweighs the interests favoring public access[.]" *Paxton*, 509 S.W.3d at 259.

[1] *See also id.* at 258 ("The meaning of the term 'compelling' is of vital importance to our analysis because it represents a qualitative limitation on the justifications that permit withholding information from public disclosure.").

[2] The Knight Institute reserves its position on the substantive applicability of the computer network security exception for the proceedings before the district court in its pending litigation over these records.

The District offers little to meet its burden to overcome the presumption of public disclosure that has attached to these records. Its own conduct demonstrates that the District did not view as urgent the need to protect the responsive records, and its application of the computer network security exception to a representative sample of the responsive records is insufficient.[3]

The District could have made a more particularized showing to establish an imminent need to protect *specific* records under the computer network security exception. *See* PUBLIC INFORMATION ACT HANDBOOK 2024, at 43 ("Conclusory assertions that a particular exception applies to requested information will not suffice."). On the other side of the equation—the interests favoring public access—it defies belief that the District has an ongoing need for blanket permission to apply the computer network security exception to nearly two-year-old records containing keywords such as "New York Times," "ACLU," "inequality" or "social construct." Ex. A, pp. 46-47 of 94.

Accordingly, the Knight Institute respectfully requests that your office either (1) abstain from issuing a decision in this matter due to pending litigation; or (2) find that the District has not met its burden to establish a compelling justification to withhold the records at issue here.

Respectfully Submitted,

/s/ Peter B. 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
psteffensen@mail.smu.edu

Thomas S. Leatherbury
State Bar No. 12095275
THOMAS S. LEATHERBURY LAW, PLLC
1901 N. Akard St.
Dallas, TX 75201

[3] Nor, given the District's actions here, should the interests that "animate" the computer network security exception mandate that the exception itself be treated as "compelling in [its] own right." *Paxton*, 509 S.W.3d at 256; *see Tex. Comm'n on Env't Quality v. Sierra Club*, No. 03-21-00256-CV, 2022 WL 17096693, at *6 (Tex. App.—Austin Nov. 22, 2022, pet. denied) (holding the deliberative process privilege on its own does not constitute a compelling reason to overcome the presumption of public disclosure); *see also* OFFICE OF THE ATTORNEY GENERAL OF TEXAS, PUBLIC INFORMATION ACT HANDBOOK 2024, at 44 ("In the great majority of cases, the governmental body will not be able to overcome that presumption and must promptly release the requested information.").

Tel. (214) 213-5004
tom@tsleatherbury.com

/s/ *Jennifer Jones*

Jennifer Jones
Katie Fallow
Mary "Allie" Schiele
KNIGHT FIRST AMENDMENT INSTITUTE
AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
Email: jennifer.jones@knightcolumbia.org

Attorneys for Knight First Amendment Institute at Columbia University

cc: Alexandra M. Williams, Attorney for the Board of Trustees for Grapevine-Colleyville Independent School District, without enclosures (via email)

Charles Crawford, Lucas Henry, without enclosures (via email)

EXHIBIT U

KEN PAXTON
ATTORNEY GENERAL OF TEXAS

June 26, 2025

Ms. Alexandra M. Williams
Counsel for the Grapevine-Colleyville Independent School District
Jackson Walker LLP
777 Main Street, Suite 2100
Fort Worth, Texas 76102

OR2025-022099

Dear Ms. Williams:

You ask whether certain information is subject to required public disclosure under the Public Information Act (the "Act"), chapter 552 of the Government Code. Your request was assigned ID# 25-016471 (Ref. ID # P000953-033023).

The Grapevine-Colleyville Independent School District (the "district"), which you represent, received a request for information, including reports pertaining to the district's use of digital surveillance systems.[1] You state you have redacted student-identifying information from the submitted documents pursuant to the Family Educational Rights and Privacy Act ("FERPA"), section 1232g of title 20 of the United States Code.[2] You claim some of the submitted information is excepted from disclosure under section 552.139 of

[1] You state, and provide documentation demonstrating, the district sought and received clarification of the information requested. *See* Gov't Code § 552.222(b) (stating if information requested is unclear to governmental body or if large amount of information has been requested, governmental body may ask requestor to clarify or narrow request, but may not inquire into purpose for which information will be used); *City of Dallas v. Abbott*, 304 S.W.3d 380 (Tex. 2010) (holding when governmental entity, acting in good faith, requests clarification of unclear or overbroad request for public information, ten-business-day period to request attorney general opinion is measured from date request is clarified or narrowed).

[2] The United States Department of Education Family Policy Compliance Office (the "DOE") has informed this office FERPA does not permit state and local educational authorities to disclose to this office, without parental or student consent, unredacted, personally identifiable information contained in education records for the purpose of our review in the open records ruling process under the Act. The DOE has determined FERPA determinations must be made by the educational authority in possession of the education records. A copy of this letter may be found on the Office of the Attorney General's website: https://www.texasattorneygeneral.gov/files/og/20060725usdoe.pdf.

the Government Code.[3] We have considered the exception you claim and reviewed the submitted representative sample of information.[4] We have also received and considered comments submitted on behalf of the requestor. *See* Gov't Code § 552.304 (interested party may submit comments stating why information should or should not be released).

Section 552.139 of the Government Code provides, in relevant part:

> (a) Information is excepted from [required public disclosure] if it is information that relates to computer network security, to restricted information under Section 2059.055 [of the Government Code], or to the design, operation, or defense of a computer network.
>
> (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; [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.

Id. § 552.139(a), (b)(1)-(2), (4). You state the submitted information consists of a report generated by the district's digital surveillance system that reveals the words and subjects that are being monitored by the system and the number of instances they are flagged by the program. You explain that the district has engaged these services to protect the safety and security of district students and employees and the safety and security of the district's

[3] We note, and the district acknowledges, the district did not comply with section 552.301 of the Government Code in requesting a ruling from this office. *See* Gov't Code § 552.301(b), (e). Nonetheless, because section 552.139 can provide a compelling reason to overcome the presumption of openness, we will consider the applicability of this exception to the information at issue. *See id.* §§ 552.007, .302, .352.

[4] We assume the "representative sample" of records submitted to this office is truly representative of the requested records as a whole. *See* Open Records Decision Nos. 499 (1988), 497 (1988). This open records letter does not reach, and therefore does not authorize the withholding of, any other requested records to the extent those records contain substantially different types of information than that submitted to this office.

network by preventing computer security incidents. Based on these arguments and our review of the information, we agree the information you marked relates to computer network security, and the design, operation, or defense of the district's computer network. Accordingly, the district must withhold the information you marked under section 552.139 of the Government Code. The district must release the remaining information.

This letter ruling is limited to the particular information at issue in this request and limited to the facts as presented to us; therefore, this ruling must not be relied upon as a previous determination regarding any other information or any other circumstances.

This ruling triggers important deadlines regarding the rights and responsibilities of the governmental body and of the requestor. For more information concerning those rights and responsibilities, please visit our website at https://www.texasattorneygeneral.gov/open-government/members-public/what-expect-after-ruling-issued or call the OAG's Open Government Hotline, toll free, at (877) 673-6839. Questions concerning the allowable charges for providing public information under the Public Information Act may be directed to the Cost Rules Administrator of the OAG, toll free, at (888) 672-6787.

Sincerely,

Simone L. Nisbett
Assistant Attorney General
Open Records Division

SLN/tb

Ref: ID# 25-016471

c: Requestor

Third Party

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: 105987364
Filing Code Description: Amended Filing
Filing Description: Plaintiff's Amended Petition and Request for Writ of Mandamus
Status as of 9/23/2025 5:05 PM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Lucas ChristopherHenry		lhenry@abernathy-law.com	9/23/2025 4:57:12 PM	SENT
Charles J.Crawford		ccrawford@abernathy-law.com	9/23/2025 4:57:12 PM	SENT
Kimberly Escamilla		kescamilla@abernathy-law.com	9/23/2025 4:57:12 PM	SENT
Laura Ball		lball@abernathy-law.com	9/23/2025 4:57:12 PM	SENT
Peter Steffensen		psteffensen@smu.edu	9/23/2025 4:57:12 PM	SENT
Jennifer Jones		jennifer.jones@knightcolumbia.org	9/23/2025 4:57:12 PM	SENT
Katie Fallow		katie.fallow@knightcolumbia.org	9/23/2025 4:57:12 PM	SENT
Thomas Leatherbury		tom@tsleatherburylaw.com	9/23/2025 4:57:12 PM	SENT

FILED
TARRANT COUNTY
9/29/2025 9:35 AM
THOMAS A. WILDER
DISTRICT CLERK

CAUSE NO. 348-362718-25

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

DEFENDANT'S ANSWER TO PLAINTIFF'S AMENDED PETITION

Defendant, Grapevine-Colleyville Independent School District ("Defendant"), files the following answer to Plaintiff's Amended Petition and Request for Writ of Mandamus ("Plaintiff's Amended Petition").

I.
GENERAL DENIAL

Pursuant to Tex. R. Civ. P. 92, Defendant generally denies the allegations in Plaintiff's Amended Petition.

II.
AFFIRMATIVE DEFENSES

The redacted emails produced by Defendant to Plaintiff about which Plaintiff complains of in Plaintiff's Amended Petition contain student information protected from disclosure by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g. Plaintiff lacks standing to challenge Defendant's redactions based on Defendant's FERPA determinations.

The Court may not assess costs of litigation and reasonable attorney's fees incurred by Plaintiff because Defendant acted in reasonable reliance on written decisions of the attorney general. See Tex. Gov't Code §552.323(a)(3).

Plaintiff's claims are barred, in whole or in part, by Defendant's governmental immunity.

II.
PRAYER

For these reasons, Defendant asks the Court to dismiss Plaintiff's claims with prejudice, render judgment that Plaintiff takes nothing, assess costs against Plaintiff, and award Defendant all other relief to which it is justly entitled.

Respectfully submitted,

ABERNATHY, ROEDER, BOYD & HULLETT, P.C.

/s/ Charles J. Crawford
CHARLES J. CRAWFORD
State Bar No. 05018900
LUCAS C. HENRY
State Bar No. 24101901
1700 Redbud Blvd., Suite 300
McKinney, Texas 75069
Telephone: (214) 544-4000
Facsimile: (214) 544-4040
ccrawford@abernathy-law.com
lhenry@abernathy-law.com

ATTORNEYS FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that on September 29, 2025, a true and correct copy of Defendant's Answer to Plaintiff's Amended Petition has been served on all counsel of record via the Court's e-filing system.

/s/ Charles J. Crawford
Charles J. Crawford

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.

Kimberly Escamilla on behalf of Charles Crawford
Bar No. 05018900
kescamilla@abernathy-law.com
Envelope ID: 106180551
Filing Code Description: Answer/Response
Filing Description: Defendant's Answer to Plaintiff's Amended Petition
Status as of 9/29/2025 11:27 AM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Lucas ChristopherHenry		lhenry@abernathy-law.com	9/29/2025 9:35:46 AM	SENT
Charles J.Crawford		ccrawford@abernathy-law.com	9/29/2025 9:35:46 AM	SENT
Kimberly Escamilla		kescamilla@abernathy-law.com	9/29/2025 9:35:46 AM	SENT
Laura Ball		lball@abernathy-law.com	9/29/2025 9:35:46 AM	SENT
Peter Steffensen		psteffensen@smu.edu	9/29/2025 9:35:46 AM	SENT
Peter Steffensen		psteffensen@smu.edu	9/29/2025 9:35:46 AM	SENT
Jennifer Jones		jennifer.jones@knightcolumbia.org	9/29/2025 9:35:46 AM	SENT
Katie Fallow		katie.fallow@knightcolumbia.org	9/29/2025 9:35:46 AM	SENT
Thomas Leatherbury		tom@tsleatherburylaw.com	9/29/2025 9:35:46 AM	SENT
MARY ALLIESCHIELE		ALLIE.SCHIELE@KNIGHTCOLUMBIA.ORG	9/29/2025 9:35:46 AM	SENT

APPENDIX 2

Bruce Schneier

Contact: schneier@schneier.com

Background

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the *Economist*. He is the *New York Times* best-selling author of 16 books—including his latest, *A Hacker's Mind*—as well as hundreds of articles, essays, and academic papers. His influential newsletter *Crypto-Gram* and blog *Schneier on Security* are read by over 250,000 people. Schneier is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of EPIC and VerifiedVoting.org. He is the Chief of Security Architecture at Inrupt, Inc.; and a partner at Alchemist Associates, LLC.

Professional Experience

2025-present, partner, Alchemist Associates, New Haven, CT.

2019–present, Chief of Security Architecture, Inrupt, Inc., Boston, MA.

2016–2019, Chief Technology Officer, IBM Resilient, and special advisor to IBM Security, Cambridge, MA.

2014–2016, Chief Technology Officer, Resilient Systems, Inc. (formerly called Co3 Systems, Inc.), Cambridge, MA.

2006–2013, Chief Security Technology Officer, British Telecom, London, UK.

1999–2006, Chief Technology Officer, Counterpane Internet Security, Inc., Cupertino, CA.

1993–1999, President, Counterpane Systems, Oak Park, IL and Minneapolis, MN.

1991–1993, Member of Technical Staff, AT&T Bell Labs., Schaumburg, IL.

1990, Director of Operations, Intelligent Resources Information Systems, Inc., Chicago, IL.

1987–1990, Program Manager, Space and Naval Warfare Systems Command, Arlington, VA.

1984–1987, Electronics Engineer, Naval Electronics Systems Security Engineering Center, Washington, DC.

Academic Experience

2016+, Lecturer in Public Policy, John F. Kennedy School of Government, Harvard University.

2016–2018, Research Fellow in the Science, Technology, and Public Policy program at the Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University.

2013+, Fellow, Berkman Klein Center for Internet and Society, Harvard University.

Board Membership

2017+, Board Member, AccessNow, New York, NY

2013+, Board Member, Electronic Frontier Foundation, San Francisco, CA.

2016–2021, Board Member, Tor Project, Cambridge, MA.

2004–2013, Board Member, Electronic Privacy Information Center, Washington DC.

Education

MS Computer Science, American University, 1986.

BS Physics, University of Rochester, 1984.

Books

Rewiring Democracy: How AI Will Transform Our Politics, Government, and Citizenship (with Nathan Sanders), MIT Press, October 21, 2025 (forthcoming).

A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back, WW Norton & Co., 2023.

We Have Root: Even More Advice from Schneier on Security, John Wiley & Sons, 2019.

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, WW Norton & Co., 2018.

Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World, WW Norton & Co,, 2015.

Carry On: Sound Advice from Schneier on Security, John Wiley & Sons, 2013.

Liars and Outliers: Enabling the Trust that Society Needs to Thrive, John Wiley & Sons, 2012.

Cryptography Engineering (with Niels Ferguson and Tadayoshi Kohno), John Wiley & Sons, 2010.

Schneier on Security, John Wiley & Sons, 2008.

Beyond Fear: Thinking Sensibly about Security in an Uncertain World, Copernicus Books, 2003.

Practical Cryptography (with Niels Ferguson), John Wiley & Sons, 2003

Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons, 2000.

The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance (with David Banisar), John Wiley & Sons, 1997.

Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

The Twofish Encryption Algorithm (with John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson), John Wiley & Sons, 1996.

E-Mail Security, John Wiley & Sons, 1995

Protect Your Macintosh, Peachpit Press, 1994

Applied Cryptography, John Wiley & Sons, 1994.

Academic Publications

B. Schneier, "AI and Trust," *Communications of the ACM*, Online First, June 12, 2025, https://dl.acm.org/doi/10.1145/3737610.

B. Schneier, N. E. Sanders, D. Jemielniak, E. Begoli, A. Sadovnik, "3 Ways to Keep AI on Our Side: AI Researchers Can Draw Lessons from Cybersecurity, Robotics, and Astrobiology," *IEEE Spectrum*, v. 62, n. 4, April 2025.

B. Schneier, "Reimagining Democracy," *Common Knowledge*, v. 30, n. 3, 2024, pp. 354–358, https://doi.org/10.1215/0961754X-11416119.

J. Kelsey and B. Schneier, "Rational Astrologies and Security," *Rossfest Festschrift*, Frank Stajano, ed., 2025, pp. 171-175.

B. Schneier and A. Vance, ""Complexity Is the Worst Enemy of Security": Studying Cybersecurity Through the Lens of Organizational Complexity," *Management Information Systems Quarterly*, v. 49, n. 1, pp. 205-210, March 1, 2025.

C. Summerfield, L. Argyle, M. Bakker, T. Collins, E. Durmus, T. Eloundou, I. Gabriel, D. Ganguli, K. Hackenburg, G. Hadfield, L. Hewitt, S. Huang, H. Landemore, N. Marchal, A. Ovadya, A. Procaccia, M. Risse, B. Schneier, E. Seger, D. Siddarth, H. S. Sætra, M. H. Tessler, M. Botvinick, "How Will Advanced AI Systems Impact Democracy?," *arXiv:2409.06729 [cs.CY]*, August 27, 2024.

C. Porios, L. Guerin, and B. Schneier, "Assessing the Neutrality of Edits on Wikipedia," *Wiki Workshop (11th edition)*, June 20, 2024.

F. Heiding, B. Schneier, and A. Vishwanath, "AI Will Increase the Quantity—and Quality—of Phishing Scams," *Harvard Business Review*, May 30, 2024.

F. Heiding, B. Schneier, A. Vishwanath, J. Bernstein, P. S. Park, "Devising and Detecting Phishing Emails Using Large Language Models," *IEEE Access*, March 11, 2024.

B. Raghavan and B. Schneier, "A Bold New Plan for Preserving Online Privacy and Security: Decoupling Our Identities from Our Data and Actions Could Safeguard Our Secrets," *IEEE Spectrum*, December 2023.

N. E. Sanders, A. Ulinich, and B. Schneier, "Demonstrations of the Potential of AI-based Political Issue Polling," arXiv:2307.04781 [cs.CY], July 10, 2023.

J. Penney and B. Schneier, "Platforms, Encryption, and the CFAA: The Case of *WhatsApp v. NSO Group*," *Berkeley Technology Law Journal*, v. 36, n. 1, 2021.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, V. Teague, C. Troncoso, "Bugs in our Pockets: The Risks of Client-Side Scanning," arXiv:2110.07450 [cs.CR], October 14, 2021.

N. E. Sanders and B. Schneier, "Machine Learning Featurizations for AI Hacking of Political Systems," arXiv:2110.09231 [cs.CY], October 8, 2021.

H. Farrell and B. Schneier, "Rechanneling Beliefs: How Information Flows Hinder or Help Democracy," Stavros Niarchos Foundation SNF Agora Institute, Johns Hopkins, May 24, 2021.

B. Schneier, "The Coming AI Hackers," Belfer Center for Science and International Affairs, Harvard Kennedy School, April 2021.

G. Corn, J. Daskal, J. Goldsmith, C. Inglis, P. Rozenzweig, S. Sacks, B. Schneier, A. Stamos, V. Stewart, "Chinese Technology Platforms Operating in the United States: Assessing the Threat," *Joint Report of the National Security, Technology, and Law Working Group at the Hoover Institution at Stanford University and the Tech, Law & Security Program at American University Washington College of Law*, February 11, 2021.

R. S. S. Kumar, J. Penney, B. Schneier, K. Albert, "Legal Risks of Adversarial Machine Learning Research," arXiv:2006.16179.

N. Kim, T. Herr, and B. Schneier, "The Reverse Cascade: Enforcing Security on the Global IoT Supply Chain," *Atlantic Council*, June 2020.

K. Levy and B. Schneier, "Privacy Threats in Intimate Relationships," *Journal of Cybersecurity*, v. 6, n. 1, 2020.

M. Bourdeaux, G. Abiola, B. Edgar, J. Pershing J. Wang, M. Van Loon, B. Schneier, "Weaponizing Digital Health Intelligence," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, January 2020.

K. Albert, J. Penney, B. Schneier, R. Shankar, and S. Kumar, "Politics of Adversarial Machine Learning," *arXiv:2002.05648*, February 2020.

A. Adams, F. Ben-Youssef, B. Schneier, K. Murata, "Superheroes on Screen: Real Life Lessons for Security Debates," *Security Journal*, 2019.

H. Farrell, B. Schneier, "Common-Knowledge Attacks on Democracy," Berkman Klein Center Research Publication No. 2018-7, October 2018.

T. Herr, B. Schneier, and C. Morris, "Taking Stock: Estimating Vulnerability Rediscovery," *Belfer Cyber Security Project White Paper Series*, Harvard Kennedy School, March 7, 2017, http://dx.doi.org/10.2139/ssrn.2928758.

O. S. Kerr, B. Schneier, "Encryption Workarounds," *Georgetown Law Journal*, v. 106, 2017, p. 989-1019.

S. Shackelford, B. Schneier, M. Sulmeyer, A. Boustead, B. Buchanan, A. Craig, T. Herr, and J. Z. Malekos Smith, "Making Democracy Harder to Hack: Should Elections Be Classified as 'Critical Infrastructure'?," *University of Michigan Journal of Law Reform*, v. 50, n. 3, Spring 2017, pp. 629–668.

J. Quinn and B. Schneier, "A Proportional Voting System for Awards Nominations Resistant to Voting Blocs," *Voting Matters*, n. 31, to appear.

B. Schneier, K. Seidel, S. Vijayakumar, "A Worldwide Survey of Encryption Products," Berkman Center Report, February 11, 2016.

U. Gasser, M. G. Olsen, N. Gertner, D. Renan, J. Goldsmith, J. Sanchez, S. Landau, B. Schneier, J. Nye, L. Schwartztol, D. R. O'Brien, J. Zittrain, "Don't Panic: Making Progress on the 'Going Dark' Debate," Berkman Center Report, February 1, 2016.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter, D. J. Weitzner, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity,* November 2015.

105 additional academic publications before January 2015.

Published Articles

"The Age of Integrity," *IEEE Security & Privacy*, June 17, 2025.

"Will AI Take Your Job? the Answer Could Hinge on the 4 S's of the Technology's Advantages over Humans," *The Conversation*, June 16, 2025.

"Testimony to the House Committee on Oversight and Government Reform," *House Committee on Oversight and Government Reform*, June 4, 2025.

"Why Take9 Won't Improve Cybersecurity," *Dark Reading*, May 28, 2025.

"The Voter Experience," *Harvard Kennedy School Ash Center*, May 14, 2025.

"AI-Generated Law Isn't Necessarily a Terrible Idea," *Foreign Policy*, May 14, 2025.

"How the Signal Chat Leak Makes the NSA's Job Harder," *Foreign Policy*, March 28, 2025.

"Web 3.0 Requires Data Integrity," *Communications of the ACM*, March 24, 2025.

"What the UK Wants from Apple Will Make Our Phones Less Safe," *Foreign Policy*, February 25, 2025.

"DOGE Is Hacking America," *Foreign Policy*, February 11, 2025.

"It's Time to Worry About DOGE's AI Plans," *The Atlantic*, February 10, 2025.

"AIs and Robots Should Sound Robotic," *IEEE Spectrum*, January 30, 2025.

"AI Will Write Complex Laws," *Lawfare*, January 16, 2025.

"AI Mistakes Are Very Different from Human Mistakes," *IEEE Spectrum*, January 13, 2025.

"Trust Issues," *Boston Review*, December 6, 2024.

"The Apocalypse That Wasn't: AI Was Everywhere in 2024's Elections, but Deepfakes and Misinformation Were Only Part of the Picture," *The Conversation*, December 4, 2024.

"Algorithms Are Coming for Democracy—but It's Not All Bad," *Wired*, November 27, 2024.

"The SEC Whistleblower Program Is Dominating Regulatory Enforcement," *The American Prospect*, October 18, 2024.

"AI Could Still Wreck the Presidential Election," The Atlantic, September 27, 2024.

"Israel's Pager Attacks Have Changed the World," The New York TImes, September 22, 2024.

"Let's Start Treating Cybersecurity Like It Matters," Defense One, August 2, 2024.

"The CrowdStrike Outage and Market-Driven Brittleness," Lawfare, July 25, 2024.

"The Hacking of Culture and the Creation of Socio-Technical Debt," *e-flux*, June 18, 2024.

"Using AI for Political Polling," *Harvard Kennedy School Ash Center*, June 11, 2024.

"Indian Election Was Awash in Deepfakes—but AI Was a Net Positive for Democracy," *The Conversation*, June 7, 2024.

"How Online Privacy Is Like Fishing," *IEEE Spectrum*, June 4, 2024.

"How AI Will Change Democracy," *Cyberscoop*, May 28, 2024.

"Seeing Like a Data Structure," *Harvard Kennedy School Belfer Center*, May 25, 2024.

"Lattice-Based Cryptosystems and Quantum Cryptanalysis," *Communications of the ACM*, May 25, 2024.

"LLMs' Data-Control Path Insecurity," *Communications of the ACM*, May 12, 2024.

"AI and Trust," *The Herald Business*, April 30, 2024.

"It's the End of the Web as We Know It," *The Atlantic*, April 24, 2024.

"Backdoor in XZ Utils That Almost Happened," *Lawfare*, April 9, 2024.

"In Memoriam: Ross Anderson, 1956-2024," *Communications of the ACM*, April 9, 2024.

"Public AI as an Alternative to Corporate AI," *New America*, March 14, 2024.

"Let's Not Make the Same Mistakes with AI That We Made with Social Media," *MIT Technology Review*, March 13, 2024.

"How Public AI Can Strengthen Democracy," *Brookings*, March 4, 2024.

"How the 'Frontier' Became the Slogan of Uncontrolled AI," *Jacobin*, February 28, 2024.

"Building a Cyber Insurance Backstop Is Harder Than It Sounds," *Lawfare*, February 26, 2024.

"CFPB's Proposed Data Rules Would Improve Security, Privacy and Competition," *Cyberscoop*, January 26, 2024.

"Don't Talk to People Like They're Chatbots," *Atlantic*, January 17, 2024.

"AI Needs to Be Both Trusted and Trustworthy," *Wired*, January 1, 2024.

"AI Could Improve Your Life by Removing Bottlenecks between What You Want and What You Get," *The Conversation*, December 21, 2023.

"The Internet Enabled Mass Surveillance. AI Will Enable Mass Spying," *Slate*, December 4, 2023.

"AI and Trust," *Harvard Kennedy School Belfer Center*, December 1, 2023.

"Ten Ways AI Will Change Democracy," *Harvard Kennedy School Ash Center*, November 6, 2023.

"Trustworthy AI Means Public AI," *IEEE Security & Privacy*, November 1, 2023.

"Who's Accountable for AI Usage in Digital Campaign Ads? Right Now, No One," *Harvard Kennedy School Ash Center*, October 11, 2023.

"AI Disinformation Is a Threat to Elections—Learning to Spot Russian, Chinese and Iranian Meddling in Other Countries Can Help the Us Prepare for 2024," *The Conversation*, September 29, 2023.

"The A.I. Wars Have Three Factions, and They All Crave Power," *New York Times*, September 28, 2023.

"Robots Are Already Killing People," *Atlantic*, September 6, 2023.

"Nervous About ChatGPT? Try ChatGPT With a Hammer," *Wired*, August 29, 2023.

"Re-Imagining Democracy for the 21st Century, Possibly Without the Trappings of the 18th Century," *The Conversation*, August 7, 2023.

"Six Ways That AI Could Change Politics," *MIT Technology Review*, July 28, 2023.

"Can You Trust AI? Here's Why You Shouldn't," *The Conversation*, July 20, 2023.

"AI Microdirectives Could Soon Be Used for Law Enforcement," *Slate*, July 17, 2023.

"Will AI Hack Our Democracy?," *Harvard Kennedy School Magazine*, July 14, 2023.

"Snowden Ten Years Later," *RFC 9446*, July 1, 2023.

"Artificial Intelligence Can't Work Without Our Data," *Politico*, June 29, 2023.

"AI Could Shore Up Democracy—Here's One Way," *The Conversation*, June 20, 2023.

"Build AI by the People, for the People," *Foreign Policy*, June 12, 2023.

"Big Tech Isn't Prepared for A.I.'s Next Chapter," *Slate*, May 30, 2023.

"Rethinking Democracy for the Age of AI," *Cyberscoop*, May 10, 2023.

"Can We Build Trustworthy AI?," *Gizmodo*, May 4, 2023.

"Just Wait Until Trump Is a Chatbot," *The Atlantic*, April 28, 2023.

"How Artificial Intelligence Can Aid Democracy," *Slate*, April 21, 2023.

"Brace Yourself for a Tidal Wave of ChatGPT Email Scams," *Wired*, April 4, 2023.

"How AI Could Write Our Laws," *MIT Technology Review*, March 14, 2023.

"Why the U.S. Should Not Ban TikTok," *Foreign Policy*, February 23, 2023.

"Everything Is Hackable," *Slate*, February 10, 2023.

"We Don't Need to Reinvent Our Democracy to Save It from AI," *Harvard Kennedy School Belfer Center*, February 9, 2023.

"The Big Idea: Bruce Schneier," *Whatever*, February 7, 2023.

"Opinion: What Peter Thiel and the 'Pudding Guy' revealed," *CNN*, February 7, 2023.

"How ChatGPT Hijacks Democracy," *New York Times*, January 15, 2023.

"How to Decarbonize Crypto," *Atlantic*, December 6, 2022.

"Centralized vs. Decentralized Data Systems—Which Choice Is Best?" *VentureBeat*, September 12, 2022.

"NIST's Post-Quantum Cryptography Standards Competition," *IEEE Security & Privacy*, August 7, 2022.

"When Corporate Interests and International Cyber Agreements Collide," *Cipher Brief*, May 5, 2022.

"Why Vaccine Cards Are So Easily Forged," *The Atlantic*, March 8, 2022.

"Letter to the US Senate Judiciary Committee on App Stores," January 31, 2022.

"Robot Hacking Games," *IEEE Security & Privacy*, January 1, 2022.

"How to Cut Down on Ransomware Attacks Without Banning Bitcoin," *Slate*, June 17, 2021.

"Hacked Drones and Busted Logistics Are the Cyber Future of Warfare," *Brookings TechStream*, June 5, 2021.

"Russia's Hacking Success Shows How Vulnerable the Cloud Is," *Foreign Policy*, May 24, 2021.

"'Grassroots' Bot Campaigns Are Coming. Governments Don't Have a Plan to Stop Them.," *The Washington Post*, May 20, 2021.

"Hackers Used to Be Humans. Soon, AIs Will Hack Humanity," *Wired*, April 19, 2021.

"Bitcoin's Greatest Feature Is Also Its Existential Threat," *Wired*, March 9, 2021.

"Illuminating SolarStorm: Implications for National Strategy and Policy," *Aspen Institute*, March 04, 2021.

"Why Was SolarWinds So Vulnerable to a Hack?" *New York Times*, February 23, 2021.

"The Government Will Guard Biden's Peloton from Hackers. What About the Rest of Us?," *The Washington Post*, February 2, 2021.

"The Solarwinds Hack Is Stunning. Here's What Should Be Done," *CNN*, January 5, 2021.

"Audio: Firewalls Don't Stop Dragons Podcast," *Firewalls Don't Stop Dragons*, December 28, 2020.

"Audio: The Hack by Russia Is Huge. Here's Why It Matters.," *MPR News*, December 28, 2020.

"Review of Data and Goliath (German)," *Nerdhalla*, December 27, 2020.

"Video: The Most Consequential Cyber-Attack in History Just Happened. What Now?," *LA Times*, December 24, 2020.

"Video: AshbrookLIVE #14 – Bruce Schneier," *AshbrookLIVE*, December 24, 2020.

"Audio: Full Disclosure with Bruce Schneier," *BarCode*, December 20, 2020.

"Audio: How Your Digital Footprint Makes You the Product," *TechSequences*, December 16, 2020.

"Video: Hack in the Box Security Conference Keynote Interview," *Hack In The Box Security Conference*, December 3, 2020.

"Video: Election Security: Securing the Vote While Securing the System," *The Legal Edition*, November 19, 2020.

"#ISC2Congress: Modern Security Pros Are Much More than Technologists, Says Bruce Schneier," *Infosecurity*, November 18, 2020.

"Audio: Ballot Question 1: Risks & Regulations Regarding Right to Repair," *Pioneer Institute*, October 13, 2020.

"Audio: We Live in a Security and Privacy World that Science Fiction Didn't Predict," *OWASP PDX Podcast*, October 4, 2020.

"How Amazon and Walmart Could Fix IoT Security," *Data Breach Today*, June 26, 2020.

"The Cyberflâneur #29: Bruce Schneier," *The Syllabus*, June 16, 2020.

"Audio: Interview with Bruce Schneier for Blockchain Rules Podcast Series," *Blockchain Rules Podcast*, June 16, 2020.

"Audio: Is Contact Tracing Dumb? False Positives, Loss of Trust, and an Uncertain Path Back to Normalcy," *Policy Punchline*, June 2, 2020.

"Coronavirus, il guru Bruce Schneier: «Le app di contact tracing? Inutili. Margini di errore troppo alti»," *Open*, June 2, 2020.

"Audio: Click Here to Kill Everybody: Security and Survival in a Hyper-connected World," *Policy Punchline*, May 29, 2020.

"Audio: Bruce Schneier on Truth, Reality, and Contact Tracing," *Reality 2.0*, May 27, 2020.

"Video: Public Interest Technologists—Interview with Bruce Schneier and Jon Callas," *Cyber Cyber Cyber Cyber*, May 19, 2020.

"The Public Good Requires Private Data," *Foreign Policy*, May 16, 2020.

"How Hackers and Spies Could Sabotage the Coronavirus Fight," *Foreign Policy*, February 28, 2020.

"Technologists vs. Policy Makers," *IEEE Security & Privacy*, January/February 2020.

"We're Banning Facial Recognition. We're Missing the Point.," *The New York Times*, January 20, 2020.

"China Isn't the Only Problem With 5G," *Foreign Policy*, January 10, 2020.

"Bots Are Destroying Political Discourse As We Know It," *The Atlantic*, January 7, 2020.

"We Must Bridge the Gap Between Technology and Policymaking. Our Future Depends on It," *World Economic Forum*, November 12, 2019.

"Every Part of the Supply Chain Can Be Attacked," *The New York Times*, September 25, 2019.

"The Real Threat from China Isn't 'Spy Trains,'" *CNN*, September 21, 2019.

"What Digital Nerds and Bio Geeks Have to Worry About," *CNN*, September 13, 2019.

"The Myth of Consumer Security," *Lawfare*, August 26, 2019.

"8 Ways to Stay Ahead of Influence Operations," *Foreign Policy*, August 12, 2019.

"Attorney General William Barr on Encryption Policy," *Lawfare*, July 23, 2019.

"We Must Prepare for the Next Pandemic," *The New York Times*, June 17, 2019.

"AI Has Made Video Surveillance Automated and Terrifying," *Motherboard*, June 13, 2019.

"AI Can Thrive in Open Societies," *Foreign Policy*, June 13, 2019.

"When Fake News Comes to Academia," *Lawfare*, May 24, 2019.

"Democracy's Dilemma," *Boston Review*, May 15, 2019.

"Russia's Attacks on Our Democratic Systems Call for Diverse Countermeasures," *The Hill*, May 7, 2019.

"Toward an Information Operations Kill Chain," *Lawfare*, April 24, 2019.

"A New Privacy Constitution for Facebook," *OneZero*, March 8, 2019.

"Cybersecurity for the Public Interest," *IEEE Security & Privacy*, January/February 2019.

"There's No Good Reason to Trust Blockchain Technology," *Wired*, February 6, 2019.

"The Public-Interest Technologist Track at the RSA Conference," *RSA Conference Blogs*, January 29, 2019.

"Defending Democratic Mechanisms and Institutions against Information Attacks," *Defusing Disinfo*, January 28, 2019.

"Evaluating the GCHQ Exceptional Access Proposal," *Lawfare*, January 17, 2019.

"Machine Learning Will Transform How We Detect Software Vulnerabilities," *SecurityIntelligence*, December 18, 2018.

"The Most Damaging Election Disinformation Campaign Came From Donald Trump, Not Russia," *Motherboard*, November 19, 2018.

"Surveillance Kills Freedom By Killing Experimentation," *Wired*, November 16, 2018.

"Information Attacks on Democracies," *Lawfare*, November 15, 2018.

"We Need Stronger Cybersecurity Laws for the Internet of Things," *CNN*, November 9, 2018.

"Nobody's Cellphone Is Really That Secure," *The Atlantic*, October 26, 2018.

"Internet Hacking Is About to Get Much Worse," *New York Times*, October 11, 2018.

"Cryptography after the Aliens Land," *IEEE Security & Privacy*, September/October 2018.

"Don't Fear the TSA Cutting Airport Security. Be Glad That They're Talking about It," *Washington Post*, August 17, 2018.

"Censorship in the Age of Large Cloud Providers," *Lawfare*, June 7, 2018.

"Why the FBI Wants You to Reboot Your Router — and Why That Won't Be Enough Next Time," *The Washington Post*, June 6, 2018.

"Data Protection Laws Are Shining a Needed Light on a Secretive Industry," *The Guardian*, June 1, 2018.

"What 'Efail' Tells Us About Email Vulnerabilities and Disclosure," *Lawfare*, May 24, 2018.

"Banning Chinese Phones Won't Fix Security Problems with Our Electronic Supply Chain," *The Washington Post*, May 8, 2018.

"American Elections Are Too Easy to Hack. We Must Take Action Now," *The Guardian*, April 18, 2018.

"It's Not Just Facebook. Thousands of Companies are Spying on You," *CNN*, March 26, 2018.

"Artificial Intelligence and the Attack/Defense Balance," *IEEE Security & Privacy*, March/April 2018.

"Can Consumers' Online Data Be Protected?," *CQ Researcher*, February 9, 2018.

"How to Fight Mass Surveillance Even Though Congress Just Reauthorized It," *The Washington Post*, January 25, 2018.

"The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018.

"The Security of Pretty Much Every Computer on the Planet Has Just Gotten a Lot Worse," *CNN*, January 5, 2018.

"How the Supreme Court Could Keep Police From Using Your Cellphone to Spy on You," *The Washington Post*, November 27, 2017.

"Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection," , November 1, 2017.

"Don't Waste Your Breath Complaining to Equifax about Data Breach ," *CNN*, September 11, 2017.

"IoT Security: What's Plan B?," *IEEE Security & Privacy*, September/October 2017.

"'Twitter and Tear Gas' Looks at How Protest Is Fueled and Crushed by the Internet," *Motherboard*, July 11, 2017.

"Why the NSA Makes Us More Vulnerable to Cyberattacks," *Foreign Affairs*, May 30, 2017.

"Who Are the Shadow Brokers?," *The Atlantic*, May 23, 2017.

"What Happens When Your Car Gets Hacked?," *The New York Times*, May 19, 2017.

"Why Extending Laptop Ban Makes No Sense," *CNN*, May 16, 2017.

"The Next Ransomware Attack Will Be Worse than WannaCry," *The Washington Post*, May 16, 2017.

"Three Lines of Defense against Ransomware Attacks," *New York Daily News*, May 15, 2017.

"Online Voting Won't Save Democracy," *The Atlantic*, May 10, 2017.

"Who Is Publishing NSA and CIA Secrets, and Why?," *Lawfare*, April 27, 2017.

"The Quick vs the Strong: Commentary on Cory Doctorow's *Walkaway*," *Crooked Timber*, April 26, 2017.

"Infrastructure Vulnerabilities Make Surveillance Easy," *Al Jazeera*, April 11, 2017.

"Snoops May Soon Be Able to Buy Your Browsing History. Thank the US Congress," *The Guardian*, March 30, 2017.

"Puzzling out TSA's Laptop Travel Ban," *CNN*, March 22, 2017.

"Security Orchestration for an Uncertain World," *SecurityIntelligence*, March 21, 2017.

"How to Keep Your Private Conversations Private for Real," *The Washington Post*, March 8, 2017.

"Botnets of Things," *MIT Technology Review*, March/April 2017.

"Click Here to Kill Everyone," *New York Magazine*, January 27, 2017.

"Why Proving the Source of a Cyberattack is So Damn Difficult," *CNN*, January 5, 2017.

"Class Breaks," *Edge*, December 30, 2016.

"U.S. Elections Are a Mess, Even Though There's No Evidence This One Was Hacked," *The Washington Post*, November 23, 2016.

"Testimony at the U.S. House of Representatives Joint Hearing 'Understanding the Role of Connected Devices in Recent Cyber Attacks,'" November 16, 2016.

"American Elections Will Be Hacked," *The New York Times*, November 9, 2016.

"Your WiFi-Connected Thermostat Can Take Down the Whole Internet. We Need New Regulations.," *The Washington Post*, November 3, 2016.

"Lessons From the Dyn DDoS Attack," *SecurityIntelligence*, November 1, 2016.

"Cybersecurity Issues for the Next Administration," *Time*, October 13, 2016.

"We Need to Save the Internet from the Internet of Things," *Motherboard*, October 6, 2016.

"How Long Until Hackers Start Faking Leaked Documents?," *The Atlantic*, September 13, 2016.

"Someone Is Learning How to Take Down the Internet," *Lawfare*, September 13, 2016.

"Stop Trying to Fix the User," *IEEE Security & Privacy*, September/October 2016.

"New Leaks Prove It: The NSA Is Putting Us All at Risk to Be Hacked," *Vox*, August 24, 2016.

"Hackers Are Putting U.S. Election at Risk," *CNN*, July 28, 2016.

"By November, Russian Hackers Could Target Voting Machines," *The Washington Post*, July 27, 2016.

"The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters," *Motherboard*, July 25, 2016.

"Credential Stealing as Attack Vector," *Xconomy*, April 20, 2016.

"The Value of Encryption," *The Ripon Forum*, April 2016.

"Can You Trust IRS to Keep Your Tax Data Secure?," *CNN*, April 13, 2016.

"Your iPhone Just Got Less Secure. Blame the FBI.," *The Washington Post*, March 29, 2016.

"Cryptography Is Harder Than It Looks," *IEEE Security & Privacy*, January/February 2016.

"Data Is a Toxic Asset, So Why Not Throw It Out?," *CNN*, March 1, 2016.

"A 'Key' for Encryption, Even for Good Reasons, Weakens Security," *The New York Times Room for Debate*, February 23, 2016.

"Why You Should Side With Apple, Not the FBI, in the San Bernardino iPhone Case," *The Washington Post*, February 18, 2016.

"Candidates Won't Hesitate to Use Manipulative Advertising to Score Votes," *The Guardian*, February 4, 2016.

"The Internet Of Things Will Be The World's Biggest Robot," *Forbes*, February 2, 2016.

"Security vs. Surveillance," *Don't Panic: Making Progress on the 'Going Dark' Debate*, February 1, 2016.

"When Hacking Could Enable Murder," *CNN*, January 26, 2016.

"How an Overreaction to Terrorism Can Hurt Cybersecurity," *MIT Technology Review*, January 25, 2016.

"The Internet of Things That Talk About You Behind Your Back," *Motherboard*, January 8, 2016.

"The Risks—and Benefits—of Letting Algorithms Judge Us," *CNN*, January 6, 2016.

"How the Internet of Things Limits Consumer Choice," *The Atlantic*, December 24, 2015.

"Can Laws Keep Up with Tech World?," *CNN*, December 21, 2015.

"The Automation of Reputation," *Edge.org*, November 5, 2015.

"The Rise of Political Doxing," *Motherboard*, October 28, 2015.

"Face Facts about Internet Security," *CNN*, October 23, 2015.

"The Era Of Automatic Facial Recognition And Surveillance Is Here, *Forbes*, September 29, 2015.

"Stealing Fingerprints," *Motherboard*, September 29, 2015.

"VW Scandal Could Just Be the Beginning," *CNN*, September 28, 2015.

"Living in Code Yellow," *Fusion*, September 22, 2015.

"Hacking Team, Computer Vulnerabilities, and the NSA," *Georgetown Journal of International Affairs*, September 13, 2015.

"Is It OK to Shoot Down a Drone over Your Backyard?" *CNN*, September 9, 2015.

"The Meanest Email You Ever Wrote, Searchable on the Internet," *Atlantic*, September 8, 2015.

"Should Some Secrets Be Exposed?" *CNN*, July 7, 2015.

452 additional published articles before July 2015.

Patents

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for educational testing," U.S. Patent 8,725,060, May 13, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers," U.S. Patent 8,712,920, April 29, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, "Conditional purchase offer management system," U.S. Patent 8,700,481, April 15, 2014.

J.S. Walker, B. Schneier, M.M Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, "Method and apparatus for promoting the selection and use of a transaction card," U.S. Patent 8,632,005, January 21, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce," U.S. Patent 8,626,667, January 7, 2014.

77 additional patents before 2014.

Previous Declarations and Depositions

British Telecommunications PLC and BT Americas, Inc. v. Fortinet, Inc., In JAMS Arbitration, Case No. 5425002197. Fact witness for British Telecommunications, Proskauer Rose LLP, attorneys. Deposition, report, and testification (2025).

Anibal Rodriguez, Sal Cataldo, Julian Santiago, and Susan Lynn, individually and on behalf of all similarly situated v. Google LLC, Case No. 4:20-cv-04688-RS, United States District Court for the Northern California District. Expert witness for Brown et. al., Susman Godfrey LLP, attorneys. Declarations and deposition (2023).

Chasom Brown, William Byatt, Jeremy David, Christopher Castillo, and Monique Trujillo, individually and on behalf of all similarly situated v. Google LLC, Case No. 4:20-cv-03664-YGR-SVK, United States District Court for the Northern California District. Expert witness for Brown et. al., Susman Godfrey LLP, attorneys. Declarations and deposition (2022).

Mon Cheri Bridals, LLC and Maggie Sottero Designs, LLC v. Cloudflare, Inc., Case No. 2:18-cv-09453-MWF-AS, United States District Court for the Central District of California. Expert witness for Cloudflare, Inc., Fenwick & West, LLP, attorneys. Declarations (2020 and 2021).

17 additional declarations and depositions before 2021.

EXHIBIT U

CAUSE NO. 348-362718-25

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

EXPERT REPORT OF KYLE BERGER

Kyle Berger provides the following expert report in the above-styled lawsuit.

1. Introduction

I am the Chief Technology Officer for Grapevine-Colleyville Independent School District ("GCISD"). As Chief Technology Officer my duties and responsibilities include direct the technology vision and strategy for the school district. I oversee the entire Technology Department, including network infrastructure, data management, cybersecurity, and operational support. A detailed description of my experience and qualifications is attached hereto as Exhibit 1.

I have been asked to (1) opine on whether the materials at issue in this lawsuit that were withheld from disclosure by GCISD "relates to computer network security, to restricted information under Section 2059.055, or to the design, operation, or defense of a computer network" (see Tex. Gov't Code §552.139(a)), and (2) comment on the opinions expressed in the Expert Report of Bruce Schneier.

I am not being compensated for this report over and above my normal salary as GCISD's Chief Technology Officer.

2. Opinion

The GCISD network is founded on a dedicated, high-capacity fiber optic backbone spanning over 45 miles, which provides resilient connectivity to all 24 instructional and operational facilities across the district community. This highly dense infrastructure supports a 1:1 digital learning environment, managing in excess of 45,000 unique device connections daily for over 16,000 assigned end-users (students and staff) across both comprehensive wired and high-density wireless systems. GCISD utilizes a robust hybrid operational model, maintaining two distinct physical data center facilities integrated seamlessly with multi-tenant cloud services, all managed with a critical 24/7/365 operational commitment to ensure continuous availability.

The network is engineered to support all critical district functions, including high-bandwidth instructional services, Voice over IP (VoIP) telephony, Safety and Security systems (surveillance and access control), and administrative Enterprise Resource Planning (ERP). To protect this mission-critical environment, the network employs a defense-in-depth approach utilizing top-tier firewall systems and comprehensive cybersecurity protection tools specifically compliant with student data regulations. The overall complexity of the network is significantly elevated by its capacity to support and securely manage global virtual learning platforms, necessitating sophisticated remote access infrastructure and bandwidth optimization for a geographically distributed user base.

GCISD, as a recipient of federal funding, is subject to the Children's Internet Protection Act ("CIPA"), Pub. L. No. 106-554, 114 Stat. 2763 (2000), which was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the internet. This legislative requirement, which must be fulfilled for GCISD to remain eligible for federal funding, forces the adoption of core technology for GCISD's computer network, including content filtering. As GCISD's Chief Technology Officer, part of my duties and responsibilities include

making sure that the design and operation of GCISD's computer network complies with CIPA – importantly, relevant to the design or operation of GCISD's computer network, ***student email accounts and internet access are part of GCISD's computer network***.

Critical to GCISD's design or operation of its computer network, GCISD is required under CIPA to have blocking or filtering measures in place to address the following: access by minors to inappropriate matter on the internet; the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; unauthorized access, including so-called "hacking," and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal information regarding minors; and measures restricting minors' access to materials harmful to them. Beyond simple blocking, CIPA further requires schools to approve and publicly adopt an internet safety policy that covers restricting access to harmful content, ensuring safe communications, preventing unlawful online activities, and protecting student data. The filtering and monitoring systems provide the necessary auditing and enforcement tools to prove that this policy is actively implemented and adhered to across all devises used by students to access the internet.

As part of its efforts to comply with CIPA, GCISD has retained the services of third-party vendors Lightspeed Solutions and Gaggle.Net to create and implement appropriate blocking and filtering measures for its computer network. GCISD has service contracts with both Gaggle.Net and Lightspeed Solutions to provide filter/monitoring systems for GCISD's computer network. These systems are used as a tool to maximize the detection of unsafe, graphic, and/or obscene student communications and website content on school district devices. With Gaggle.Net, for example, search terms that implicate computer searches that indicate suicide ideation, or self-harm and threats of violence, or obscenity will result in email notifications to GCISD and immediate

emergency phone calls if necessary. Similarly, Lightspeed Solutions monitors students' online activity on GCISD's computer network by utilizing web content filtering technology to protect students from harmful online content – in other words, Lightspeed Solutions' filter technology blocks obscene material on any devise using GCISD's computer network.[1] Notably, GCISD does ***not*** customize the lists of keywords or phrases to be monitored; rather, these lists are solely created and maintained by the district's computer service providers Lightspeed Solutions and Gaggle.Net. Both vendors consider their lists to be proprietary.

To comply with CIPA, Gaggle.Net's system works by monitoring school provided accounts or devices for words and web searches that, for example, if discovered might prevent a predator from sending a 12-year-old student obscene pictures or other communications by email or Google docs. Similarly, in addition to blocking explicit material, Lightspeed Solutions' content filtering for CIPA compliance protects against malware, extremist propaganda, sites that promote eating disorders, and online threats that could compromise student data – as promoted on Lightspeed Solutions' website (see https://www.lightspeedsystems.com/solutions/security-compliance/cipa), GCISD's computer network infrastructure, in addition to students and staff, is holistically protected from online dangers with the Lightspeed Solutions filtering system.

When I say Lightspeed's filtering system "protects against malware and online threats," I mean it acts as a proactive gatekeeper that monitors, categorizes, and blocks high-risk traffic before exposure occurs. This reduces the likelihood of exploit delivery, phishing, or ransomware reaching endpoints and helps safeguard student data. How Lightspeed's filtering system helps defend K-12 (kindergarten – 12th grade) school environments against malware and cyberthreats includes:

[1] Content filtering solutions, such as Lightspeed Filter, are designed to function as the first line of defense, proactively preventing users from initiating connections with known malicious domains or downloading harmful content. Modern content filtering solutions has evolved from basic CIPA compliance tools into sophisticated security components akin to next-generation firewalls, capable of addressing the complex challenges of the contemporary threat landscape.

- The system blocks and detects attempts to access or search for known or potentially malicious websites or services, including those hidden in encrypted traffic through TLS inspection. This reduces the attack surface and improves both cybersecurity and digital safety posture.

- It integrates threat-intelligence feeds from multiple industry sources, including PhishTank, vxIntel, Internet Watch Foundation (IWF), and MI6, paired with Lightspeed's proprietary AI categorization engine to detect new and emerging threat domains and proactively block newly registered or uncategorized sites.

- It uses devise-level SmartAgents and extensions on Windows, Chrome, Mac, and iOS so filtering and threat prevention apply whether district-owned devices are on the school network or off-campus/home.

- It detects and blocks access to domain-sharing and file-hosting services frequently used to distribute malware, phishing pages, or inappropriate material, reducing risk across both cybersecurity and student-safety vectors.

- It blocks anonymizers and high-risk networks like TOR outright and continues filtering VPN traffic since enforcement occurs at the device level.

- Beyond blocking malicious sites, the monitoring and reporting of our system detects users activity, such as suspicious search terms, to identify users who are attempting to circumvent protections, evade filtering, and put compliance and security at risk.

Solutions like Lightspeed's filtering system provide end-to-end content filtering, offering critical protection against cyber risks and distractions. The system employs device-level agents to ensure comprehensive coverage across platforms such as Windows, macOS, and Chrome/Edge browsers, meaning protection follows the device regardless of whether it is on or off the campus network. This focus on coverage across all devices is functionally an evolution of the filtering system into a network-aware Endpoint Detection and Response (EDR) component, ensuring that infections acquired off-network do not compromise the district network upon reconnection. The Filter leverages specific, cybersecurity-focused categories to prevent users from accessing harmful content, including features designed to trigger immediate "internet lockouts" when malicious or harmful content is detected. This capability supports the containment phase of incident response, limiting the potential spread of malware. The accuracy of blocking is enhanced by the

incorporation of AI into filtering processes, which analyzes context to prevent the misclassification of legitimate educational resources. This precise, adaptive security posture minimizes false positives while maintaining robust protection, which helps ensure that technical controls support, rather than hinder, educational objections. Content Monitoring Systems (CMS), such as Gaggle Safety Management and Lightspeed Alert, fulfill the crucial cybersecurity role of internal detection. They analyze the contents of user-generated communications and files within school-issued platforms to identify threats that have bypassed perimeter filters or originated from compromised internal accounts.

Content Filtering Systems (CFS) and Content Monitoring Systems (CMS) are no longer specialized compliance tools but are mandatory, high-impact security layers essential for modern K-12 cyber defense. The CFS provides proactive, perimeter-level prevention, characterized by deep SSL/TLS inspection and integration with external threat intelligence, stopping threats before they enter the network. The CMS provides crucial internal visibility and defense against lateral movement and data exfiltration, functioning as the district's primary Data Loss Prevention (DLP) mechanism within cloud environments. Their combined, integrated application forms a cohesive security fabric, delivering protection that follows the student and device regardless of location, effectively mitigating complex threats like sophisticated phishing and ransomware.

GCISD operates proprietary content filtering and student monitoring systems (e.g., Lightspeed and Gaggle) as essential security controls mandated by federal and state law, including CIPA. Disclosure of the operational specifics of these systems – including algorithmic logic, proprietary detection rules, and specific trigger word lists – would not merely compromise security; it would instantly and irreparably nullify the effectiveness of these protective measures. The efficacy of any preventive security control is directly dependent upon the confidentiality of its

mechanism. Compelled disclosure transforms a necessary and effective security control into a known and exploitable vulnerability.

The request for information by the Knight Institute seeks highly sensitive operational data integral to the systems' ability to detect and prevent harm. The release of this confidential material poses immediate, foreseeable, and catastrophic harm across multiple domains. Operationally, it allows student or external malicious actors to craft communications, documents, and network activities specifically designed to bypass detection, directly enabling prohibited activities like cyber-bullying, accessing harmful content, or coordinating violence and self-harm. Disclosure would likely result in the nullification of CIPA compliance, the exposure of GCISD's critical infrastructure, and the destruction of the third-party vendors' valuable intellectual property.

GCISD's affirmative duty to protect students under federal laws such CIPA requires the implementation of safety policies that prevent "hacking" and "unlawful activities." If the compelled disclosure of the system's operational logic provides a guaranteed roadmap for circumvention, this disclosure itself fundamentally renders GCISD's CIPA policy inadequate, violating the federal mandate. The security mandate, therefore, functions as a legal shield against disclosure.

The monitoring and filtering systems (like Lightspeed and Gaggle) are the core technological mechanisms GCISD utilizes to fulfill CIPA's mandates. If the precise logic and trigger lists are known, students can easily adjust their communication patterns to guarantee non-detection, thereby achieving "unauthorized access" to harmful content and circumventing security policies. This outcome would instantaneously render GCISD non-compliant with federal law.

The monitoring system's ability to proactively flag and prevent incidents of self-harm, bullying violence, and drug use is entirely dependent on the secrecy of its detection thresholds.

The moment the specific algorithmic logic, scoring weights, and trigger word lists are publicized, malicious actors gain the perfect blueprint for evasion. If the system is designed to detect certain phrases associated with suicidal ideation, publishing those phrases allows a determined student – or a peer coercing them – to craft messages or documents that successfully bypass the filter. This deliberate circumvention guarantees non-detection, resulting in the catastrophic failure of GCISD's mandate duty to intervene.

The information sought by the Knight Institute provides far more than just content filtering insight; it offers critical intelligence regarding GCISD's overall network architecture, security layers, and defense protocols. Knowledge of the filtering system's operational parameters and vulnerabilities allows sophisticated malicious actors – including external hackers – to execute targeted, stealthy cyberattacks. For example, by understanding the specific monitoring traps set by the Lightspeed or Gaggle systems, a hacker can design phishing emails or ransomware deployment tools that are specifically tailored to bypass those known security filters. This outcome creates a known, actionable vulnerability. It directly facilitates "unauthorized access" and "hacking," placing GCISD in direct conflict with the anti-hacking mandates of CIPA. If the disclosure provides the key to unlocking the network for data exfiltration or ransomware deployment, GCISD will have actively compromised its own network security architecture, contravening its primary obligation to safeguard student data under the Family Educational Rights and privacy Act ("FERPA").

Section 552.139(a) of the Texas Government Code provides that "Information is excepted [from disclosure] if it is ***information that relates to*** computer network security, to restricted information under Section 2059.005, or to ***the design, operation, or defense of a computer network.***"

I have been informed by counsel that the courts have held that the phrase "relates to," as used in other sections of the Public Information Act, "is ***very broad***, encompassing even information that would not be 'relevant,' in the evidentiary sense, during litigation." *B.W.B. v. Eanes Indep. Sch. Dist.*, 2018 Tex. App. Lexis 223, *19 (Tex. App. – Austin 2018, no pet.) (emphasis added); see also *City of San Antonio v. Abbott*, 432 S.W.3d 429, 432 (Tex. App. – Austin 2014, pet. denied) ("The plain meaning of the phrase 'relates to' is 'to have a connection with, to refer to, or to concern.' In ordinary use, the phrase 'relates to' is ***very broad***.") (emphasis added).

To summarize, GCISD has "designed" and is "operating" its computer network by using/installing/incorporating the Gaggle.Net and Lightspeed Solutions filtering systems into the school district's computer network. Thus, interpreting the term "relates to" as used in Government Code §552.139(a) ***"very broadly,"*** the word lists and analytical reports created by Lightspeed Solutions and Gaggle.Net "relates to" the "design or operation" of GCISD's computer network and, therefore, should be excepted from disclosure to the Knight Institute pursuant to Tex. Gov't Code §552.139(a).

3. Response to Schneier Report

I first note that Mr. Schneier's report only addresses whether the disclosure of the information requested by the Knight Institute would increase the risk of a threat to GCISD's "computer network security." His report fails, however, to address whether the requested information "relates to" "the design, operation or defense of [GCISD's] computer network." See Tex. Gov't Code § 552.139 (excepting from disclosure information that "relates to" either "network security" or[2] "the design, operation or defense of a computer network"). As stated above,

[2] The word "or" as used in the Government Code is defined in the dictionary as "used as a function word to indicate an alternative." See *Webster's New Collegiate Dictionary* (1981) p. 800.

it is my opinion that the requested information ***does*** "relate to" the "the design, operation or defense of GCISD's computer network."

Next, I firmly reject Mr. Schneier's conclusion that disclosing the mechanisms used to monitor and trigger alerts would pose no threat to GCISD's computer network security. This conclusion relies on an overly narrow, traditional industry definition of "computer network security" that fails to account for the unique, mandatory, and integrated statutory duties placed on K-12 institutions regarding student safety and critical infrastructure protection.

Mr. Schneier, defines "computer network security" in the cybersecurity industry as defenses against unauthorized access by external actors, focusing on threats like cyberattacks, malware, and ransomware. He explicitly states that network security measures are not used to refer to defenses against unauthorized use by someone who already has authorized access.

Based on this distinction, Mr. Schneier concludes that releasing the requested information – the specific blocked websites and monitored keywords – concerns "impedes uses of its devices by authorized users" (students). Therefore, disclosing this information would not increase the likelihood of a computer security incident because it would not facilitate unauthorized access by external actors or lead to the harm or destruction of digital devices.

I counter this argument by asserting that in the K-12 environment, student safety monitoring (Content Monitoring Systems, or CMS) and network security (Content Filtering Systems, or CFS) have a strategic convergence, and compromising one fatally compromises the other, resulting in the "catastrophic failure" of mandated federal duties.

The key vulnerability created by disclosure is not merely allowing "unauthorized use" by enabling circumvention, which GCISD's duties explicitly prohibit. For example,

- Guaranteed Roadmap for Evasion: The requested information includes proprietary trigger word lists, specific algorithmic weights, and confidential machine learning model parameters. Disclosure of this core proprietary logic would provide a guaranteed roadmap for circumvention, resulting in non-detection.
- Circumvention Equates to Unauthorized Activity: CIPA mandates that GCISD must implement safety policies addressing "unauthorized access, including so-called 'hacking,' and other unlawful activities by minors online". If the precise detection logic and trigger lists are known, students can easily adjust their communication patterns to guarantee non-detection, thereby achieving "unauthorized access" to harmful content and circumventing security policies. This outcome instantly renders GCISD non-compliant with the federal anti-hacking mandate.
- Facilitating External Cyberattacks: The expert's view focuses solely on external intrusion. However, the defense brief argues that knowledge of the filter and monitoring system's operational parameters and vulnerabilities allows sophisticated malicious actors (external hackers) to execute targeted, stealthy cyberattacks. A hacker could design phishing emails or ransomware deployment tools specifically tailored to bypass those known security filters, which directly facilitates "unauthorized access" and "hacking". The system's ability to flag a student researching security bypass methods is simultaneously generating a critical Indicator of Compromise (IOC).
- Critical Infrastructure Information (CII): GCISD's network infrastructure, which holds massive amounts of PII for minors and serves as the primary early warning system for preventing imminent violence/self-harm, must be legally recognized as

Critical Infrastructure (CII). This status warrants protection under public records law exemptions that shield "detection mechanisms or security configurations". Publishing detection logic creates a systemic vulnerability comparable to publishing the blueprints or a power grid's security systems.

In conclusion, GCISD's use of Lightspeed and Gaggle is a layered security approach integrating proactive prevention (CFS) and internal detection (CMS). To separate the "security" function (external hacking prevention) from the "safety" function (internal threat detection) is to ignore the reality that these systems converge operationally and rely on the same proprietary detection logic. Disclosure would transform GCISD's security controls into a known, actionable vulnerability, directly contravening its non-delegable statutory duties to protect students and secure its digital environment.

4. Conclusion

To comply with CIPA, Gaggle.Net's system works by monitoring school provided accounts or devices for words and web searches that, for example, if discovered might prevent a predator from sending a 12-year-old student obscene pictures or other communications by email or Google docs. Similarly, in addition to blocking explicit material, Lightspeed Solutions' content filtering for CIPA compliance protects against malware, extremist propaganda, sites that promote eating disorders, and online threats that could compromise student data – as promoted on Lightspeed Solutions' website (see https://www.lightspeedsystems.com/solutions/security-compliance/cipa), GCISD's computer network infrastructure, in addition to students and staff, is holistically protected from online dangers with the Lightspeed Solutions filtering system.[3]

[3] In addition to CIPA compliance, Lightspeed Solutions' filtering system also assists GCISD with complying with other student internet safety regulations such as Texas Senate Bill 1893 (effective September 1, 2023), which "prohibit[s] the use of certain social media applications and services on devices owned or leased by governmental entities."

To summarize, GCISD has "designed" and is "operating" its computer network by using/installing/incorporating the Gaggle.Net and Lightspeed Solutions filtering systems into the school district's computer network. Thus, interpreting the term "relates to" as used in Government Code §552.139(a) ***"very broadly,"*** the word lists and analytical reports created by Lightspeed Solutions and Gaggle.Net "relates to" the "design or operation" of GCISD's computer network and, therefore, should be excepted from disclosure to the Knight Institute pursuant to Tex. Gov't Code §552.139(a).

Date: November 19, 2025.

Kyle Berger

EXHIBIT 1

Kyle R. Berger is eminently qualified to render expert opinions concerning **K-12 Educational Technology** and **K-12 Network and Cybersecurity** based on over 24 years of technology leadership experience within the Texas public education system. Mr. Berger currently serves as the Chief Technology Officer (CTO) for the Grapevine-Colleyville Independent School District (ISD), a district of 14,000 students in North Texas. He holds a Bachelor of Science in Information Systems from the University of Texas at Arlington.

Mr. Berger's extensive executive career includes serving as CTO for Grapevine -Colleyville ISD (4/17 - current) , Chief Technology officer for Duncanville ISD (1/14– 4/17), Executive Director of Technology at Cedar Hill ISD (10/12– 12/14), Executive Director of Technology Services for Alvarado ISD (10/03 – 10/12), and Project Manager for Keller ISD (12/00 – 10/03). This history demonstrates leadership over technology for districts ranging from approximately 3,400 students across eight locations to over 27,000 end users.

Expertise in K-12 Educational Technology

Mr. Berger is widely known as a **transformer of educational technology**. His experience highlights his deep involvement in integrating technology into instructional practices, managing large-scale system deployments, and developing digital content standards:

- **Instructional Oversight and Planning:** Across various districts, Mr. Berger has been responsible for long-range technology planning, establishing e-plans, and overseeing the district's instructional technology departments and training programs. He established instructional technology positions and corresponding training curriculum to facilitate the integration of technology into the classroom at Alvarado ISD.
- **System Deployment and Revitalization:** His service includes **vast experience in one-to-one deployment** and complete district revitalization. He oversaw the District Student Information System (SIS) and PEIMS (Public Education Information Management System), utilizing specific skills in **Skyward SMS** and serving as the President and Vice President of the Skyward State Steering Committee.
- **Standards and Interoperability:** Mr. Berger's work in the K-12 standardization process includes overseeing buildouts of standardized solutions for near seamless data exchange via SIF integrations. He has been involved with the **IMS standards movement** since 2016, driven by the need for streamlined digital content integration, and is a **member of the IMS Global Board of Directors**. His work in identity management processing has been featured in various publications for decreasing operational overhead while increasing performance.
- **Virtual Learning and Curriculum:** Mr. Berger currently oversees Grapevine-Colleyville ISD's Virtual School (Iuniversity Prep), which is the top virtual school in Texas and has ranked among the top five or two in the country for the past decade. He also oversaw the

addition of video-on-demand and distance learning equipment and evaluated technology curriculum to broaden class offerings. He has overseen the development of **State Championship Esports programs** for high school competitions.

Expertise in K-12 Network and Cyber Security

Mr. Berger's expertise in network infrastructure, physical security systems, and cybersecurity is demonstrated by his hands-on management of complex network environments, critical infrastructure projects, and participation in national security discussions:

- **National Cybersecurity Involvement:** Mr. Berger has been **invited to the White House** to discuss **K-12 cyber security at the national level** and to be part of National Education Planning and Cyber Security initiatives.
- **National Presenter on K12 CyberSecurity** : Mr. Berger has presented across the nation on K12 cyber security initiatives, as well as best pratices for student cyber protection.
- **Certified Cybersecurity Rubric Evaluator (CCRE)** :a certification for individuals who can help schools assess and improve their cybersecurity practices. The program is part of the Cybersecurity Coalition for Education. Mr Berger is a certified CCRE which conduct third-party evaluations for schools to assess their cybersecurity posture, identify vulnerabilities, and help them create a plan for improvement.
- **Network Infrastructure and Management:** He has **specific technical skills** in **WAN and Fiber network development**, **Data center design**, **CISCO**, and **Voice over IP (VoIP)**. He has overseen the expansion of the Wide Area Network (WAN) across multiple districts and supervised district-wide fiber backbone growth and placement.
- **Physical Security and Construction Management:** Mr. Berger is proficient in **Physical Security Systems** and **IT construction**. He has extensive experience in **Bond Program Management**.

Professional Recognition and Authority

Mr. Berger's expertise is recognized nationally and internationally, underscoring his position as a leading authority in the field:

- He is a recipient of multiple prestigious awards, including the **Technology Director of the Year for Texas** (2009), the **2020 National Edtech Leadership Winner**, and the Institutional Leadership Award for interoperability.
- In 2023, he was named one of 16 nationwide by the **COSN Impact 30 Award** as a leader impacting educational technology and leading change into the future. He has also been recognized as a Top K-12 IT Influencer 2022 and one of the Top 100 Influencers in Edtech by Edtechdigest.

- Mr. Berger serves as a member of several corporate advisory boards, including the **Google Board of Advisors**, **Cisco Board of Advisors**, **Lenovo Board of Advisors**,**Gradiant Cyber Advisory Board, Newline Customer Advisory Board, Bluum Advisory Board** and propr **Dell Board of Advisors, HP Board of Advisors**.
- His work has been featured in educational technology magazines, industry case studies, and published books since 2005. He is a global IT presenter, presenting at all major industry conferences across the US and globally as part of a US delegation to Japan for K12 Technology innovation and collaboration.

Through this extensive background in strategic planning, large-scale deployment, infrastructure development, and policy leadership, Kyle Berger demonstrates the comprehensive knowledge required to offer expert analysis on the complexities of K-12 educational technology and network and cybersecurity systems.

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: 110691845
Filing Code Description: Motion (No Fee)
Filing Description: Plaintiff's Motion for Summary Judgment
Status as of 2/2/2026 9:19 AM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Lucas ChristopherHenry		lhenry@abernathy-law.com	1/30/2026 6:50:13 PM	SENT
Charles J.Crawford		ccrawford@abernathy-law.com	1/30/2026 6:50:13 PM	SENT
Kimberly Escamilla		kescamilla@abernathy-law.com	1/30/2026 6:50:13 PM	SENT
Laura Ball		lball@abernathy-law.com	1/30/2026 6:50:13 PM	SENT
Peter Steffensen		psteffensen@smu.edu	1/30/2026 6:50:13 PM	SENT
Jennifer Jones		jennifer.jones@knightcolumbia.org	1/30/2026 6:50:13 PM	SENT
Katie Fallow		katie.fallow@knightcolumbia.org	1/30/2026 6:50:13 PM	SENT
Thomas Leatherbury		tom@tsleatherburylaw.com	1/30/2026 6:50:13 PM	SENT
Kiran Wattamwar		Kiran.Wattamwar@knightcolumbia.org	1/30/2026 6:50:13 PM	SENT