FILED
TARRANT COUNTY
1/30/2026 12:21 PM
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 MOTION FOR SUMMARY JUDGMENT

Pursuant to Tex. R. Civ. P. 166a, Defendant Grapevine-Colleyville Independent School District ("GCISD"), files the following motion for summary judgment seeking dismissal of Plaintiff's claims to remedy alleged violations of the Texas Public Information Act.

I. INTRODUCTION

1. In March 2023 Plaintiff Knight First Amendment Institute at Columbia University ("Knight") sent a Texas Public Information Act request to GCISD asking for "records related to the District's use of surveillance systems to monitor students' activity on school-issued devises and software." Knight subsequently clarified and/or narrowed its request twice.

2. In response to Knight's requests, GCISD, as allowed by law, sought an Attorney General opinion on whether some or all of the requested information is exempt from disclosure under Tex. Gov't Code §552.139.[1] In three separate written decisions, the Attorney General determined that the majority of the requested records were exempt from disclosure under section 552.139 and that GCISD "***must*** withhold the information." In compliance with the Attorney

[1] Section 552.139(a) excepts from disclosure information that "relates to computer network security, to restricted information under Section 2059.055, or to the design, operation, or defense of a computer network."

General's decisions, GCISD has withheld several documents and has also produced 824 heavily redacted emails.

3. Not satisfied with the Attorney General's decisions and GCISD's subsequent withholding and redacted production, Knight filed the instant lawsuit seeking a writ of mandamus "compelling [GCISD] to disclose all responsive information." In support of its request for mandamus relief, Plaintiff's Original Petition alleges that:

> (1) "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";
>
> (2) "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";
>
> (3) "Finally, the Knight Institute is entitled to a fee waiver. Tex. Gov't Code §552.267(a)."

See Plaintiff's Original Petition, ¶¶ 42-44. Knight also asks for its attorney's fees. Id. at ¶ 47.

4. In response, GCISD has filed a general denial and asserted the following two affirmative defenses:

> (1) The redacted emails produced by Defendant to Plaintiff about which Plaintiff complains of in Plaintiff's Original 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.
>
> (2) 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).

5. As further detailed below, the information requested by Knight, as correctly determined by the Attorney General, "relates to computer network security or the design,

operation, or defense of GCISD's computer network" and, as such, this information has been properly withheld from disclosure under section 552.139 as a matter of law. For this reason, the Court should enter summary judgment in GCISD's favor dismissing all of Knight's claims for relief, including (1) Knight's request for a writ of mandamus requiring production of the withheld and/or redacted information, (2) Knight's request for attorney's fees, and (3) Knight's request for a fee waiver.

II.
SUMMARY JUDGMENT EVIDENCE

6. GCISD's motion relies on the following summary judgment evidence:

Exhibit A – Declaration of Paula Barbaroux, plus attachments[2]

Exhibit B – Declaration of Kyle Berger, plus attachment

Exhibit C – Declaration of Jeff Patterson

III.
UNDISPUTED MATERIAL FACTS

7. According to Plaintiff's Original Petition, Knight "is a not-for-profit corporation based in Columbia University in New York, New York. Knight defends the freedoms of speech and 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." Plaintiff's Original Petition, ¶ 5.

[2] In addition to the attachments to the Barbaroux Declaration, GCISD will submit the documents and unredacted emails that the Attorney General determined must be withheld from disclosure to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order. See Tex. Gov't Code § 552.3221 (information at issue may be filed with court for *in camera* inspection "as is necessary for the adjudication of the case," and on receipt of information the court shall enter an order that prevents release to or access by any person other than the court, a reviewing court of appeals, or parties permitted to inspect information pursuant to a protective order).

8. "Knight 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." Plaintiff's Original Petition, ¶ 15.

9. "As part of its ongoing work on free speech and surveillance, Knight seeks to learn more about how schools use A.I.-powered technology to restrict and monitor students' activity on school-issued devices and applications. 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. ... There is a widespread concern that school districts' use of these technologies causes serious privacy, expressive, associational, and equity harms." Plaintiff's Original Petition, ¶¶ 17, 18.

10. "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.[3] The Center for Democracy & Technology's report on online surveillance found that some schools block, filter, or monitor LGBTQ+ and race-related content." Plaintiff's Original Petition, ¶ 19.

11. As part of its investigation into these issues, on March 29, 2023, Knight sent a Texas Public Information Act request to GCISD for records related to its use of surveillance

[3] However, GCISD does ***not*** customize lists of keywords or phrases to be monitored. Rather, these lists are created and maintained by the district's computer service providers Lightspeed Solutions and Gaggle.Net. Both vendors consider their lists to be proprietary. Berger Declaration, ¶ 7; Patterson Declaration, ¶ 4.

systems to monitor students' activity on school-issued devises and accounts, 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; 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. Plaintiff's Original Petition, ¶ 20; Barbaroux Declaration, ¶ 3 and Exhibit 1 thereto.

12. In response, on April 5, 2023, GCISD sent a letter to Knight notifying them of a potential exception to disclosure under the Public Information Act and the school district's intent to seek an Attorney General opinion. The letter also included a request to Knight to clarify its request and to provide search terms. Barbaroux Declaration, ¶ 4 and Exhibit 2 thereto. GCISD then followed up this letter with two letters (a 10-day letter and a 15-day letter) to the Attorney General's office. Barbaroux Declaration, ¶ 4 and Exhibits 3 and 4 thereto.[4]

13. On June 2, 2023, Knight sent a first clarified request for information which narrowed the scope of its original request and provided a list of search terms and the names of vendors. Plaintiff's Original Petition, ¶ 24; Barbaroux Declaration, ¶ 5 and Exhibit 5 thereto. Then, on June 8, 2023, GCISD sent a letter to Knight notifying them that the first part of Knight's request resulted in 2.4 million potential emails with attachments and asked Knight to again narrow the search. GCISD also included a cost estimate for other records potentially responsive to a portion of the original request that required it to seek other documents from all GCISD employees and

[4] A copy of Exhibit 3 to GCISD's April 20, 2023, request to the Attorney General will be submitted to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order. See Tex. Gov't Code § 552.3221.

former employees (estimated to be at least 1,000 records). Finally, GCISD confirmed the two computer monitoring systems being used by the school district were Gaggle.Net and Lightspeed Solutions.[5] Barbaroux Declaration, ¶ 5 and Exhibit 6 thereto.

14. On June 14, 2023, after being informed that the clarified request resulted in 2.4 million potentially responsive emails, Knight once again clarified and narrowed its request to only include analytic reports and emails to/from GCISD's computer surveillance vendors Lightspeed Solutions and Gaggle.Net (the second clarified request). Plaintiff's Original Petition, ¶ 26; Barbaroux Declaration, ¶ 6 and Exhibit 7 thereto.

15. In response to the original information request, in April 2023 GCISD asked for an opinion from the Attorney General whether certain of the information requested is excepted from disclosure under Section 552.139 of the Texas Government Code, which 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." Barbaroux Declaration, ¶ 7 and Exhibit 8 thereto.[6] On June 16, 2023, GCISD received a written Attorney General decision that most of the items submitted to the Attorney General for review were to be withheld pursuant to Section 552.139 of the Government

[5] GCISD has service contracts with both Gaggle.Net and Lightspeed Solutions to provide filter/monitoring systems for GCISD's computer network. To comply with relevant federal and state law, 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. Berger Declaration, ¶ 7-12; Patterson Declaration, ¶ 3-5.

[6] A copy of Exhibit 3 to GCISD's June 28, 2023, request to the Attorney General will be submitted to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order. See Tex. Gov't Code § 552.3221.

Code because they "relate[] to computer network security, and the design, operation or defense of the district's computer network." Barbaroux Declaration, ¶ 8 and Exhibit 9 thereto.[7]

16. On June 21, 2023, GCISD notified Knight that the second clarified request resulted in 824 emails with attachments, with a $741.60 cost estimate to produce. However, GCISD advised that the attachments included reports that were previously ruled by the Attorney General to be withheld and that GCISD would withhold these reports and/or seek another Attorney General determination. Accordingly, on June 28, 2023, GCISD sent a second request to the Attorney General for a determination that the first part of Knight's clarified request was also excepted from disclosure. Plaintiff's Original Petition, ¶¶ 28-29; Barbaroux Declaration, ¶ 9 and Exhibits 10 and 11 thereto.

17. On July 27, 2023, GCISD released the non-excepted records to Knight as directed in the Attorney General's first opinion. Barbaroux Declaration, ¶ 10.

18. On August 31, 2023, GCISD received the Attorney General's written response to the second letter to the Attorney General regarding the second clarified request, which included an analytical report generated by one of the digital surveillance vendors. According to the Attorney General's decision, "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." Barbaroux Declaration, ¶ 11 and Exhibit 12 thereto.[8]

[7] GCISD will submit the documents the Attorney General ordered withheld from production to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order. See Tex. Gov't Code § 552.3221.

[8] GCISD will submit the documents the Attorney General ordered withheld from production to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order. See Tex. Gov't Code § 552.3221.

19. Next, on October 4, 2023, GCISD received the $741.60 payment for costs from Knight for the 824 emails. In response, on October 23, 2023, GCISD sent a letter to Knight explaining that the contents in the 824 emails related to information either already deemed to be excepted from disclosure by the Attorney General or protected from disclosure by FERPA, and would therefore be heavily redacted. Because the emails would be so heavily redacted, GCISD offered to refund the fee in lieu of production. Knight responded to GCISD's letter on November 7, 2023, and directed GCISD to continue with the request and disputing that GCISD could redact the information based on prior Attorney General determinations and arguing that the search terms they provided would not reveal information related to the "design, operation, or defense of a computer network." Knight also argued that another request by GCISD to the Attorney General concerning the redacted emails would be untimely. Plaintiff's Original Petition, ¶¶ 34-35; Barbaroux Declaration, ¶ 12 and Exhibits 13 and 14 thereto.

20. On November 14, 2023, GCISD's counsel notified Knight that GCISD would process the request for records as directed and again notified Knight that GCISD would redact information in accordance with FERPA and the previous Attorney General rulings regarding the subject matter of Knight's request. Barbaroux Declaration, ¶ 13 and Exhibit 15 thereto.

21. On November 17, 2023, GCISD released the 824 emails with heavy redactions to Knight. Plaintiff's Original Petition, ¶ 38; Barbaroux Declaration, ¶ 14 and Exhibit 16 thereto.[9]

22. Shortly after this lawsuit was filed, on April 17, 2025, GCISD requested a third Attorney General Opinion specifically relating to the 824 redacted emails. Barbaroux Declaration,

[9] GCISD will submit unredacted copies of the emails to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order. See Tex. Gov't Code § 552.3221.

¶ 15 and Exhibit 17 thereto.[10] On June 26, 2025, the Attorney General responded in a written decision that GCISD's request would not be rejected as untimely and that "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." Barbaroux Declaration, ¶ 16 and Exhibit 18 thereto.[11]

23. Relevant to the "design or operation of GCISD's computer network," *student email accounts and internet access are part of GCISD's computer network*. See Berger Declaration, ¶ 5. Importantly, 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). CIPA was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the internet. Critical to GCISD's "design or operation" of its computer network, GCISD is <u>required</u> 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

[10] As part of its request, GCISD provided the Attorney General with a representative sample of the 824 emails. Tex. Gov't Code § 552.301(e)(1)(D) permits a governmental body seeking an Attorney General decision about whether requested information is excepted from disclosure under the Texas Public Information Act to submit representative samples of the information if a voluminous amount of information was requested. GCISD will submit unredacted copies of the representative samples to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order. See Tex. Gov't Code § 552.3221.

[11] GCISD will submit the documents the Attorney General ordered withheld from production to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order. See Tex. Gov't Code § 552.3221.

restricting minors' access to materials harmful to them.[12] See, e.g., *Parents, Families & Friends of Lesbians & Gays, Inc. v. Camdenton R-III Sch. Dist.*, 853 F.Supp.2d 888, 891 (W.D. Mo. 2012) (CIPA "requires schools to protect children using school computers from viewing visual depictions that are obscene, child pornography, or harmful to minors."); see also Berger Declaration, ¶ 5-6; Patterson Declaration, ¶ 2. Accordingly, 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. Berger Declaration, ¶ 7; Patterson Declaration, ¶ 3-5.

24. 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. Berger Declaration, ¶ 8-17; Patterson Declaration, ¶ 4-5.

[12] GCISD's Policy CQ (LOCAL) and (LEGAL) incorporates the computer/internet safety requirements of CIPA. Barbaroux Declaration, ¶ 17 and Exhibit 19 thereto.

IV.
ARGUMENT AND AUTHORITIES

A. Summary Judgment Standard

25. A defendant is entitled to summary judgment on a plaintiff's cause of action if the defendant can disprove at least one element of the plaintiff's cause of action as a matter of law. *Stanfield v. Neubaum,* 499 S.W.3d 90, 96 (Tex. 2016).

26. When a party moves for summary judgment based upon an affirmative defense, the movant must establish each element of its defense as a matter of law. *Johnson & Johnson Med., Inc. v. Sanchez*, 924 S.W.2d 925, 927 (Tex. 1996). Once the movant proves each essential element of its affirmative defense, the burden shifts to the non-movant to raise a fact issue either on the movant's affirmative defense or as to each element of an affirmative defense of its own. *See Se. Tex. Indus. v. Helmerich & Payne Int'l Drilling Co.*, 70 S.W.3d 181, 184 (Tex. App.—San Antonio 2001, no pet.) (*citing Ryland Group, Inc. v. Hood*, 924 S.W.2d 120, 121 (Tex. 1996) (per curiam)).

27. Where, like here, the parties file cross-motions for summary judgment, "each party bears the burden of establishing that it is entitled to judgment as a matter of law." *City of Garland v. Dallas Morning News,* 22 S.W.3d 351, 356 (Tex. 2000).

28. "Because the parties do not dispute the relevant facts, this is a proper case for summary judgment." *City of Garland,* 22 S.W.3d at 356. And, "[s]pecifically, whether information is subject to the [Public Information] Act and whether an exception to disclosure applies to the information are questions of law." *Id.* at 357.

B. The Information Requested by Knight is Excepted from Disclosure Under the Public Information Act's Computer Network Security or Infrastructure Exception

29. Knight asks for mandamus relief "compelling [GCISD] to disclose all responsive information" because it alleges that "[t]he 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." Plaintiff's Original Petition, ¶¶ 39-46. However, for the reasons below, GCISD is entitled to summary judgment in its favor because, as a matter of law, the information requested by Knight is excepted from disclosure under section 552.139 (a) since it "relates to" the "design [or] operation" of GCISD's computer network.

1. The Attorney General's decision that the requested information is excepted from disclosure is entitled to "great weight"

30. As detailed above, the Attorney General has issued three written decisions determining that the requested information must be withheld under Tex. Gov't Code §552.139 because the information "relates to computer network security or the design, operation, or defense of GCISD's computer network." Notably, although not binding on the courts, "[b]ecause the legislature has charged the Attorney General with rendering an initial decision each time a governmental entity asserts an exception under the Act, the Attorney General's construction of the Act has ***great weight***." *University of Tex. Law Sch. v. Texas Legal Found.*, 958 S.W.2d 479, 481 (Tex. App. – Austin 1997, no pet.) (emphasis added); see also *Rainbow Group v. Texas Employment Comm'n*, 897 S.W.2d 946, 949 (Tex. App. – Austin 1995, writ denied) ("Although they are not binding on us, this Court gives due consideration to Attorney General decisions, especially in cases involving the Open Records Act under which the Attorney General has a mandate to determine the applicability of exceptions to public disclosure."). Accordingly, the Attorney General's decisions in this case – that the information requested by Knight is excepted from disclosure by GCISD under Tex. Gov't Code §552.139 – are entitled to "great weight" by this Court. *Id*.

2. The requested information "relates to" the "design and/or operation" of GCISD's computer network

31. 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***."

32. Unfortunately, other than the Attorney General decisions in this instant case, there is no case law interpreting § 552.139(a) – i.e., there is no judicial guidance on what qualifies as information that "relates to … the design, operation, or defense of a computer network." However, of assistance, the courts have held that the phrase "relates to," as used in other sections of the Act, "is ***very broad***, encompassing even information that would not be 'relevant,' in the evidentiary sense, during litigation." *B.W.B. v. Eans 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).

33. Here, student email accounts and internet access are part of GCISD's computer network. See Berger Declaration, ¶ 5. Importantly, 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). CIPA was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the internet. Critical to GCISD's "design or operation"[13] of its computer network, GCISD is <u>required</u> 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

[13] Notably, the Act does not define the terms "design" or "operation" as used in § 552.139(a). The relevant dictionary definitions of these terms are: (1) "design" – "a plan or protocol for carrying out or accomplishing something," and (2) "operation" – "a method or manner of functioning" / "a single step performed by a computer in the execution of a program." *Merriam-Webster's Collegiate Dictionary* 313, 815 (10th ed.).

by minors online; unauthorized disclosure, use, and dissemination of personal information regarding minors; and measures restricting minors' access to materials harmful to them.[14] See, e.g., *Parents, Families & Friends of Lesbians & Gays, Inc. v. Camdenton R-III Sch. Dist.*, 853 F.Supp.2d 888, 891 (W.D. Mo. 2012) (CIPA "requires schools to protect children using school computers from viewing visual depictions that are obscene, child pornography, or harmful to minors."); see also Berger Declaration, ¶ 5-6; Patterson Declaration, ¶ 2. Accordingly, 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. Berger Declaration, ¶ 7; Patterson Declaration, ¶ 3-5.

34. 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. Berger Declaration, ¶ 8-17; Patterson Declaration, ¶ 4-5.[15]

[14] GCISD's Policy CQ (LOCAL) and (LEGAL) incorporates the computer/internet safety requirements of CIPA. Barbaroux Declaration, ¶ 17 and Exhibit 19 thereto.

[15] 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."

35. 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 Knight pursuant to Tex. Gov't Code §552.139(a).

36. Because the word lists and the analytical reports created by Lightspeed Solutions and Gaggle.Net "relates to" the "design or operation" of GCISD's computer network, summary judgment in GCISD's favor is proper and Knight's mandamus claim requesting disclosure of this information should therefore be dismissed as a matter of law.

3. The Attorney General properly considered and approved GCISD's belated request to produce responsive emails in redacted form

37. In support of its request for mandamus relief, Plaintiff's Original Petition also alleges that "[m]oreover, 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." According to Knight, "[t]he 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 [and] [t]o date, GCISD has not requested an opinion from the Attorney General that a TPIA exception applies to the information requested in the second part of Clarified Request II [i.e., the information redacted from the 824 emails]." See Plaintiff's Original Petition, ¶ 43. Accordingly, Knight asks the Court to "enter a writ of mandamus requiring GCISD to produce to the Knight

Institute the requested information in Clarified Request II." Id. at ¶ 48. However, like the Attorney General, the Court should find that this information is protected from disclosure to Knight.

38. Because the 824 emails included keywords that correspond to the information the Attorney General had determined must be withheld in the Attorney General's August 31, 2023, decision, without first seeking a third Attorney General opinion GCISD redacted that information previously determined to be withheld pursuant to Section 552.139 when producing the emails with redactions. More specifically, these emails 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 Knight's clarified request, which the Attorney General determined must be withheld pursuant to Section 552.139. See Barbaroux Declaration, ¶ 13. As discussed above, the redacted information in the 824 emails "relates to" the "operation or design" of GCISD's computer network.

39. GCISD acknowledges that more than 10 business days passed between when the school district received Knight's request and when it sought the third Attorney General opinion specifically addressing the 824 emails. However, as the Attorney General has determined in this case, Tex. Gov't Code §552.139 provides a compelling reason to overcome the presumption of openness and, as such, the Attorney General decided to evaluate the applicability of that section to the emails submitted by GCISD past the 10-day deadline. See June 26, 2025, Attorney General Opinion, note 3, attached as Exhibit 18 to Barbaroux Declaration; see also Tex. Atty. Gen. Op. OR2020-15920; Tex. Atty. Gen. Op. OR2018-02510.

40. There is no reason for the Court to not follow the Attorney General's decision in this case, a decision which should be given "great weight," and to find that GCISD properly withheld the redacted information in the 824 emails pursuant to Tex. Gov't Code §552.139 and

that Tex. Gov't Code §552.302's presumption of openness does not require disclosure of the redacted information.

C. Knight lacks standing to challenge GCISD's withholding of student information under FERPA

41. In addition to the information redacted from the 824 emails pursuant to Tex. Gov't Code § 552.139, GCISD also redacted from the 824 emails all student-identifying information protected from disclosure by the Family Educational Rights and Privacy Act ("FERPA"), section 1232g of title 20 of the United States Code. See Barbaroux Declaration, ¶ 14.

42. Importantly, FERPA determinations are solely made by the educational authority in possession of the student records (here, GCISD), and Knight ***lacks standing*** to challenge GCISD's FERPA determinations. *B.W.B.*, 2018 Tex. App. Lexis 223 at *12, 21-22 ("we agree with EISD that B.W.B. lacks standing to challenge EISD's FERPA determinations"; "neither this Court, nor the trial court, nor OAG [Office of Attorney General] is the proper entity to interpret FERPA and its application to EISD's records – it is EISD that must make FERPA determinations"; "FERPA creates no private right of action"); *Tarleton State Univ. v. Found. for Individual Rights & Expression*, 2025 Tex. App. Lexis 3082, *6-11 (Tex. App. – Austin 2025, no pet.) ("We agree with the University that this Court lacks the authority to judicially review its FERPA determinations for the information at issue. … Because courts cannot resolve disputes as to the University's determinations on what information is subject to FERPA's nondisclosure provisions, the University can withhold or redact FERPA information without judicial review."); *IDEA Pub. Sch. v. Socorro Indep. Sch. Dist.*, 2020 Tex. App. Lexis 122, *4-7 (Tex. App. – Corpus Christi 2020, pet. denied) (finding the plaintiff lacked standing to complain about school's FERPA determinations "[b]ecause such determinations under FERPA must be made by the institution from whom they are requested

[and] neither this Court, nor the trial court, nor the Office of the Attorney General of Texas is the proper entity to interpret FERPA and its application to [the school's] records").

43. Accordingly, any challenge by Knight of GCISD's redactions to the 824 emails based on its FERPA determinations must be dismissed for a lack of standing.

D. Knight is Not Entitled to Attorneys' Fees Because GCISD Acted in Reasonable Reliance on Written Decisions of the Attorney General

44. In addition to a mandamus requiring production of the withheld information, Knight also asks for its attorney's fees pursuant to Tex. Gov't Code §552.323. Plaintiff's Original Petition, ¶¶ 47, 48(E).

45. Section 552.323(a) requires a court to "assess costs of litigation and reasonable attorney fees incurred by a plaintiff who substantially prevails" *unless* "the court finds that the governmental body acted in reasonable reliance on" an Attorney General decision. *Univ. of Tex. at Austin v. GateHouse Media Tex. Holdings II Inc.*, 2024 Tex. Lexis 1166, *11-12 (Tex. 2024) (quoting section 552.323(a)). Critically, here, GCISD acted in reasonable reliance on multiple Attorney General decisions determining that it "***must*** withhold the information" requested by Knight.

46. Because GCISD acted in reasonable reliance on multiple Attorney General decisions determining that it "***must*** withhold the information" requested by Knight, even assuming *arguendo* that Knight substantially prevails and a mandamus requiring disclosure of the withheld/redacted information is eventually issued, Knight is not entitled to its attorney's fees under section 552.323 as a matter of law.

E. Knight is Not Entitled to a Fee Waiver for its Request

47. Finally, Knight asks that the Court order that it "is entitled to a fee waiver for its Request, and that GCISD reimburse the Knight Institute for its previous payment [$741.60] for public information." Plaintiff's Original Petition, ¶¶ 44, 48(D).

48. The Texas Public Information Act permits governmental entities such as GCISD to impose charges for the cost of copying records and, in certain circumstances, preparing them for inspection. See Tex. Gov't Code §§ 552.261, .271. Relevant here, the governmental entity may also, in its *sole* discretion, grant a waiver or reduction of those charges. See Tex. Gov't Code § 552.267 (charges may be reduced or waived "***if*** the governmental body determines [to do so]"); 1 TAC § 70.1 ("the governmental body ***may*** grant a waiver or reduction for charges"). Importantly, however, whether to waive or reduce the charges in the present case is to be determined by GCISD *alone*, not the Court – as held by the Austin Court of Appeals, "Nowhere in the Act or the administrative code do we find any provision authorizing a court to limit the amount of reimbursement a governing body may seek from the requestor." *Thomas v. Cornyn*, 71 S.W.3d 473, 491 (Tex. App. – Austin 2014, pet. denied).

49. Here, GCISD has determined that it will not waive or reduce the $741.60 it charged to redact and produce the 824 emails responsive to Knight's request.[16] For example, regardless of Knight's intended use of the requested information, GCISD was nevertheless compelled to spend valuable school district resources to review for and redact FERPA protected student information in response to Knight's public information request, and has determined that waiver or reduction of

[16] See July 7, 2023, email from Ali Williams to Jennifer Jones, attached as Exhibit L to Plaintiff's Original Petition ("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.").

these incurred costs is not warranted.[17] Critically, the Public Information Act does not authorize Knight's requested reversal of GCISD's statutorily allowed discretionary decision. See *Cornyn*, 71 S.W.3d at 491. Summary judgment in GCISD's favor on this claim is therefore proper.

V.
CONCLUSION AND PRAYER

50. For these reasons, GCISD asks the Court to grant this motion and sign a final summary judgment that dismisses all causes of action and requests for relief asserted in Plaintiff's Original Petition and Request for Writ of Mandamus.

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

[17] See June 21, 2023, email from Ali Williams to Jennifer Jones, attached as Exhibit L to Plaintiff's Original Petition ("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.").

CERTIFICATE OF SERVICE

I hereby certify that on January 30, 2026, a true and correct copy of Defendant's Motion for Summary Judgment has been served on all counsel of record via the Court's e-filing system.

/s/ Charles J. Crawford
Charles J. Crawford

EXHIBIT A

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**

DECLARATION OF PAULA BARBAROUX

1. My name is Paula Barbaroux. I am competent to make this declaration. The facts stated in this declaration are within my personal knowledge and are true and correct.

2. I am the Chief Operations Officer for Grapevine-Colleyville Independent School District ("GCISD"). As Chief Operations Officer, my duties and responsibilities include overseeing eight departments and managing GCISD's processing and response to requests for records in accordance with the Texas Public Information Act.

3. On March 29, 2023, Knight First Amendment Institute at Columbia University ("Knight") sent a Texas Public Information Act request to GCISD for records related to its use of surveillance systems to monitor students' activity on school-issued devices and accounts, 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; 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. A true and correct copy of Knight's request is attached as Exhibit 1 hereto.

4. In response, on April 5, 2023, GCISD sent a letter to Knight notifying them of a potential exception to disclosure under the Public Information Act and the school district's intent to seek an Attorney General opinion. The letter also included a request to Knight to clarify its request and to provide search terms. A true and correct copy of this letter is attached as Exhibit 2 hereto. GCISD then followed up this letter with two letters (a 10-day letter and a 15-day letter) to the Attorney General's office. True and correct copies of these two letters are attached as Exhibits 3 and 4 hereto.

5. On June 2, 2023, Knight sent a first clarified request for information, which narrowed the scope of its original request and provided a list of search terms and the names of vendors. A true and correct copy of this clarified request is attached as Exhibit 5 hereto. Then, on June 8, 2023, GCISD sent a letter to Knight notifying them that the first part of Knight's request resulted in 2.4 million potential emails with attachments and asked Knight to again narrow the search. GCISD also included a cost estimate for other records potentially responsive to a portion of the original request that required it to seek other documents from all GCISD employees and former employees (estimated to be at least 1,000 records). Finally, GCISD confirmed the two computer monitoring systems being used by the school district were Gaggle.Net and Lightspeed Solutions. A true and correct copy of GCISD's letter is attached as Exhibit 6 hereto.

6. On June 14, 2023, after being informed that the clarified request resulted in 2.4 million potentially responsive emails, Knight once again clarified and narrowed its request to only include analytic reports and emails to/from GCISD's computer surveillance vendors Lightspeed

Solutions and Gaggle.Net (the second clarified request). A true and correct copy of this second clarified request is attached as Exhibit 7 hereto.

7. In response to the original information request, in April 2023 GCISD asked for an opinion from the Attorney General whether certain of the information requested is excepted from disclosure under Section 552.139 of the Texas Government Code, which 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." A true and correct copy of GCISD's request to the Attorney General (less Exhibit 3 thereto) is attached as Exhibit 8 hereto.[1]

8. On June 16, 2023, GCISD received a written Attorney General decision that most of the items submitted to the Attorney General for review were to be withheld pursuant to Section 552.139 of the Government Code because they "relate[] to computer network security, and the design, operation or defense of the district's computer network." A true and correct copy of the Attorney General's opinion is attached as Exhibit 9 hereto.[2]

9. On June 21, 2023, GCISD notified Knight that the second clarified request resulted in 824 emails with attachments, with a cost estimate of $741.60 to produce the records. However, GCISD advised that the attachments included reports that were previously ruled by the Attorney General to be withheld and that GCISD would withhold these reports and/or seek another Attorney General determination. A true and correct copy of GCISD's notice to Knight is attached as Exhibit 10 hereto. Accordingly, on June 28, 2023, GCISD sent a second request to the Attorney General

[1] GCISD will submit Exhibit 3 to the request to the Attorney General to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order.

[2] GCISD will submit the documents the Attorney General ordered withheld from production to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order.

for a determination that the first part of Knight's clarified request was also excepted from disclosure. A true and correct copy of GCISD's second request to the Attorney General (less Exhibit 3 thereto) is attached as Exhibit 11 hereto.[3]

10. On July 27, 2023, GCISD released the non-excepted records to Knight as directed in the Attorney General's first opinion.

11. On August 31, 2023, GCISD received the Attorney General's written response to the second letter to the Attorney General regarding the second clarified request, which included an analytical report generated by one of the digital surveillance vendors. According to the Attorney General's decision, "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." A true and correct copy of the second Attorney General opinion is attached as Exhibit 12 hereto.[4]

12. Next, on October 4, 2023, GCISD received the $741.60 payment for costs from Knight for the 824 emails. In response, on October 23, 2023, GCISD sent a letter to Knight explaining that the contents in the 824 emails related to information either already deemed to be excepted from disclosure by the Attorney General or protected from disclosure by the Family Educational Rights and Privacy Act ("FERPA"), section 1232g of title 20 of the United States Code, and would therefore be heavily redacted. Because the emails would be so heavily redacted, GCISD offered to refund the fee in lieu of production. A true and correct copy of GCISD's letter is attached as Exhibit 13 hereto. Knight responded to GCISD's letter on November 7, 2023, and

[3] GCISD will submit Exhibit 3 to the request to the Attorney General to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order.

[4] GCISD will submit the documents the Attorney General ordered withheld from production to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order.

directed GCISD to continue with the request, disputed that GCISD could redact the information based on prior Attorney General determinations, and argued that the search terms they provided would not reveal information related to the "design, operation, or defense of a computer network." Knight also argued that another request by GCISD to the Attorney General concerning the redacted emails would be untimely. A true and correct copy of Knight's letter is attached as Exhibit 14 hereto.

13. On November 14, 2023, GCISD's counsel notified Knight that GCISD would process the request for records as directed and again notified Knight that GCISD would redact information in accordance with FERPA and the previous Attorney General rulings regarding the subject matter of Knight's request. A true and correct copiy of tht communication via email to Knight is attached as Exhibit 15 hereto.

14. On November 17, 2013, GCISD released the 824 emails with heavy redactions to Knight. In addition to the information redacted from the 824 emails pursuant to Tex. Gov't Code § 552.139, GCISD also redacted from the 824 emails all student-identifying information protected from disclosure by FERPA. True and correct copies of the redacted emails released to Knight are attached as Exhibit 16 hereto.

15. Shortly after this lawsuit was filed, on April 17, 2025, GCISD requested a third Attorney General Opinion specifically relating to the 824 redacted emails. As part of its request, as allowed by Tex. Gov't Code § 552.301(e)(1)(D) GCISD provided the Attorney General with a representative sample of the 824 emails. A true and correct copy of GCISD's third Attorney General request (less Exhibit 4 thereto) is attached as Exhibit 17 hereto.[5]

[5] GCISD will submit Exhibit 4 to the request to the Attorney General to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order.

16. On June 26, 2025, the Attorney General responded in a written decision that GCISD's request would not be rejected as untimely and that "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." A true and correct copy of the third Attorney General opinion is attached as Exhibit 18 hereto.[6]

17. 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). To comply with CIPA, GCISD's Policy CQ (LOCAL) and (LEGAL) incorporates the computer/internet safety requirements of CIPA. A true and correct copy of Policy CQ (LOCAL) and (LEGAL) is attached as Exhibit 19 hereto.

18. I declare under penalty of perjury that the foregoing is true and correct.

EXECUTED ON December 1, 2025.

Paula Barbaroux

[6] GCISD will submit the documents the Attorney General ordered withheld from production to the Court in a hand delivered sealed wrapper for the Court's *in camera* inspection and sealing order.

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 2

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 3

Jackson Walker LLP

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)

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 4

JW | Jackson Walker LLP

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)

EXHIBIT 5

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

"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 6

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 DISTRICT

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 7

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 8

JW | Jackson Walker LLP

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)

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 2

JW | Jackson Walker LLP

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)

EXHIBIT 3

EXHIBIT 9

THE OFFICE OF THE ATTORNEY GENERAL OF TEXAS

June 16, 2023

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

OR2023-20568

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
>
> (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 [d]istrict'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.

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

DMH/jxd

Ref: ID# 062638

Enc. Submitted documents

c: Requestor
(w/o enclosures)

EXHIBIT 10

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

JW | 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 11

JW | Jackson Walker LLP

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 ☒

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

JW | Jackson Walker LLP

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)

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 2

JW | Jackson Walker LLP

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.

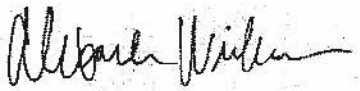
There are documents responsive to this Request. However, the District believes that the items responsive to this Request may be excepted from public disclosure under Texas Government Code § 552.139.

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)

EXHIBIT 3

THE OFFICE OF THE ATTORNEY GENERAL OF TEXAS

June 16, 2023

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

OR2023-20568

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
>
> (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 [d]istrict'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.

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

DMH/jxd

Ref: ID# 062638

Enc. Submitted documents

c: Requestor
(w/o enclosures)

EXHIBIT ☒

Williams, Ali

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Wednesday, June 14, 2023 5:52 PM
To: Williams, Ali
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 3

EXHIBIT 12

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

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 13

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 DISTRICT

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 14

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 15

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 16

Documents can be Downloaded with the Following ShareFile Link:
https://abernathy-law.sharefile.com/d-s5ae2c970054d4c04b38f3135fdd3fddb

EXHIBIT 17

Jackson Walker LLP

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)

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

JW | Jackson Walker LLP

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)

JW | Jackson Walker LLP

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)

THE OFFICE OF THE ATTORNEY GENERAL OF TEXAS

June 16, 2023

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

OR2023-20568

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
>
> (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 [d]istrict'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.

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

DMH/jxd

Ref: ID# 062638

Enc. Submitted documents

c: Requestor
(w/o enclosures)

Williams, Ali

From: Jennifer Jones <jennifer.jones@knightcolumbia.org>
Sent: Wednesday, June 14, 2023 5:52 PM
To: Williams, Ali
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

Jackson Walker LLP

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)

THE OFFICE OF THE ATTORNEY GENERAL OF TEXAS

August 31, 2023

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

OR2023-30020

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;

[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).

> (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 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.

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

MRG/mo

Ref: ID# 077074

c: Requestor

EXHIBIT 18

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 19

Note: For Board member use of District technology resources, see BBI. For student use of personal electronic devices, see FNCE.

For purposes of this policy, "technology resources" means electronic communication systems and electronic equipment.

Availability of Access

Access to the District's technology resources, including the internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations.

Limited Personal Use

Limited personal use of the District's technology resources shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's technology resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

Use by Members of the Public

Access to the District's technology resources, including the internet, shall be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the District; and
2. Does not unduly burden the District's technology resources.

Acceptable Use

The Superintendent shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy.

Access to the District's technology resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the District's technology resources and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

Internet Safety

The Superintendent shall develop and implement an internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

Filtering

Each District computer with internet access and the District's network systems shall have filtering devices or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent.

The Superintendent shall enforce the use of such filtering devices. Upon approval from the Superintendent, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.

Monitored Use

Electronic mail transmissions and other use of the District's technology resources by students, employees, and members of the public shall not be considered private. Designated District staff shall be authorized to monitor the District's technology resources at any time to ensure appropriate use.

Disclaimer of Liability

The District shall not be liable for users' inappropriate use of the District's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the availability of the District's technology resources or the accuracy, age appropriateness, or usability of any information found on the internet.

Record Retention

A District employee shall retain electronic records, whether created or maintained using the District's technology resources or using personal technology resources, in accordance with the District's record management program. [See CPC]

Electronically Signed Documents

At the District's discretion, the District may make certain transactions available online, including student admissions documents,

student grade and performance information, contracts for goods and services, and employment documents.

To the extent the District offers transactions electronically, the District may accept electronic signatures in accordance with this policy.

When accepting electronically signed documents or digital signatures, the District shall comply with rules adopted by the Department of Information Resources, to the extent practicable, to:

- Authenticate a digital signature for a written electronic communication sent to the District;
- Maintain all records as required by law;
- Ensure that records are created and maintained in a secure environment;
- Maintain appropriate internal controls on the use of electronic signatures;
- Implement means of confirming transactions; and
- Train staff on related procedures as necessary.

Next Generation Technology

A district, in the administration of the district, shall consider using next generation technologies, including cryptocurrency, blockchain technology, robotic process automation, and artificial intelligence. *Gov't Code 2054.601*

Children's Internet Protection Act

"Harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

Definitions

Harmful to Minors

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

47 U.S.C. 254(h)(7)(G); 20 U.S.C. 7131(e)(6)

Technology Protection Measure

"Technology protection measure" means a specific technology that blocks or filters internet access to the material covered by a certification described at Certifications to the FCC, below, to which such certification relates. *47 U.S.C. 254(h)(7)(I)*

Universal Service Discounts (E-Rate)

An elementary or secondary school having computers with internet access may not receive universal service discount rates unless the district submits to the FCC the certifications described below at Certifications to the FCC and a certification that an internet safety policy has been adopted and implemented as described at Internet Safety Policy, below, and ensures the use of computers with internet access in accordance with the certifications. *47 U.S.C. 254(h)(5)(A); 47 C.F.R. 54.520*

Certifications to the FCC

A district that receives discounts for internet access and internal connections services under the federal universal service support mechanism for schools must make certifications in accordance with 47 C.F.R. 54.520(c) each funding year. A district that only receives discounts for telecommunications services is not subject to the certification requirements, but must indicate that it only receives discounts for telecommunications services. *47 C.F.R. 54.520(b)*

With Respect to Minors

A certification under 47 U.S.C. 254(h)(5)(B) is a certification that the district is:

1. Enforcing a policy of internet safety for minors that includes monitoring their online activities and the operation of a tech-

nology protection measure with respect to any of its computers with internet access that protects against access through such computers to visual depictions that are obscene, child pornography, or harmful to minors;

2. Enforcing the operation of such technology protection measure during any use of such computers by minors; and

3. Educating minors, as part of its internet safety policy, about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

47 U.S.C. 254(h)(5)(B); 47 C.F.R. 54.520(c)(1)

With Respect to Adults

A certification under 47 U.S.C. 254(h)(5)(C) is a certification that the district is:

1. Enforcing a policy of internet safety that includes the operation of a technology protection measure with respect to any of its computers with internet access that protects against access through such computers to visual depictions that are obscene or child pornography; and

2. Enforcing the operation of such technology protection measure during any use of such computers.

47 U.S.C. 254(h)(5)(C); 47 C.F.R. 54.520(c)(1)

Disabling for Adults

An administrator, supervisor, or other person authorized by the district may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. *47 U.S.C. 254(h)(5)(D)*

Internet Safety Policy

A district shall adopt and implement an internet safety policy that addresses:

1. Access by minors to inappropriate matter on the internet and the World Wide Web;

2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

3. Unauthorized access, including "hacking," and other unlawful activities by minors online;

4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and

5. Measures designed to restrict minors' access to materials harmful to minors.

47 U.S.C. 254(l); 47 C.F.R. 54.520(c)(1)(ii)

Public Hearing — A district shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed internet safety policy. *47 U.S.C. 254(h)(5)(A)(iii), (l)(1)(B)*

Inappropriate for Minors — A determination regarding what matter is inappropriate for minors shall be made by the board or designee. *47 U.S.C. 254(l)(2)*

Noncompliance — A district that knowingly fails to submit required certifications shall not be eligible for discount services under the federal universal service support mechanism for schools until such certifications are submitted.

A district that knowingly fails to ensure the use of computers in accordance with the required certifications must reimburse any funds and discounts received under the federal universal service support mechanism for schools for the period in which there was noncompliance.

47 C.F.R. 54.520(d), (e); 47 U.S.C. 254(h)(5)(F)

ESEA Funding — No federal funds made available under Title IV, Part A of the ESEA for an elementary or secondary school that does not receive universal service discount rates may be used to purchase computers used to access the internet, or to pay for direct costs associated with accessing the internet unless a district:

1. Has in place a policy of internet safety for minors that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors; and enforces the operation of the technology protection measure during any use by minors of its computers with internet access; and

2. Has in place a policy of internet safety that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene or child pornography; and enforces the operation of the technology protection measure during any use of its computers with internet access.

An administrator, supervisor, or other person authorized by the district may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

Certification to U.S. Department of Education

A district shall certify its compliance with these requirements during each annual program application cycle under the ESEA.

20 U.S.C. 7131

Uniform Electronic Transactions Act (UETA)

The UETA (Business and Commerce Code Chapter 322) applies to electronic records and electronic signatures relating to a transaction. *Business and Commerce Code 322.003(a)*

The UETA applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. The UETA does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form. A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. This right may not be waived by agreement. *Business and Commerce Code 322.005(a)–(c)*

Except as otherwise provided in Business and Commerce Code 322.012(f), the UETA does not require a district to use or permit the use of electronic records or electronic signatures. *Business and Commerce Code 322.017(c)*

Records Retention

If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:

1. Accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

2. Remains accessible for later reference.

A record retained as an electronic record in accordance with the provisions above satisfies a law requiring a person to retain a record for evidentiary, audit, or like purposes, unless a law enacted after January 1, 2002, specifically prohibits the use of an electronic record for the specified purpose.

Business and Commerce Code 322.012(a), (f)

[For more information on records management, see CPC.]

Definitions

"Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means.

"Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

"Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Business and Commerce Code 322.002(7), (8), (15)

Digital Signature

A digital signature may be used to authenticate a written electronic communication sent to a district if it complies with rules adopted by the board. Before adopting the rules, the board shall consider the rules adopted by the Department of Information Resources (DIR) and, to the extent possible and practicable, make the board's rules consistent with DIR rules. *Gov't Code 2054.060(b)* [See 1 Administrative Code Chapter 203 for DIR rules related to management of electronic transactions and signed records.]

"Digital signature" means an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature. *Gov't Code 2054.060(e)(1)*

Interception of Communications

For information on the unlawful interception, use, or disclosure of communications, see the Electronic Communications Privacy Act (18 USC 2510–2523 [federal wiretap act] and 2701–2713 [Stored Communications Act]) and Penal Code 16.02 (state wiretap law) and 16.04 (Unlawful Access to Stored Communications).

EXHIBIT B

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**

DECLARATION OF KYLE BERGER

1. My name is Kyle Berger. I am competent to make this declaration. The facts stated in this declaration are within my personal knowledge and are true and correct.

2. I am the Chief Technology Officer for Grapevine-Colleyville Independent School District ("GCISD"). As Chief Technology Officer my duties and responsibilities include directing 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.

3. 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.

4. 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.

5. 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***.

6. 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.

7. 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

[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.

solely created and maintained by the district's computer service providers Lightspeed Solutions and Gaggle.Net. Both vendors consider their lists to be proprietary.

8. 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.

9. 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:

- 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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").

18. Attached to this declaration as Exhibit 1 is a true and correct copy of my November 19, 2025, expert report in this lawsuit. I re-affirm the statements and opinions in my report, which are incorporated into this declaration by this reference.

19. I declare under penalty of perjury that the foregoing is true and correct.

EXECUTED ON Dec 3rd, 2025.

Kyle Berger

EXHIBIT 1

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 C

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**

DECLARATION OF JEFF PATTERSON

1. My name is Jeff Patterson. I am competent to make this declaration. The facts stated in this declaration are within my personal knowledge and are true and correct.

2. I am the founder and CEO of Gaggle.Net, Inc. The company's mission is to leverage people and technology to protect students and save lives. Gaggle's services are designed to help schools proactively identify and address student safety concerns, including self-harm, substance abuse, cyberbullying, and other threats. Part of Gaggle's services are intended to assist school districts to comply with the requirements of the Children's Internet Protection Act ("CIPA"), Pub. L. No. 106-554, 114 Stat. 2763 (2000).

3. Gaggle.Net has a service contract with Grapevine-Colleyville ISD ("GCISD") to provide a filter/monitoring system for GCISD's computer network. As provided in Gaggle.Net's service contract with GCISD, "Gaggle provides Services to your organization to assist it in the protection of your students and your organization. Gaggle shall undertake every commercially reasonable effort to maximize the detection of unsafe, graphic, and/or obscene communications."

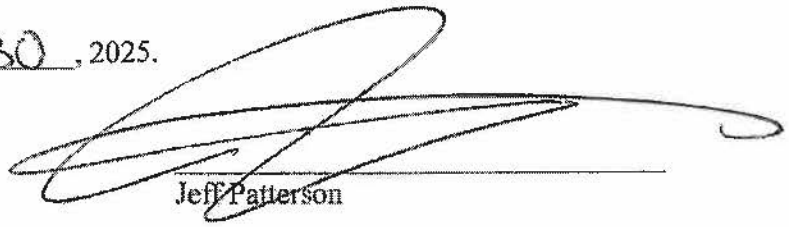
4. To assist with GCISD's compliance with relevant federal and state law, including CIPA, Gaggle.Net's blocking and filtering system uses proprietary keywords and combinations of

those keywords as a tool to maximize the detection of unsafe, graphic, and/or obscene student communications and website content on school district devices. For example, search terms that 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.

5. In compliance with CIPA, Gaggle.Net's system works by monitoring GCISD 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.

6. I declare under penalty of perjury that the foregoing is true and correct.

EXECUTED ON October 30, 2025.



Jeff Patterson

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: 110662822
Filing Code Description: Motion (No Fee)
Filing Description: Defendant's Motion for Summary Judgment
Status as of 1/30/2026 2:38 PM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Lucas ChristopherHenry		lhenry@abernathy-law.com	1/30/2026 12:21:39 PM	SENT
Charles J.Crawford		ccrawford@abernathy-law.com	1/30/2026 12:21:39 PM	SENT
Kimberly Escamilla		kescamilla@abernathy-law.com	1/30/2026 12:21:39 PM	SENT
Laura Ball		lball@abernathy-law.com	1/30/2026 12:21:39 PM	SENT
Peter Steffensen		psteffensen@smu.edu	1/30/2026 12:21:39 PM	SENT
Peter Steffensen		psteffensen@smu.edu	1/30/2026 12:21:39 PM	SENT
Jennifer Jones		jennifer.jones@knightcolumbia.org	1/30/2026 12:21:39 PM	SENT
Katie Fallow		katie.fallow@knightcolumbia.org	1/30/2026 12:21:39 PM	SENT
Thomas Leatherbury		tom@tsleatherburylaw.com	1/30/2026 12:21:39 PM	SENT
MARY ALLIESCHIELE		ALLIE.SCHIELE@KNIGHTCOLUMBIA.ORG	1/30/2026 12:21:39 PM	SENT
Kiran Wattamwar		Kiran.Wattamwar@knightcolumbia.org	1/30/2026 12:21:39 PM	SENT