No. 128300

IN THE
SUPREME COURT OF ILLINOIS

MATT CHAPMAN,

Plaintiff-Appellee,

v.

CHICAGO DEPARTMENT OF FINANCE,

Defendant-Appellant.

On Appeal from the Appellate Court of Illinois
First Judicial District, No. 1-20-0547
There Heard on Appeal from the Circuit Court of Cook County, Illinois
County Department, Chancery Division
No. 2018-CH-14043
The Honorable Sanjay T. Tailor, Judge Presiding

BRIEF AND APPENDIX OF DEFENDANT-APPELLANT

Corporation Counsel
of the City of Chicago
2 N. LaSalle Street, Suite 580
Chicago, Illinois 60602
(312) 742-5147
ellen.mclaughlin@cityofchicago.org
appeals@cityofchicago.org

MYRIAM ZRECZNY KASPER
Deputy Corporation Counsel
SUZANNE LOOSE
Chief Assistant Corporation Counsel
ELLEN W. MCLAUGHLIN
Assistant Corporation Counsel
Of Counsel

E-FILED
8/4/2022 11:51 AM
CYNTHIA A. GRANT
SUPREME COURT CLERK

TABLE OF CONTENTS AND POINTS AND AUTHORITIES

NATURE OF THE CASE

Plaintiff-appellee Matt Chapman submitted an Illinois Freedom of Information Act ("FOIA") request to the Chicago Department of Finance ("DOF"), seeking the database schema for CANVAS, the database DOF uses to store, process, and track parking and traffic citation information. DOF denied the request, stating that it was withholding the requested records under section 7(1)(o) of FOIA, which exempts from disclosure "[a]dministrative or technical information associated with automated data processing operations, including but not limited to . . . file layouts, . . . and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under" section 7(1)(o).

Chapman filed a complaint in the circuit court, alleging that DOF violated FOIA by withholding the requested records. The parties moved for summary judgment, which the court denied on the ground that there was a question of fact whether disclosure of the requested records "would jeopardize the security of the system" within the meaning of section 7(1)(o), and the case was set for a bench trial. At trial, DOF asserted that because the requested records were "file layouts," which are per se exempt under section 7(1)(o), it was not required to specifically prove their disclosure would jeopardize CANVAS's security. The circuit court rejected that argument. After trial, the court found that DOF failed to prove by clear and convincing evidence that disclosure of the requested records would jeopardize the security of

CANVAS and ordered DOF to produce them. The appellate court affirmed.

DOF appeals. No questions are raised on the pleadings.

ISSUES PRESENTED

1. Whether the plain language of section 7(1)(o) of FOIA expressly exempts the records Chapman requested from disclosure.

2. Whether DOF demonstrated by clear and convincing evidence that disclosure of the requested records would facilitate unauthorized access to data and thus would jeopardize the security of the CANVAS system, within the meaning of section 7(1)(o).

JURISDICTION

On January 9, 2020, the circuit court entered judgment against DOF and ordered it to produce the requested records. A25; C. 79.[1] Because Chapman's request for attorney's fees was pending, C. 91, that was not a final appealable order. On March 12, 2020, the circuit court entered an order stating that the parties had resolved the fee issue, making the January 9, 2020 order final and appealable; the court also stayed the production order. A26; C. 92. On March 19, 2020, DOF filed a notice of appeal. A27-30; C. 93-96. On February 14, 2022, the appellate court affirmed the circuit court's judgment. A18. On March 21, 2022, DOF filed a petition for leave to appeal,

[1] The record on appeal consists of the common law record and the report of proceedings. We cite the common law record as "C. __," the report of

which this court allowed on May 25, 2022. This court has jurisdiction under Ill. Sup. Ct. R. 315.

STATUTORY PROVISION INVOLVED

Section 7(1)(o) of FOIA exempts from disclosure:

> Administrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section.

5 ILCS 140/7(1)(o).

STATEMENT OF FACTS

On August 30, 2018, Chapman submitted a FOIA request to DOF seeking "[a]n index of the table and columns within each table of CANVAS," along with the "column data type." C. 13. Chapman referred to this information as the "database schema." C. 14-15. On September 12, 2018, DOF denied the request under section 7(1)(o) of FOIA. C. 16-17. On November 9, 2018, Chapman filed a complaint in the circuit court seeking injunctive relief and civil penalties, C. 8-12, alleging that DOF "violated FOIA by failing to produce the records requested," C. 10.

The parties filed cross-motions for summary judgment. C. 31-36, 41-

---

proceedings as "R. __," and the appendix to this brief as "A__."

48, 51-59, 62-67. DOF relied on the affidavit of Bruce Coffing, Chief Information Security Officer with the City's Department of Innovation and Technology, C. 46-48, who explained that release of the information "would provide the public at large with a roadmap of the entire CANVAS system," jeopardizing the system's security, C. 43-44. Chapman, meanwhile, argued that Coffing's affidavit failed to show the records "would jeopardize the security of the system or its data," C. 52, and submitted the affidavit of information security professional Thomas Ptacek in support. C. 58-59. The court denied both motions. R. 12.

The court held a bench trial on January 9, 2020. R. 15-197. Before the trial began, DOF argued to the court that the information Chapman requested constituted a "file layout" or "source listing," both of which are expressly exempt from disclosure under section 7(1)(o), with no need for the public body to specifically show disclosure would pose a security risk. R. 25-27. Rejecting that argument, the court ruled "as a matter of law" that the phrase "if disclosed, would jeopardize the security of the system" in section 7(1)(o) qualifies every term that proceeds it, including "file layouts" and "source listings." A20; R. 34. Because, according to the court, the section 7(1)(o) exemption applies only upon a showing that disclosure "would jeopardize the security of the system," the issue for trial was whether DOF could make that showing regarding the information Chapman requested. A20; R. 34.

Each side called one witness at trial. DOF called Coffing, R. 57, the City's Chief Information Security Officer, who is responsible for protecting CANVAS – and the sensitive data it contains – from cyberattack. R. 61. He recounted his more than two decades of experience working in cybersecurity and experience working with CANVAS. R. 58. He explained that DOF uses CANVAS "to store and process and track citation information around parking tickets, speed-light camera tickets, stoplight traffic tickets, [and] booting and towing tickets," R. 59, and CANVAS contains "sensitive information relating to the constituents that receive these tickets," including the vehicle owner's name, address, and driver's license number; whether the vehicle owner has a disability parking placard; details about the City official who issued the ticket; and information related to payment of the ticket, such as payment plan information and bankruptcy status, R. 59-60.

Coffing explained that the database schema Chapman sought includes CANVAS's tables, columns within each table, and column data type – information that constitutes a "file layout," which he defined as "the instructions that the database management system uses to create the database that the data is then stored in." R. 67-68. Coffing explained that one "layer of defense" the City uses to defend a data system involves "limiting the information that's known about a system, so that the adversary has less to capture in their efforts to perform recognizance about the system." R. 62. An adversary with less information about the system, Coffing explained, will

be "nois[ier] when they are attempting their attack, which provides more data to the defenders to alert them an attack is underway." R. 62. In contrast, if someone has "precise information about the system, their activity may blend in and look like normal activity." R. 63. Disclosure of the information Chapman requested would undermine that "layer of defense strategy," R. 70, as it would allow an adversary to "perform recognizance on a target or a system and . . . more precisely craft their attack," "limit the noise that they would make," and "limit the likelihood of them being detected," R. 69, thereby making an attack "more effective," R. 70.

Coffing further testified that the information Chapman requested would facilitate a type of attack known as a SQL injection.[2] SQL, he explained, "is the language that a database management system uses," and a SQL injection uses that language, or code, to "make the system do something that it was not intended to do." R. 70. For example, an adversary could create a malicious SQL instruction and "attempt to inject that [instruction] into an existing interface," such as a field that asks for a last name, and "force the system to spit out another type of data or information." R. 72. The last name field would act as "a window into the system," or vulnerability, that the adversary could exploit to gain access to sensitive data in the

[2] "SQL" stands for "structured query language," a programming language used to create large databases. E.g., https://www.ibm.com/docs/en/db2/10.5?topic=fundamentals-sql.

system. R. 72-73. In addition to being exposed, the data could be modified or deleted, making it "unusable" and "impairing the City's ability to manage citations." R. 74. Knowledge of the information Chapman requested would enable an adversary to "precisely write" a SQL injection. R. 72-73.

Coffing explained that the requested information could also facilitate a "zero-day" attack, which is an attack based on "a vulnerability that is known to an attacker" but not "to the defender." R. 75. An adversary who has identified a "zero-day" vulnerability can exploit it to attack the system before the defender has an opportunity to "create a patch for it." R. 75. Finally, Coffing explained, the City had already made some information about CANVAS's hardware and software components, operating system, and monitoring tools publicly available, in a request for proposals. R. 65-66, 78-79. Making even more information about the system public would give an adversary "more at their disposal to attempt an attack." R. 76.

On cross-examination, Coffing agreed that "CANVAS is a competently built system" that employs "best practices in the industry." R. 80. He further elaborated on SQL injections, explaining that CANVAS has three interfaces for ticket recipients to request a hearing, for fleet owners to get information about their fleet, and for ticket recipients to request a payment plan. R. 87-88. Each of these has fields an adversary "could attempt to compromise" with a SQL instruction. R. 87-88. He explained that these interfaces are also vulnerable to "insider attacks," which occur when people with "some level of

appropriate access" either "misus[e] that access" or use it to "compromise the system." R. 90. Coffing agreed that it would not be too difficult for an adversary to figure out what types of information CANVAS contains, R. 90-91, but explained that, without the file layout, an adversary would not know "precisely what the column name is," R. 92. For example, the last name field could be "f underscore name," "L underscore name," "last underscore name," or something else. R. 92. Without that information, an adversary would "have to guess," R. 92, and "those inaccurate guesses are going to generate errors" and "logs," which are "the things that defenders look for to try to determine whether or not there is a threat actor in the environment," R. 93. Finally, Coffing acknowledged that other public bodies have released database schema but explained that, unlike CANVAS, some systems have "completely public information," R. 100, whereas CANVAS "has sensitive data" about the City's constituents, R. 101.

Chapman called information security professional Thomas Ptacek, C. 58-59, a "friend of" Chapman's, R. 156. Ptacek likened the database schema to "a collection of spread sheets," including the spread sheets' names and column headings, which "together compris[e] the database that the CANVAS application . . . runs off." R. 123. He testified that the information Chapman requested would be of little use in initiating a database attack, R. 118-19, because no competently built system "could be attacked solely with the schema," R. 126. In his own work, he is "never provided with schemas"

and does not ask for "schema information." R. 119. According to Ptacek, an adversary would typically use the source code, not the schema, to launch an SQL injection attack or find system vulnerabilities, R. 127-28, and "to attack the system more precisely and more quietly," R. 135. He further opined that "there is already a huge amount of noise" in database systems, and "the schema doesn't change the amount of noise that [an adversary] would generate." R. 135.

Ptacek conceded, however, that if a hacker breached a database, knowledge of the schema would be "of value in that it would allow [the hacker] to select . . . which application . . . to target." R. 146. For example, "[i]t would help isolate the systems that would contain Social Security information," or other sensitive information like credit card numbers, so an adversary "wouldn't have to take the time to attack lots of other applications" without valuable information. R. 149-50; see also R. 137, 146-47. Ptacek also stated that the first thing an adversary would do upon breaching the system is "dump the schema from the system," R. 151, and "then use" it "to make a targeted query of the database," R. 131. For that reason, he rejected the notion that the schema has "no value" to a hacker. R. 161.

Ptacek further acknowledged that he has never worked with CANVAS, does not know "the source code and system architecture," is not "familiar with the varying levels of security that the City has in place," and does "not know all of the details of how that system is configured." R. 157. He testified

that he is "broadly familiar with all of the available options for securing any system that looks like CANVAS," but does not "know how any of the available tools that the City has have been specifically configured." R. 158.

At the close of evidence, the circuit court ruled that DOF had "not met its burden of proof" to show that disclosure of the database schema "would jeopardize the security of the CANVAS system." A21; R. 193. The court explained that, while Coffing testified that knowledge of the schema would allow an adversary to "more precisely plan and execute an attack without making noise," A21; R. 193, he did not "go into it more beyond that, as far as explaining how that would work, at least not in a way that [the court] found persuasive," A22; R. 194. The court acknowledged that the schema may "help guide" an adversary "on which system he might want to pursue," but called that "really of no moment," A23; R. 195, because CANVAS "by definition" contains "the kind of information that would attract a threat actor," A23-A24; R. 195-96. The court entered judgment for Chapman and against DOF and ordered DOF to produce the records Chapman requested. A25; C. 79.

The appellate court affirmed. A18. The court first addressed DOF's claim to a per se exemption for file layouts, rejecting the argument that the "would jeopardize" clause in section 7(1)(o) modifies only the catchall phrase "any other information" that immediately precedes it, and not file layouts and other items specifically enumerated in that section. The court stated that because the language of the statute was unambiguous, it "need not resort to

the last antecedent canon of statutory construction." A10. The court further ruled that this court's decisions in Lieber v. Board of Trustees of Southern Illinois University, 176 Ill. 2d 401 (1997), and Mancini Law Group, P.C. v. Schaumburg Police Department, 2021 IL 126675 – which, DOF explained, instruct how to interpret specifically enumerated FOIA exemptions in section 7 – were not dispositive. A11-A13. The appellate court stated that, although other sub-sections of section 7 contain per se exemptions, section 7(1)(o) does not because "additional requirements are expressly provided," so "those requirements must be satisfied before the requested information may be classified as exempt." A13 (quotation marks omitted). The court stated that under DOF's construction, section 7(1)(o)'s enumerated items "would never be disclosed to the public," which "runs contrary to the principle that FOIA exemptions should be "read narrowly." A14. The court held that "under the plain and ordinary language of section 7(1)(o), the reasonable meaning of 'if disclosed, would jeopardize' must apply to every item listed, not only to the catchall phrase of 'and any other information.'" A14.

The appellate court also interpreted the phrase "would jeopardize." A15-A16. The court held that because the General Assembly used the word "would" instead of "could" in section 7(1)(o), the section requires clear and convincing evidence of "more than the *possibility* of a threat to the security of the CANVAS system," and DOF had not met that burden. A16-A17. The appellate court therefore affirmed the circuit court's judgment. A18. DOF

filed a petition for leave to appeal, which this court allowed.

ARGUMENT

The CANVAS database contains sensitive personal and financial information about individuals cited for parking and traffic violations. Chapman requested information about how data is organized within CANVAS. This information constitutes a "file layout," which, under the plain language of section 7(1)(o), is expressly exempt from disclosure – no specific showing that disclosure would jeopardize the system's security is required. The appellate court's contrary interpretation of section 7(1)(o) departs from its plain language and conflicts with this court's decisions.

And even on the appellate court's view that DOF was required to show that disclosure of the requested information would jeopardize CANVAS's security, DOF's evidence satisfies that standard. The lower courts' contrary conclusion begins with an incorrect reading of the plain language of section 7(1)(o). A public body must show only that disclosure would result in the *possibility* of harm to data system security. The evidence clearly established this here, where it is undisputed that the information Chapman requested could expedite the theft of information from CANVAS.

This appeal raises several questions of statutory interpretation of the exemptions in section 7(1)(o), as well as a challenge to the circuit court's findings. Issues concerning the interpretation of FOIA are reviewed de novo. Rushton v. Department of Corrections, 2019 IL 124552, ¶ 13. The court's

factual findings will be reversed if they are against the manifest weight of the evidence. Corral v. Mervis Industries, Inc., 217 Ill. 2d 144, 154 (2005). A finding is against the manifest weight of the evidence "'when an opposite conclusion is apparent or when the findings appear to be unreasonable, arbitrary, or not based on the evidence.'" Id. at 155 (quoting Eychaner v. Gross, 202 Ill. 2d 228, 252 (2002)). Under these standards, the appellate court's judgment should be reversed.

I. SECTION 7(1)(o) EXPRESSLY EXEMPTS THE RECORDS CHAPMAN REQUESTED FROM DISCLOSURE.

Section 7(1)(o) exempts:

> Administrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, computer program abstracts, *file layouts*, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section.

5 ILCS 140/7(1)(o) (emphasis added). Chapman requested file layouts, one of the enumerated categories of data processing information that are exempt under the section. He requested "an index of the tables and columns within each table of CANVAS" and "the column data type," C. 13; in other words, he sought information about how CANVAS is laid out. Courts appropriately consult dictionaries for undefined terms, Lacey v. Village of Palatine, 232 Ill. 2d 349, 363 (2009)), and when legislation involves technological or scientific matters, courts presume the legislature made "an intentional effort to confer

the flexibility to forestall . . . obsolescence" by using "broad language." Massachusetts v. EPA, 549 U.S. 497, 532 (2007). "File layout" broadly describes "the arrangement of the data in a file." McGraw-Hill Dictionary of Scientific & Technical Terms, 6E (2003), available at https://encyclopedia2.thefreedictionary.com/file+layout (retrieved June 29, 2022); see CMAX/Cleveland, Inc. v. UCR, Inc., 804 F. Supp. 337, 344 n.3 (M.D. Ga. 1992) ("file layout" is the "blueprint for data storage" and the "foundation upon which a computer system is built"). CANVAS's "file layout" is therefore the arrangement of the information in the database, which is what Chapman requested.[3]

As we now explain, section 7(1)(o)'s plain language reflects the General Assembly's intent to expressly exempt file layouts and the other enumerated categories of information from FOIA's disclosure requirements. Because the requested records are per se exempt from disclosure, DOF is not required to show that disclosure "would jeopardize the security of the system," see 5 ILCS 140/7(1)(o), as is required for "any other information" about data processing operations that is not specifically listed.

---

[3] Ptacek called the requested information the "database schema." R. 145. The definitions of "schema" and "file layout" are materially identical. Just as a file layout is the arrangement of data or the blueprint of a database, a schema is the framework, plan, or outline of a database. See, e.g., Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/schema ("framework", "plan," or "outline"). Ptacek stated without explanation that "schemas are not file layouts," R. 145, but he did not identify any difference.

A. Section 7(1)(o) Expressly Exempts File Layouts From Disclosure.

File layouts are per se exempt from disclosure. The first clause of section 7(1)(o) contains general language that exempts "[a]dministrative or technical information associated with automated data processing operations." 5 ILCS 140/7(1)(o). The section then provides that this category of information specifically "includ[es]": "software, operating protocols, computer program abstracts, *file layouts*, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, [and] employee manuals." Id. (emphasis added). Where the General Assembly lists specific examples in a statute, those examples, by definition, "fall within the ambit of the statute." People v. Newton, 2018 IL 122958, ¶ 17; see also People v. Perry, 224 Ill. 2d 312, 328 (2007) (when "including" is "followed by a listing of items," this "means that the preceding general term encompasses the listed items"). Because the list in section 7(1)(o) includes file layouts, they are among the items deemed "administrative or technical information associated with data processing operations," and, as such, are expressly exempt.

In addition to listing specific categories of information that are exempt, the General Assembly also included a catchall category of "any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section." 5 ILCS 140/7(1)(o). Nothing about this catchall provision alters the automatic, per se

exemption for the items that appear before it on the list. Rather, the catchall provision reflects the General Assembly's recognition "that it would not be possible to specifically list" every example that may fall within the statute's scope. Newton, 2018 IL 122958, ¶ 17. This makes sense given that FOIA was enacted in 1983, and at that time, the General Assembly could not have predicted the technological innovations and attendant security risks that would arise in the future. Thus, items specifically listed in section 7(1)(o) – including file layouts – are those the General Assembly had, in 1983, already determined would, if disclosed, jeopardize data system security, while the catchall allows for the exemption of additional information upon a showing that disclosure would jeopardize security.

As we now explain, multiple other features of section 7(1)(o)'s statutory language likewise confirm that the categories of documents listed before the catchall provision are per se exempt.

1. The last antecedent rule supports a per se exemption for file layouts.

Application of the last antecedent rule requires an interpretation that expressly exempts file layouts from disclosure. "The last antecedent is the last word, phrase or clause that can be made an antecedent without impairing the meaning of the sentence." Advincula v. United Blood Services, 176 Ill. 2d 1, 26-27 (1996). Under the rule, "qualifying words or phrases in a statute serve only to modify words or phrases which are immediately preceding" and are not construed as extending to "those which are more

remote." McMahan v. Industrial Commission, 183 Ill. 2d 499, 511-12 (1998); see also In re E.B., 231 Ill. 2d 459, 467 (2008).

This court has routinely applied the last antecedent rule, as have other state and federal courts. E.g., Lockhart v. United States, 577 U.S. 347, 351 (2016) ("This Court has applied the [last antecedent] rule from our earliest decisions to our more recent."). For example, in McMahan, this court construed section 16 of the Workers' Compensation Act, which authorizes an award of attorney's fees when the employer is "'guilty of unreasonable or vexatious delay, intentional under-payment of compensation benefits, or has engaged in frivolous defenses which do not present a real controversy, within the purview of the provisions of paragraph (k) of Section 19 of this Act.'" 183 Ill. 2d at 511 (quoting 820 ILCS 305/16 (1992)). Rejecting the employer's argument that "within the purview of the provisions of paragraph (k) of Section 19" modifies the phrase "unreasonable or vexatious delay," the court applied the last antecedent rule to hold that, because the "final qualifying phrase 'within the purview of [section 19(k)]' is not immediately preceded by the clause 'unreasonable or vexatious delay,'" but rather is separated from it by two other clauses, the "'unreasonable or vexatious delay' does not have to fall 'within the purview of [section 19(k)]' before section 16 attorney['s] fees can be awarded." Id. at 511-12; see also In re E.B., 231 Ill. 2d at 467; Advincula, 176 Ill. 2d at 26-27; Benjamin v. Cablevision Programming Investments, 114 Ill. 2d 150, 167-68 (1986); Lockhart, 577 U.S. at 350 (all

applying the last antecedent rule to hold that a qualifying phrase modified only the immediately preceding phrase in a statute).

Applying the last antecedent rule to section 7(1)(o), the qualifying phrase "that, if disclosed, would jeopardize the security of the system or its data" modifies only the immediately preceding clause "any other information," not the items listed earlier in section 7(1)(o). The listed items are therefore per se exempt from disclosure, with no additional showing of possible harm required.

The appellate court, for its part, did not disagree with this application of the last antecedent rule; it simply declined to apply it. A10. Although it acknowledged that the rule is "'a long-recognized grammatical canon of statutory construction,'" id. (quoting In re E.B., 231 Ill. 2d at 467), it stated that courts do not employ "canons of statutory construction" unless a statute is ambiguous, and that, according to DOF, section 7(1)(o) was not ambiguous. Id. The court then held that the qualification, "that if disclosed, would jeopardize the security of the system" applies to all information specifically listed in section 7(1)(o). A14. This analysis suffers from several flaws.

To begin, the appellate court used DOF's characterization of section 7(1)(o) as unambiguous to avoid meaningfully engaging with the provision's text itself. The court stated,

> [DOF] argues that "the *plain* language of section 7(1)(o) is a *clear* indication of the General Assembly's intent to expressly exempt file layouts from FOIA's disclosure requirements without proof that disclosing such information 'would jeopardize

> the security of the system.'" (Emphasis added.) Thus, [DOF], as confirmed during oral arguments, does not contend that the statute is ambiguous. For that reason, we need not resort to the last antecedent canon of statutory construction to interpret section 7(1)(o) as urged by [DOF].

A10. This analysis cannot stand. DOF argued that the statute has only one meaning *when read in accord with the last antecedent and other grammatical rules*: enumerated categories of information are per se exempt from disclosure. It therefore did not make sense for the appellate court to justify its *refusal* to apply the last antecedent rule by pointing to DOF's position. Furthermore, because a statute is ambiguous only when there is more than one genuinely reasonable interpretation of the text, e.g., Dynak v. Board of Education of Wood Dale School District 7, 2020 IL 125062, ¶ 16, the court's first step should have been to investigate the meaning of the statutory text. "[W]hether [a] statute is ambiguous" is a "threshold task" for the court to determine, not something a party can concede. Hyatt Corp. v. Sweet, 230 Ill. App. 3d 423, 429 (1st Dist. 1992) ("[W]e are not bound by the agreement of the parties that the statute is not ambiguous."). The appellate court therefore should not have avoided addressing whether section 7(1)(o)'s meaning is clear by relying on what it construed as a concession by DOF that the provision is unambiguous.

A second problem with the appellate court's analysis is its determination that the last antecedent rule is irrelevant because "[c]anons of statutory construction only apply if the language of the statute is

ambiguous." A10 (citations omitted). As the court acknowledged, the last antecedent rule is not merely a method of statutory interpretation, but also a "'grammatical'" rule. Id. (quoting In re E.B., 231 Ill. 2d at 467 (calling the rule "a long-recognized grammatical canon")); see also Lockhart, 577 U.S. at 361 (calling the rule "a sensible grammatical principle"). The court decided to completely ignore this grammatical rule. But rules of grammar guide the reading of any sentence, including one that is in a statute. Indeed, grammar is the most essential tool in the toolkit courts use to assess a statute's plain meaning. Accordingly, this court has held that "[s]tatutes . . . are to be read and understood primarily according to their grammatical sense, unless it is apparent from a perusal of the context of the whole statute that the Legislature did not express its intention." Warner v. King, 267 Ill. 82, 87 (1915). Not surprisingly, then, even when there is no claim of ambiguity, the appellate court has interpreted statutory terms according to "commonly understood principles of grammar and usage." Lyons Township ex rel. Kielczynski v. Village of Indian Head Park, 2017 IL App (1st) 161574, ¶ 26.[4]

Thus, contrary to the appellate court's suggestion that grammar rules like the last antecedent rule apply only if "the statute is ambiguous," A10, such rules are meant to help the court to determine *whether* a statute is

[4] If, *after* applying grammar principles, which are "intrinsic aids" to interpretation, a statute remains susceptible to multiple meanings, the court may use extrinsic, or extra-textual, aids of statutory construction, such as legislative history or narrow construction. In re E.B., 231 Ill. 2d at 469.

ambiguous. Nothing in section 7(1)(o) or elsewhere in FOIA suggests the General Assembly intended an interpretation other than one that follows established principles of grammar. Applying those principles, file layouts are per se exempt from disclosure under section 7(1)(o).

2. Numerous other features of the statute's plain language support a per se exemption for file layouts.

The appellate court ignored at least four other significant aspects of section 7(1)(o) that undermine the court's interpretation. First, the catchall phrase begins, "*any other information that*, if disclosed, would jeopardize the security of the system." 5 ILCS 140/7(1)(o) (emphasis added). No comma separates "any other information" and "that." The absence of punctuation is significant. As this court has explained, a lack of "punctuation setting [a] qualifying phrase apart from the sentence which precedes it" indicates that it qualifies "only the immediately preceding phrase." Advincula, 176 Ill. 2d at 27. In contrast, "'[e]vidence that a qualifying phrase is supposed to apply to all antecedents instead of only to the immediately preceding one may be found in the fact that it is separated from the antecedents by a comma.'" In re E.B., 231 Ill. 2d at 468 (quoting 2A N. Singer, Sutherland on Statutory Construction § 47:33, at 373 (6th ed. 2000)). Here, the absence of a comma indicates that the qualifying language, "that if disclosed, would jeopardize the security of the system," directly modifies only the immediately preceding words, "any other information," not the prior list of enumerated materials.

Second, the catchall provision exempts "any other information that, if disclosed, would jeopardize the security of the system or its data *or the security of materials exempt under this Section*." 5 ILCS 140/7(1)(o) (emphasis added). The reference to "materials exempt under this Section" assumes that the specifically enumerated categories of materials listed in section 7(1)(o) are, in fact, exempt. Indeed, the reference would be meaningless were those materials *not* exempt. And, of course, a statute must be construed so that none of its words are "rendered superfluous." Sylvester v. Industrial Commission, 197 Ill. 2d 225, 232 (2001).

Third, the General Assembly would have had no reason to list specific categories of information in section 7(1)(o) categories if a particularized showing of potential harm were required any time a public body invoked the exemption. It could have simply written, "Administrative or technical information associated with automated data processing operations that, if disclosed, would jeopardize the security of the system or its data." Written thus, the qualifying language, "that if disclosed, would jeopardize the security of the system," would apply to any requested information about data systems. But instead of this short, simple formulation, the General Assembly chose to enumerate ten specific categories of information "includ[ed]" in the exemption. 5 ILCS 140/7(1)(o). Again, statutory language should not be "rendered superfluous," Sylvester, 197 Ill. 2d at 232, and the General Assembly's decision to specifically list these materials is meaningful only if

they are per se exempt from disclosure.

Fourth, the larger context of section 7(1) shows this subsection creates per se exemptions. When the General Assembly intended each item in a list of FOIA exemptions to be subject to a specific showing, it used different language. In section 7(1)(o), no comma separates the words "any other information" and the qualifying phrase "that, if disclosed." Sections 7(1)(d), (k), and (v), on the other hand, all end with a comma followed by the phrase, "but only to the extent that disclosure . . . ." 5 ILCS 140/7(1)(d), (k), (v). And sections 7(1)(d)(v) and 7(1)(g) each end their lists with a comma followed by the phrase "and disclosure would" or "and that disclosure . . . would." Id. 7(1)(d)(v), (g). The court should assume the General Assembly's decision to use different wording and punctuation in section 7(1)(o) was deliberate. "'When the legislature includes particular language in one section of a statue but omits it in another section of the same statute, courts presume that the legislature acted intentionally and purposely in the inclusion or exclusion, and that the legislature intended different meanings and results.'" People v. Clark, 2019 IL 122891, ¶ 23 (quoting Chicago Teachers Union, Local No. 1 v. Board of Education, 2012 IL 112566, ¶ 24)). The General Assembly's choice to offset qualifying phrases with a comma elsewhere in section 7(1), but not in section 7(1)(o), reinforces that section 7(1)(o)'s qualifying phrase modifies only the immediately preceding phrase "any other information."

The appellate court ignored all these features of the plain language.

Indeed, the appellate court provided no meaningful analysis of the statutory text at all, much less an explanation of what grammatical principles allowed it to conclude that the "would jeopardize" qualification applies to all the enumerated categories of information listed in section 7(1)(o). The closest the court came was to allude in a parenthetical to the fact that the use of "and" rather than "or" within a list of requirements means that "*all* of the listed requirements" must be met. See A14 (quoting DG Enterprises, LLC-Will Tax, LLC v. Cornelius, 2015 IL 118975, ¶ 31). To the extent that grammatical principle is relevant, however, it undermines the court's interpretation. Here, the statute contains a list of categories of exempt materials rather than "requirements," so the use of "and" indicates only that all categories listed are exempt. Nothing about the use of the conjunctive "and" justifies the court's conclusion that the "would jeopardize" qualification applies to every category listed in the section.

Instead of addressing the plain language of the provision, the appellate court stated that "a blanket prohibition against disclosure of the items separately listed in section 7(1)(o) runs contrary to the principle that FOIA exceptions are to be read narrowly." A14. Ironically, the appellate court purported to apply this canon of construction even after stating, as justification for ignoring the last antecedent rule, that canons of construction do *not* apply. A10. Moreover, this approach was an incorrect application of the principle of narrow construction. Even a "narrow" reading requires the

court to read the statutory language and give its words their plain meaning. Neither "narrow construction," nor any other interpretive guideline, can override plain and easily understood statutory language. "There is no rule of construction which authorizes a court to declare that the legislature did not mean what the plain language of the statute imports." People ex rel. LeGout v. Decker, 146 Ill. 2d 389, 394 (1992); see also, e.g., Lockhart, 577 U.S. at 361 ("We will not apply the rule of lenity to override a sensible grammatical principle buttressed by the statute's text and structure."). Here, even narrowly construed, the plain language of section 7(1)(o) clearly provides that enumerated categories of information are per se exempt from production. The appellate court erred in holding otherwise.[5]

B. The Appellate Court's Reading Of Section 7(1)(o) Cannot Be Squared With This Court's Precedent.

This court's interpretations of other FOIA exemptions further support that file layouts are per se exempt. In Lieber, this court considered an exemption under a prior version of section 7(1)(b), which specifically identified certain categories of personal information, then included a catchall category – much like the catchall category at issue here – for "information

[5] The appellate court expressed concern that, were the items listed in section 7(1)(o) per se exempt, "user guides and employee manuals[ ] would never be disclosed to the public." A14. But section 7(1)(o) refers to "user guides and employee manuals" that are specifically about "*automated data processing operations*," 5 ILCS 140/7(1)(o) (emphasis added). It is unsurprising that the General Assembly would exempt those technical materials from disclosure; their release could obviously compromise data system security.

that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy." 176 Ill. 2d at 408-09. This court explained that when a document falls within one of the "specifically enumerated categories," it is per se exempt. Id. at 408. Thus, any records in the listed category at issue, "personal information maintained with respect to students or other individuals receiving educational services from a public body," would "by definition constitute 'information that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy and be automatically exempt from disclosure.'" Id. at 409-10 (alteration omitted) (quoting 5 ILCS 140/7(1)(b)(i) (1994)). The court would not need to make an "individualized assessment of whether disclosure of the information would invade anyone's personal privacy." Id. at 409.[6]

This court recently reiterated this analysis in Mancini, 2021 IL 126675, explaining that Lieber "made clear that a '*per se*' approach was to be followed where information fell into the specific, narrow exemptions set forth in section 7." Id. ¶ 30 (citing Lieber, 176 Ill. 2d at 409). It again emphasized that information that falls into "'one of these specifically enumerated categories'" is "'by definition'" exempt, without further inquiry, adding that "[t]his per se rule

[6] Lieber held that the information the plaintiff requested fell outside the enumerated exemption on which the public body relied, section 7(1)(b)(i), and therefore the court assessed whether disclosure "'would constitute a clearly unwarranted invasion of personal privacy,'" to decide whether the information was exempt under the catchall category. Id. But that analysis was required only because the per se exemption was inapplicable.

applies to most of the section 7 exemptions." Id. (quoting Lieber, 176 Ill. 2d at 408-09). And, it explained, Illinois FOIA exemptions are structured differently than those of the federal FOIA, in that "certain exemptions do not require a balancing test" because "where information falls under the express terms of a FOIA exemption," it is "automatically exempt from disclosure." Id. ¶ 50 n.9.[7]

This court has taken the same approach outside the FOIA context, too. In Newton, it considered a statute providing an enhanced penalty for drug offenses occurring "within 1,000 feet of the real property comprising any church, synagogue, or other building, structure, or place used primarily for religious worship." 2018 IL 122958, ¶ 16 (quoting 720 ILCS 570/407(b)(2) (2014)). The defendant, charged with delivering a controlled substance within 1,000 feet of a church, argued that the state was required to prove the church was "used primarily for religious worship." Id. ¶ 12. Rejecting this argument, the court explained that churches and synagogues are "examples of buildings that are, by definition, used primarily for religious worship," and the General Assembly "has already determined that a church or synagogue meets that requirement." Id. ¶ 17. The state would need to offer "particularized evidence" only if it was claiming that some "other" building,

[7] The parties in Mancini did not dispute that the requested information about traffic accident reports, which fell within the specific exemptions listed in sections 7(1)(b) and 7(1)(c), was per se exempt. Id. ¶ 37.

structure, or place was used primarily for religious worship. Id. ¶¶ 18, 22.

Under this court's precedents in Lieber, Mancini, and Newton, when a public body denies a request for records that are specifically identified in section 7(1)(o), it need not specifically demonstrate that disclosure "would jeopardize the security of the system." Like the statutory provisions creating the per se exemptions addressed in Mancini and Lieber, section 7(1)(o) carves out a specific exemption for "file layouts," so no evidentiary showing is necessary for the exemption to apply.

The appellate court's attempt to distinguish that precedent should be rejected. The court stated that the exemption Lieber addressed was "markedly different" because the phrase "*[i]nformation exempted* under this section (b) *shall include*" appeared before the list of exempted categories, while the General Assembly "did not include the directive 'shall include'" in section 7(1)(o). A12-A13. But section 7(1)(o) uses the word "including," and the court did not explain why this was materially different from the language addressed in Lieber. Regardless, this was no basis to cast Lieber aside. After all, this court discussed Lieber's analysis approvingly in Mancini, without discussing that phrase and with respect to provisions that did not contain the phrase. See 2021 IL 126675, ¶ 30.

The appellate court also stated that the section at issue in Lieber had been amended, and that Mancini was inapplicable because it (and Lieber) concerned a privacy exemption, whereas here, "no such privacy concerns are

implicated because . . . Chapman did not request any of the actual data in the fields." A13. But the interpretive principles underlying the analysis of Lieber and Mancini are not limited to cases involving the particular exemption at issue in Lieber. On the contrary, in both Lieber and Mancini, this court stated that the "per se" rule applies to other section 7 exemptions as well. Mancini, 2021 IL 126675, ¶ 30; Lieber, 176 Ill. 2d at 408.

Finally, it is worth noting that the section 7(1)(o) exemption implicates "privacy concerns" just as much as the exemptions addressed in Lieber and Mancini. Section 7(1)(o) is designed to safeguard data systems containing sensitive information. Although Chapman claims he does not seek the "actual data in the fields," he does not dispute that CANVAS contains sensitive data. By protecting information about the way CANVAS is organized, including its file layouts, from disclosure, the exemption helps to secure that data.

Because Chapman requested file layouts, which are per se exempt from disclosure under section 7(1)(o), DOF properly withheld the records.

II. DOF MET ITS BURDEN TO PROVE DISCLOSURE WOULD JEOPARDIZE CANVAS'S SECURITY.

Even on the appellate court's view that DOF was required to prove that disclosure of the requested records would jeopardize CANVAS's security, the judgment below cannot stand. The appellate court applied the wrong legal standard, concluding that DOF failed to show by clear and convincing evidence that disclosure of the requested records would create "more than the

possibility of a threat to the security of the CANVAS system." A16-A17. That heightened showing was not required. Instead, section 7(1)(o) requires only that a public body show a possibility of harm to the security of a data system. And the undisputed evidence that file layouts would aid an adversary attempting to attack CANVAS was sufficient to establish that possibility.

A. Section 7(1)(o) Requires A Public Body To Show Only A Possibility Of Harm To A Data System's Security.

Section 7(1)(o)'s catchall category exempts information "that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section." 5 ILCS 140/7(1)(o). Beginning again with the statute's plain language, which "is the most reliable indication of legislative intent," JPMorgan Chase Bank, N.A. v. Earth Foods, Inc., 238 Ill. 2d 455, 461 (2010), the operative verb in this phrase is "jeopardize," the ordinary meaning of which can be ascertained from dictionary definitions, see Lacey, 232 Ill. 2d at 363. Jeopardize means "to expose to danger or risk," Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/jeopardize; to "endanger," American Heritage Online Dictionary, https://ahdictionary.com/word/search.html?q=jeopardize; and "to put something in danger," Cambridge Online Dictionary, https://dictionary.cambridge.org/us/dictionary/english/jeopardize. The terms "risk" and "danger" are defined, in turn, as "the possibility of loss or injury,"

Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/risk; "to expose to peril" or, in other words, "to expose to the risk of harm or loss" or the "possibility of" harm or loss, American Heritage Dictionary, https://ahdictionary.com/word/search.html?q=risk; and "the possibility of harm," Cambridge Online Dictionary, https://dictionary.cambridge.org/us/dictionary/english/danger. Thus, to show that disclosure of information "would jeopardize" data system security, a public body need demonstrate only that disclosure of the requested information would create a *possibility* of harm to the security of the system.

The appellate court ignored the plain meaning of "jeopardize" and ruled that DOF must show "more than the *possibility*" of harm because section 7(1)(o) requires proof that disclosure "would," rather than merely "could," jeopardize security. A16. To be sure, "would" suggests certainty, while "could" does not. But the word "jeopardize" must also be given effect, and that word alone connotes uncertainty. By failing to consider the significance of the word "jeopardize," the appellate court erred by holding DOF to a higher burden than the General Assembly intended.

Section 7 of FOIA as a whole confirms our interpretation. The language the General Assembly used in other section 7 exemptions differs from that of section 7(1)(o). For example, section 7(1)(c) exempts personal information contained in public records, "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 ILCS

140/7(1)(c). Section 7(1)(d)(v) exempts certain records created for law enforcement purposes if "disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request." Id. 7(1)(d)(v). Section 7(1)(g) exempts trade secrets or commercial or financial information obtained from a person or business if disclosure "would cause competitive harm to the person or business." Id. 7(1)(g). And, finally, section 7(1)(k) exempts architects' plans, engineers' technical submissions, and other construction-related documents, "but only to the extent that disclosure would compromise security." Id. 7(1)(k). In each instance, the General Assembly used language describing a higher showing than "would jeopardize." And in two of these provisions, the harm must be "clear" or "demonstrable." Had the General Assembly intended to impose a similarly strict standard under section 7(1)(o), it would have used similarly definite language, rather than merely requiring a showing that disclosure would jeopardize, or pose a risk to, security.

Moreover, our reading is necessary to afford the level of protection the General Assembly intended for this type of information. Section 7(1)(o) is designed to protect the security of databases with sensitive personal and financial information. Requiring a showing that harm is probable, rather than possible, could enable the theft or manipulation of information. While courts typically construe FOIA exemptions narrowly in favor of disclosure, an interpretation must accord with "the legislature's intention or the spirit of

the statute." Kelly v. Village of Kenilworth, 2019 IL App (1st) 170780, ¶ 29. FOIA seeks to balance the goals of transparency in local government against the need to shield private information from disclosure and avoid burdens on local governments. 5 ILCS 140/1. In this case, disclosure of the requested information would do little to "shed light on the Department's actions or behavior," but would risk "'dire consequences of identity theft and other forms of fraud' attendant to disclosure of an individual's private information." Mancini, 2021 IL 126675, ¶ 54 (quoting Sherman v. U.S. Department of the Army, 244 F.3d 357, 365-66 (5th Cir. 2001)). The broad language the General Assembly used in section 7(1)(o) is necessary to avoid those possibly dire consequences.

Case law interpreting the federal FOIA reinforces our position as well. The General Assembly "patterned FOIA after the federal FOIA," and given the "similarity of the statutes, Illinois courts often look to federal case law construing the federal FOIA for guidance." In re Appointment of Special Prosecutor, 2019 IL 122949, ¶¶ 54-55; see also Mancini, 2021 IL 126675, ¶ 38 ("We . . . rely on . . . federal case law that is directly applicable to the issue before us."). The federal FOIA provision most analogous to section 7(1)(o) is 5 U.S.C. § 552(b)(7)(E) ("exemption 7(E)"), which exempts from disclosure records of information compiled for law enforcement purposes if their production "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law

enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). Because "[c]ourts have repeatedly recognized the risk of a cyber-attack as valid grounds for withholding under Exemption 7(E)," Prechtel v. FCC, 330 F. Supp. 3d 320, 335 (D.D.C. 2018) (alteration and quotation marks omitted), that exemption serves the same interests that section 7(1)(o) serves here.

Courts have interpreted the phrase "could reasonably be expected to risk circumvention of the law," which is similar to section 7(1)(o)'s phrase "would jeopardize," as requiring merely "the *chance* of a reasonably expected risk," rather than "an actual or certain risk" or "an undeniably or universally expected risk." Mayer Brown LLP v. IRS, 562 F.3d 1190, 1193 (D.C. Cir. 2009) (emphasis added). The D.C. Circuit rejected the idea that an agency "has a high burden to specifically prove how the law will be circumvented," noting that it was "aware the language of FOIA's exemptions must be narrowly construed," but "broad language" – like that used in exemption 7(E) – "is still broad language," even when it is "construed narrowly." Id. at 1194 (quotation omitted); see also Shapiro v. DOJ, 893 F.3d 796, 800 (D.C. Cir. 2018) (Exemption 7(E) is "a relatively low bar," requiring only that the agency "demonstrate logically how the release of the requested information might create a risk of circumvention of the law.") (quotation and alteration omitted). Like exemption 7(E), section 7(1)(o) also sets a relatively low bar to

show a *possibility* of harm.

In sum, section 7(1)(o)'s plain language and analogous federal case law demonstrate that to invoke the catchall exemption, a public body need show only the possibility that disclosure of requested records would harm the security of a data system. As we now explain, the undisputed evidence demonstrates that DOF made that showing.

B. DOF Showed That Disclosure Of The Database Schema Would Jeopardize CANVAS's Security.

The undisputed evidence demonstrates that the materials Chapman requested would jeopardize CANVAS's security, and that DOF properly withheld the materials under section 7(1)(o)'s catchall provision. "A 'public body can meet its burden to show that an exemption applies only by providing some *objective* indicia that the exemption is applicable under the circumstances.'" Garlick v. Naperville Township, 2017 IL App (2d) 170025, ¶ 49 (alteration omitted) (quoting Illinois Education Association v. Board of Education, 204 Ill. 2d 456, 470 (2003)). Where security concerns are present, however, a ruling for the agency is warranted where the justification for disclosure is described in reasonable detail and is "'not controverted by either contrary evidence in the record nor by evidence of agency bad faith.'" Wolf v. CIA, 473 F.3d 370, 374 (D.C. Cir. 2007) (quoting Miller v. Casey, 730 F.2d 773, 776 (D.C. Cir. 1984)). DOF satisfied those standards here, where both parties' witnesses agreed that the requested information would benefit potential hackers. The circuit court's contrary conclusion is against the

manifest weight of the evidence.

On DOF's behalf, Coffing testified that "limiting the information known about" CANVAS is a layer of defense used to protect it. R. 61-62. As Coffing explained, an adversary with less information about the system will be "noisy when they are attempting their attack," alerting the system's defenders "that an attack is underway." R. 62. Without the schema, or file layouts, an adversary would have to guess the field names, and inaccurate guesses would "generate errors" and "generate logs" that would signal a possible "threat actor in the environment." R. 92-93. But when an adversary has "precise information about the system, . . . their activity may blend in and look like normal activity." R. 63. They can "more precisely craft their attack" and "limit the likelihood of them being detected." R. 69. Thus, DOF provided evidence that, at a minimum, having the information would save a hacker time, and it could potentially allow them to evade detection.

Ptacek's testimony aligned with Coffing's in several significant ways. He admitted that the schema has "some value to [an adversary] in helping him plan his attack," R. 151-52, as it would allow an adversary to "choose which application . . . to go after," R. 149. He agreed that knowledge of the schema would "help [an adversary] isolate the systems" that contain sensitive information, "so [the adversary] wouldn't have to take the time to attack lots of other applications." R. 149-50. In addition, Ptacek admitted that, although the schema will not aid an adversary in breaching the database in

the first place, it may help him once inside the database. R. 131. As Ptacek described it, the schema is usually "the product of an attack and not the predicate," R. 136, meaning once an adversary breaches the system, he would then extract the schema, R. 131, 152, and use it "to make a targeted query of the database," R. 131. But that means that a hacker who already has the schema can skip the first step. Thus, not only did Ptacek's testimony fail to undermine Coffing's testimony that knowledge of the schema would benefit an adversary and therefore jeopardize CANVAS's security, it corroborated it.

The facts in this case are strikingly similar to those in Long v. ICE, 464 F. Supp. 3d 409 (D.D.C. 2020), in which a federal district court applied exemption 7(E) to a request for database schema. There, the plaintiffs requested from Immigration and Customs Enforcement ("ICE"): (1) names of database tables and fields; (2) codes used to record data in the databases; and (3) the "database schemas," or "the way various database tables connect to each other." Id. at 414. ICE withheld the records under exemption 7(E). Id. at 411. At a bench trial, the parties' witnesses explained that the "database schema provides the blueprint of a database," and included "the names of tables and fields." Id. at 418 (quotation and alterations omitted). ICE's witness testified that the "primary risk" in disclosing the schema is that it would enable "a hacker . . . to carry out a more efficient and effective cyberattack." Id. at 419. An adversary who "know[s] how a database is organized" can make its "attack very targeted, less likely to be noticed," and

can "cover up [its] tracks." Id. (quotation and alterations omitted). The requested information would thus allow a hacker who managed to gain access to the database "the means to create greater mischief once inside." Id. The court found that ICE satisfied its burden of proving that disclosure of the database schema would risk circumvention of the law, explaining that the agency's security countermeasures did not make access impossible, and that "greater harm might result from a cyberattack where the attacker has detailed advanced knowledge of the structure and organization of the database." Id. The court likened the schema to a "thieves' map" or "blueprints of the databases that lay out exactly where everything is and how it's stored," which could "reduce the number of queries necessary for a hacker to accomplish his attack, thereby making the attack more efficient." Id. (quotation omitted). While this "delta of time would be small," that benefit was "sufficient" to satisfy exemption 7(E), "particularly given the highly sensitive nature of the law enforcement information contained in the databases." Id. (quotation omitted).

Importantly, in reaching its decision, the Long court emphasized that the plaintiffs' expert was not familiar with the specific database, and some deference was owed to ICE's witness because of his knowledge of the system. Long, 464 F. Supp. 3d at 421; see also Wolf, 473 F.3d at 374 (giving "substantial weight" to agency's determination that disclosure would threaten security); Sheridan v. U.S. Office of Personnel Management, 278 F.

Supp. 3d 11, 25 (D.D.C. 2017). "'Judges are not cyber specialists,'" the court cautioned, "'and it would be the height of judicial irresponsibility for a court to blithely disregard such a claimed risk'" from someone familiar with the database. Long, 464 F. Supp. 3d at 421 (quoting Long v. ICE, 149 F. Supp. 3d 39, 53 (D.D.C. 2015)); see also Shapiro v. DOJ, 393 F. Supp. 3d 111, 122 (D.D.C. 2019) (deferring to agency's assertion that disclosure of database name could jeopardize its security "by making it a more attractive target for compromise") (quotation omitted).

Here, in contrast to the Long court's approach, the circuit court disregarded the risks that DOF identified. As the Long court emphasized, any small amount of time an adversary can save in launching an attack creates a risk to the security of a data system. 464 F. Supp. 3d at 422. The public body thus need only show that knowledge of the database schema would afford an adversary some small advantage in attacking the system to justify withholding that information. The circuit court, however, found that "[h]aving the schema . . . does not make it easier to do a SQL attack," because the "source code . . . is necessary to attack the system," R. 195, and that any benefit the schema has in helping an adversary identify applications to target "is really of no moment" because an adversary could infer what type of data CANVAS contains, R. 195-96. These findings appear to be based on Ptacek's testimony describing the ways hacking might be accomplished without schema. R. 127-28, 139, 152-53. But the court ignored Ptacek's own

testimony about how having the schema could speed up the hacking process, and it failed to recognize that the time saved would benefit an adversary attempting to move quickly through the system to avoid detection.

Moreover, to the extent there was any material difference between Coffing's and Ptacek's testimony on this point, the circuit court should have accorded due weight to the testimony of Coffing, the official responsible for the system. See Long, 464 F. Supp. 3d at 421 (deferring to agency's witness, who knew more about the particular database at issue). Coffing was the only witness with direct knowledge about how CANVAS is configured, the defenses used to protect it, and cybersecurity threats to the system. In contrast, Ptacek admitted that he has "never worked with the CANVAS system," "does not know all of the source code and system architecture," and does not "know all of the details of how that system is configured." R. 157-58.

Finally, it is worth noting one significant way in which the potential for hacking is even greater here than it was in Long. Chapman has indicated that if he obtains CANVAS's file layouts, he will make that information accessible to the general public, C. 15, 17; without such public disclosure, an adversary is less likely to be aware of CANVAS at all. The circuit court brushed this concern aside because CANVAS "by definition" contains "the kind of information that would attract a threat actor." R. 195-96. But the circuit court ignored that publicly disclosing the schema would highlight to potential attackers that CANVAS contains sensitive data. And when

disclosure would reveal where a public body stores sensitive data, that in itself increases vulnerability and justifies applying an exemption. See Shapiro, 393 F. Supp. 3d at 122.

In sum, the undisputed evidence demonstrates that DOF established that disclosure would jeopardize CANVAS's security. Thus, even on the view that such a showing is required, DOF is entitled to judgment.

* * * *

Section 7(1)(o) is critical to the security of databases maintained by public bodies throughout the state. Many of those databases contain sensitive personal and financial information about the public or information related to law enforcement. By imposing on public bodies a higher standard of proof than the General Assembly intended, the appellate court's decision puts those systems in danger of theft or manipulation.

CONCLUSION

This court should reverse the appellate court's judgment.

Respectfully submitted,

Corporation Counsel
of the City of Chicago

BY: /s/ Ellen Wight McLaughlin
ELLEN WIGHT MCLAUGHLIN
Assistant Corporation Counsel
2 North LaSalle Street, Suite 580
Chicago, Illinois 60602
(312) 742-5147
ellen.mclaughlin@cityofchicago.org
appeals@cityofchicago.org

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rule 341(a) & (b). The length of this brief, excluding the pages containing the Rule 341(d) cover, the Rule 341(h)(1) table of contents and points and authorities, the Rule 341(c) certificate of compliance, and the certificate of service, is 41 pages.

/s/ Ellen W. McLaughlin
ELLEN WIGHT MCLAUGHLIN, Attorney

CERTIFICATE OF FILING/SERVICE

I certify under penalty of law as provided in 735 ILCS 5/1-109 that the statements in this instrument are true and correct and that the foregoing brief was electronically filed with the office of the Clerk of the Court using the File and Serve Illinois system and served via email, to the persons named below at the email addresses listed, on August 4, 2022.

Matt Topic
Merrick Wayne
LOEVY & LOEVY
311 North Aberdeen Street, Suite 300
Chicago, Illinois 60607
foia@loevy.com

/s/ Ellen W. McLaughlin
ELLEN W. MCLAUGHLIN, Attorney

APPENDIX

TABLE OF CONTENTS OF THE APPENDIX

Page

2022 IL App (1st) 200547

FIRST DISTRICT
FIRST DIVISION
February 14, 2022

No. 1-20-0547

MATT CHAPMAN, Plaintiff-Appellee, v. THE CHICAGO DEPARTMENT OF FINANCE, Defendant-Appellant.	)))))))))	Appeal from the Circuit Court of Cook County No. 18 CH 14043 The Honorable Sanjay T. Tailor, Judge Presiding.

JUSTICE COGHLAN delivered the judgment of the court, with opinion.
Presiding Justice Hyman and Justice Walker concurred in the judgment and opinion.

OPINION

¶ 1 Following a bench trial, the trial court granted plaintiff Matt Chapman's Freedom of Information Act (FOIA) (5 ILCS 140/1 *et seq.* (West 2018)) request directed at defendant the Chicago Department of Finance (Department), seeking disclosure of an "index of the tables and columns within each table" of the Citation Administration and Adjudication System (CANVAS), a system used to store, process, and track citation information for parking tickets, speed-light camera tickets, stoplight traffic tickets, booting, and towing tickets. On appeal, the Department argues that the requested information was exempt from disclosure because it constituted a "file layout" and its dissemination "would jeopardize" the security of the CANVAS system and database. We affirm.

¶ 2 I. BACKGROUND

¶ 3 On August 30, 2018, Chapman submitted the following to the Department:

"To Whom It May Concern:

1-20-0547

Pursuant to the Illinois Freedom of Information Act, I hereby request the following records:

An index of the tables and columns within each table of CANVAS. Please include the column data type as well.

Per the CANVAS specifications, the database in question is Oracle, so the below SQL query will likely yield the records pursuant to this request:

select utc .column_name as colname, uo.object_name as tablename, utc.data_type from user_objects uo

join user_tab_columns utc on uo.object_name = utc.table_name where uo.object_type = 'TABLE'

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

***

Sincerely,

Matt Chapman – Free Our Info, NFP"

On September 12, 2018, the Department notified Chapman of its decision to deny his request, stating that the requested records were exempt from disclosure because the "dissemination of [the] pieces of network information could jeopardize the security of the systems of the City of Chicago." On September 17, 2018, Chapman disputed the Department's decision, arguing that "database schemas are specifically releasable through FOIA."[1] On October 2, 2018, after consulting with the City of Chicago's (City) law department, the Department reiterated its decision to deny the FOIA request.

[1]Chapman stated that the released records would be added to Chicago's public "Data Dictionary" (a/k/a "metalicious") and "will be used for further research of parking tickets."

¶ 4 On November 1, 2018, Chapman filed a complaint, asserting a "willful violation of the Freedom of Information Act, to respond to [his] Freedom of Information Act requests seeking records regarding database schema information of CANVAS, a system used to store parking ticket information." The parties filed cross-motions for summary judgment. The Department's motion included the affidavit of Bruce Coffing, chief information security officer with the city's Department of Innovation and Technology (DoIT), attesting that the "[r]elease of the requested information, especially in combination with the information already made public about the CANVAS system, would jeopardize the security of not only the CANVAS system and database, but also the data contained therein." Chapman's motion included the affidavit of Thomas Ptacek, an information and software security "vulnerability researcher," attesting that "[w]ith respect to the security of a computer application backed by a database, knowledge of the 'schema'—the collection of tables and their constituent columns—would, in a competently built system, be of marginal value to the adversary." Following a hearing, the trial court denied the cross-motions for summary judgment, finding a factual issue regarding the meaning of "marginal value" as stated in Ptacek's affidavit. At trial, both Coffing and Ptacek testified.

¶ 5 Coffing has worked in cybersecurity for about 22 years. He testified that the CANVAS system stores "sensitive information," consisting of "first name and last name of the primary vehicle owners and the secondary vehicle owner, driver's license numbers, addresses, whether or not there is handicap parking related to that individual, [and] information about who wrote the tickets." Coffing stated that CANVAS is a "competently built system" that was built based on the best practices in the industry.

¶ 6 Coffing also testified that he is responsible for protecting the CANVAS system from a "cyberattack," which occurs when an unauthorized user of the CANVAS system "is attempting to achieve a goal that is not in alignment for business purposes for that system." To prevent a

cyberattack, "a layer of defense" is employed, consisting of "numerous controls that all build upon each other to provide a defense against adversaries." One layer of defense includes "limiting the information that's known about a system, so that the adversary has less to capture in their efforts to perform recognizance about the system." By restricting the information that is available, an attacker would have to be more "noisy," which alerts defenders that an attack is underway. The activity of an "attacker" who has precise information about the target system "may blend in and look like normal activity in the system." Attacks made by people with more knowledge of the system are more precise and effective than attacks made by people who are just conducting recognizance.

¶ 7 Coffing stated that Chapman requested a "file layout" because "table names and column names" are "the information that the database management system uses to create the structure of the database" that stores the data. He explained that using file layouts or source listings, "threat actor[s] would perform recognizance on a target or a system and *** would use this information to more precisely craft their attacks, again to limit the noise that they would make to limit the likelihood of them being detected." He stated that Chapman's request undermines "the layer defense" strategy because, "by addressing the information that's available on the system," more information is available "for a threat actor to perform recognizance again to more precisely tailor their attacks." Coffing acknowledged that Chapman's request did not seek any of the actual data in the field, such as parking ticket, red light camera, or speed camera data.

¶ 8 Coffing next explained "SQL" or "sequel for short," which stands for "structured query language" and "is the language that a database management system uses." A SQL injection is a type of cybersecurity attack. "A threat actor would attempt to use sequel to create a sequel statement, which is an instruction, and it would attempt to inject that into an existing interface that is expecting *** a field that says 'last name' " and then "force the system to do something that it

was not intended to do" but "something that the threat actor wants the system to do." "[I]f you have more information about the database, the table names, the column names, you know where to look for what you are going after" and "you can precisely write your attack, your SQL Injection, when you are entering into that field." Regarding the CANVAS system specifically, a SQL injection is a threat because it "could allow a threat actor to gain access to the data in the system *** to exfiltrate data to find out information about *** our constituents to use for whatever purposes they have." Information in the system could also be modified, such as changing a ticket from not paid to paid, or from $500 to $1. A threat actor "could do something to delete or otherwise modify the data to make it unusable for the system and, therefore, impairing the City's ability to manage citations."

¶ 9 Coffing also explained that "Zero-day" is another type of an attack and refers "to those vulnerabilities that aren't known except to the attacker *** so, therefore, the defenders don't have the opportunity to defend against them." He opined that "by making public more information about a system, it gives a threat actor more at their disposal to attempt to attack."

¶ 10 On cross-examination, Coffing agreed that the FOIA request was "for the listing of tables in the CANVAS database, what the fields are in those tables, and a general description of the type of data in each field." He explained that "if you precisely know what that field name is, then you can more precisely craft your attack and you are not going to make noise you are going to go undetected or less detected than if you don't have that information." Without the information, an attacker would have "to make some guesses" and "those inaccurate guesses are going to generate errors, they are going to generate logs," which "are the things that defenders look for to try to determine whether or not there is a threat actor in the environment." Coffing stated that "[o]ne of the things that helps us defend that system is not making this information available." He did not "want to make it easier for the bad guys and bad gals out there to attack our system and *** put

our constituents' private data at risk." According to Coffing, someone who knows any of the field names within CANVAS with the proper training could attempt to change data in the system or do any of the other attacks that he described.

¶ 11 Ptacek testified that he has worked in the information and software security field for 25 years. As a "vulnerability researcher," he looks for and helps fix identified vulnerabilities in systems. In other words, he "hacks systems for a living." Ptacek has never worked with the CANVAS system, but his general statements "apply to virtually any application built on these types of technologies."

¶ 12 Ptacek interpreted the FOIA request as seeking "the schema of the database that backs the CANVAS application, the tables and the columns of those tables." He defined the "schema" as "a term of art *** use[d] to describe all of the fields and the database that sit behind these applications." Ptacek would not describe the "schema" as the blueprint of the database or a file layout, explaining that the schema "is simply the names of the spread sheets and the column matters *** there is a lot more information that would go into the configuration of the database, and how that database was used than simply the column headers and the names of those tables."

¶ 13 Ptacek stated that the "system that could be attacked solely with the schema would by definition be incompetently built" and potential attackers would not be successful in breaching the security of the system because they had the schema. He explained some of the ways that the security of a system could be jeopardized. For example, an attacker could perform a SQL injection "if [he] knew the specific information about the configuration of the system itself, what operating system it was running on, [and] the version of the orbital database that it was using." As to the CANVAS system, he "could enter a citation number, like a ticket number, and get all of the information about that ticket." If an "application was susceptible or vulnerable to a SQL Injection attack, instead of entering simply the citation number for that ticket, [he] would enter a number

and then in sequel language for every other record in the database." "If the application was vulnerable then it would honor the additional instructions that [he] gave it and would return not just the ticket information but also all other data in the database." The best practices to defend against a SQL injection in the citation field "would be to not allow anything but a number in that field."

¶ 14 Ptacek also explained that the schema would be "one of the first things you would get from an attack, the product of an attack and not a predicate of an attack." Ptacek stated that in his "professional experience doing this for 25 years I've never asked for a database schema before I start an attack" and "can't imagine a situation where having the schema would determine whether or not I would bother or take the time to attack the system."

¶ 15 Ptacek testified that a vulnerability in the database must exist to break into it. A publicly available schema "is not considered a vulnerability in the system." Knowledge of the schema in conjunction with publicly available information "would not make it easier to attack the system." In fact, federal database schemas are publicly available on data.gov. He explained that, "[i]f the schema for an application was unexpectedly disclosed, it would not be normal partial best practices to purport a vulnerability or an incident in that system simply as a result of the schema being disclosed."

¶ 16 As to the phrase "marginal value to the adversary" used in his affidavit, Ptacek elaborated that, "based on [his] 25 years of experience doing precisely this kind of work, [he] could not think of a thing [he] would do with that information that would allow [him] to in any way more effectively attack or compromise the system or do so more precisely or quietly." But he explained that having the schema has some value in helping plan an attack because, for example, it "would help isolate the systems that would contain Social Security information so I wouldn't have to take the time to attack lots of other applications."

¶ 17 Regarding "noise," Ptacek stated that "it is the source code that would allow you to not make noise as an attacker," not the schema. With the source code, an attacker "would be substantially less noisy, but not with the schema, it wouldn't help." "The source code is valuable and the schema I would say as an attacker is not valuable." Ptacek testified that he "cannot think of a way which publicly disclosing the schema would jeopardize the security of that system."

¶ 18 On January 9, 2020, the trial court entered judgment for Chapman and ordered the Department "to produce the requested records by Feb. 10, 2020." At the Department's request, "the production of all requested records [was] stayed pending the outcome of appeal."

¶ 19 II. ANALYSIS

¶ 20 In construing the FOIA and the applicability of any exemption, we are guided by familiar statutory interpretation principles. "The primary objective in statutory construction is to ascertain and give effect to the intent of the legislature." *Haage v. Zavala*, 2021 IL 125918, ¶ 44. "The most reliable indicator of legislative intent is the language of the statute, given its plain and ordinary meaning." *In re Appointment of Special Prosecutor*, 2019 IL 122949, ¶ 23. "Each word, clause, and sentence of a statute must be given a reasonable meaning, if possible, and should not be rendered superfluous." *Haage*, 2021 IL 125918, ¶ 44. A "court may consider the reason for the law, the problems sought to be remedied, the purposes to be achieved [citations], and the consequences of construing the statute one way or another [citations]." *Id.*

¶ 21 In section 1 of the FOIA, the Illinois legislature expressed its intent in enacting the statute, stating that it is "the public policy of the State of Illinois that access by all persons to public records promotes the transparency and accountability of public bodies at all levels of government" and it "is a fundamental obligation of government to operate openly and provide public records as expediently and efficiently as possible in compliance with this Act." 5 ILCS 140/1 (West 2018). To achieve the legislature's intent, the FOIA "is to be liberally construed to achieve the goal of

providing the public with easy access to government information," and "exceptions to disclosure are to be construed narrowly so as not to defeat the intended statutory purpose." *In re Appointment of Special Prosecutor*, 2019 IL 122949, ¶ 25. "Thus, when a public body receives a proper request for information, it must comply with that request unless one of FOIA's narrow statutory exemptions applies." *Id.*

¶ 22 The Department claims that "section 7(1)(*o*) expressly exempts the records Chapman requested." Section 7(1)(*o*) exempts from disclosure:

> "(*o*) Administrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section." 5 ILCS 140/7(1)(*o*) (West 2018).

"Any public body that asserts that a record is exempt from disclosure has the burden of proving by clear and convincing evidence that it is exempt." *Id.* § 1.2. Whether an exemption applies under the FOIA is a question of statutory construction, which we review *de novo*. *Chicago Public Media v. Cook County Office of the President*, 2021 IL App (1st) 200888, ¶ 22; *Turner v. Joliet Police Department*, 2019 IL App (3d) 170819, ¶ 20.

¶ 23 The Department interprets section 7(1)(*o*) as providing a *per se* exemption from disclosure for "file layouts," which it claims was the information that Chapman requested. The Department argues that the phrase "would jeopardize the security of the system or its data or the security of materials exempt under this Section" modifies *only* the catchall phrase "any other information" and not "file layouts" based on an application of the last antecedent canon of statutory

interpretation.

¶ 24 "The last antecedent doctrine, a long-recognized grammatical canon of statutory construction, provides that relative or qualifying words, phrases, or clauses are applied to the words or phrases immediately preceding them and are not construed as extending to or including other words, phrases, or clauses more remote, unless the intent of the legislature, as disclosed by the context and reading of the entire statute, requires such an extension or inclusion." *In re E.B.*, 231 Ill. 2d 459, 467 (2008). Canons of statutory construction only apply if the language of the statute is ambiguous. See *Palm v. Holocker*, 2018 IL 123152, ¶ 21; *Salier v. Delta Real Estate Investments, LLC*, 2020 IL App (1st) 181512, ¶ 36 ("Where the text of a statute is clear and unambiguous, *** we need not resort to canons of statutory construction ***."). But, here, the Department contends the opposite. The Department argues that "the *plain* language of section 7(1)(*o*) is a *clear* indication of the General Assembly's intent to expressly exempt file layouts from FOIA's disclosure requirements without proof that disclosing such information 'would jeopardize the security of the system.' " (Emphasis added.) Thus, the Department, as confirmed during oral arguments, does not contend that the statute is ambiguous. For that reason, we need not resort to the last antecedent canon of statutory construction to interpret section 7(1)(*o*) as urged by the Department.

¶ 25 In *Lieber v. Board of Trustees of Southern Illinois University*, 176 Ill. 2d 401, 409 (1997), a case relied heavily upon by the Department in its brief and during oral arguments, the Illinois Supreme Court determined whether information requested from a university was exempt from disclosure based on privacy expectations. Lieber, an apartment building owner near the university's campus, requested from the university disclosure of the names and addresses of incoming freshman who had contacted the school inquiring about housing. *Id.* at 403-04. The university had previously supplied him with the information, but this practice was later changed.

Id. at 405. Lieber filed a FOIA request for the information, which the university denied. *Id.* at 405-06. Lieber then sought judicial review of the denial. *Id.* at 406. In response, the university asserted that the requested information was exempt from disclosure under section 7(1)(b) of FOIA. *Id.*

¶ 26 Section 7(1)(b) of the version of FOIA in effect at the time of *Lieber* exempted

> "(b) Information that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information. *** Information exempted under this subsection (b) shall include but is not limited to:
>
> (i) files and personal information maintained with respect to *** students[.]" 5 ILCS 140/7(1)(b) (West 1994).

In interpreting that section, the appellate court applied a balancing test, considering "an individualized assessment of whether disclosure of the information would invade anyone's personal privacy." *Lieber*, 176 Ill. 2d at 409. Based on the statute's "clear and unambiguous language," the supreme court determined that a *per se* approach was better suited than the case-by-case balancing approach. *Id.* The court explained that the "*per se* rule applies to the specific exemptions set forth in the subsections of section 7(1)(b) of the Act (5 ILCS 140/7(1)(b) (West 1994)), which pertains to '[i]nformation that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy,' just as it does to the other exemptions in section 7." *Id.* at 408. Ultimately, the court concluded that the names and addresses of accepted individuals, but who were not "students" because they had not yet enrolled in the university, were not exempt from public disclosure. *Id.* at 411, 414.

¶ 27 After oral argument was held in this case, our supreme court decided *Mancini Law Group, P.C. v. Schaumburg Police Department*, 2021 IL 126675, which we allowed the Department to cite as additional authority. We disagree with the Department's argument that *Mancini* "adopted

as part of its holding *Lieber*'s construction of the section 7 exemptions to require a '*per se*' approach." Because the public body in *Mancini Law Group*, as here, relied on *Lieber*, the court provided "a detailed discussion of *Lieber*," reciting the case's facts and holding. *Id.* ¶¶ 23-34. In any event, *Mancini Law Group* is not dispositive.

¶ 28 In *Mancini Law Group*, the plaintiff sent a commercial FOIA request to the police department, seeking disclosure of traffic accident reports for all motor vehicle accidents that occurred within the village for a specified period of time. *Id.* ¶ 3. The police department provided redacted accident reports, asserting that the redacted information, including home addresses, was "private information" exempt from disclosure under section 7(1)(b) of FOIA. *Id.* Mancini Law Group filed suit, alleging that the police department "had willfully and intentionally violated FOIA by refusing to produce unredacted accident reports." *Id.* ¶ 4. The supreme court recognized that, since *Lieber*, the legislature amended the statute by adding "the exemption for private information," which the court explained, "indicates that the legislature decided to break with *Lieber* on this basis" (holding that names and addresses were subject to disclosure) "and afford protection to a broader category of information that was not previously deemed to be exempt." *Id.* ¶ 36. The court, though, considered *Lieber* not for its exemption analysis but on a separate waiver issue. *Id.*

¶ 29 In *Lieber*, the case analyzed a different exemption under a prior version of the statute. In addition, the plain and ordinary language of the exemption in *Lieber* is markedly different from section 7(1)(*o*). Significantly, the relevant statutory language in *Lieber* stated that the "*[i]nformation exempted* under this subsection (b) *shall include*" and then enumerated five different categories of information. (Emphases added.) 5 ILCS 140/7(1)(b) (West 1994); see *Gibson v. Illinois State Board of Education*, 289 Ill. App. 3d 12, 18 (1997) ("The exemptions of section 7 are clearly written and explicitly state that information contained in any of the subsections

of section 7(1)(b) is exempt."). Because the legislature did not include the directive "shall include" language in section 7(1)(*o*), the Department's reliance on the *per se* approach enunciated in *Lieber* as to section 7(1)(b) is misplaced.

¶ 30 Likewise, *Mancini Law Group* does not compel a finding that the requested "schema" was a protected record falling within an exemption. *Mancini Law Group* recognized that subsequent amendments to the FOIA since *Lieber* demonstrated the legislature's intent to provide broader protection from disclosure of "private information," noting that "the legislature later clarified that home addresses are exempt information." *Mancini Law Group*, 2021 IL 126675, ¶¶ 36-37. As this court has recognized, "*Lieber* involved statutory language that is no longer in effect; it was decided in an era when privacy expectations were different." *Timpone v. Illinois Student Assistance Comm'n*, 2019 IL App (1st) 181115, ¶ 35. Here, no such privacy concerns are implicated because, as the parties' experts acknowledged, Chapman did not request any of the actual data in the fields.

¶ 31 In this case, the relevant exemption pertains to "administrative or technical information associated with automated data processing operations." We are mindful that section 7(1) explicitly sets forth categories of public records that are exempt from disclosure. *Lieber*, 176 Ill. 2d at 409. In other words, if the requested information falls within the enumerated categories provided in section 7(1)(a) through (jj), then it "shall be exempt from inspection and copying." 5 ILCS 140/7(1) (West 2018). But where, as in section 7(1)(*o*), additional requirements are expressly provided, those requirements must be satisfied before the requested information may be classified as "exempt from inspection and copying." See *Mancini Law Group*, 2021 IL 126675, ¶ 16 (reiterating that public records are " 'presumed to be open and accessible' " (quoting *Illinois Education Ass'n v. Illinois State Board of Education*, 204 Ill. 2d 456, 462 (2003))). Therefore, the phrase "if disclosed, would jeopardize the security of the system or its data or the security of

materials exempt under this Section" imposes an additional requirement ("would jeopardize") that must be demonstrated before a public body may exempt information from disclosure.

¶ 32 We find that, under the plain and ordinary language of section 7(1)(*o*), the reasonable meaning of "if disclosed, would jeopardize" must apply to every item listed, not only to the catchall phrase of "and any other information" as urged by the Department. See *DG Enterprises, LLC-Will Tax, LLC v. Cornelius*, 2015 IL 118975, ¶ 31 ("generally the use of a conjunctive such as 'and' indicates that the legislature intended that *all* of the listed requirements be met" (emphasis in original)); *People v. Lattimore*, 2011 IL App (1st) 093238, ¶ 105 (a list of statutes following the conjunction "or" that was preceded with a comma modified only the type of adjudication following the "or" rather than all of the adjudications). Under the Department's proposed *per se* interpretation, the items separately listed in section 7(1)(*o*), which include user guides and employee manuals, would never be disclosed to the public. A blanket prohibition against disclosure of the items separately listed in section 7(1)(*o*) runs contrary to the principle that exceptions are to be read narrowly and would frustrate the legislature's goal in enacting the FOIA of providing "the public with easy access to government information." *In re Appointment of Special Prosecutor*, 2019 IL 122949, ¶ 25; see *Lucy Parsons Labs v. City of Chicago Mayor's Office*, 2021 IL App (1st) 192073, ¶ 18 (all doubts should be resolved "in favor of disclosure in light of the public policy underlying" the FOIA); see also 5 ILCS 140/2(c) (West 2018) (public records subject to disclosure include "electronic data processing records"); *Hites v. Waubonsee Community College*, 2016 IL App (2d) 150836, ¶ 68 ("Illinois courts permit disclosure of electronic records under FOIA").

¶ 33 Because we find that the phrase "if disclosed, would jeopardize" applies to every item enumerated in section 7(1)(*o*), we need not determine whether the information Chapman requested was a "file layout" or falls within the catchall of "any other information," as both are subject to

the "would jeopardize" requirement. See *Hites*, 2016 IL App (2d) 150836, ¶ 71 (adopting the following analogy of a database to a file cabinet: "[T]he database is akin to a file cabinet, and the data that populates the database is like the files. FOIA permits a proper request for a single file, some of the files, or all of the files.").

¶ 34 The Department next argues that it was only required to establish by clear and convincing evidence the *possibility* that disclosure of the requested information could cause harm.[2] We disagree.

¶ 35 This court's decision in *Chicago Sun-Times v. Chicago Transit Authority*, 2021 IL App (1st) 192028, ¶ 39, is instructive regarding the meaning of "could" and "would" in the context of an exemption to the disclosure of information under the FOIA. In that case, the Sun-Times sought disclosure under the FOIA of surveillance video of the Chicago Transit Authority's (CTA) subway platform that showed one customer pushing another customer off the platform. *Id.* ¶ 1. The CTA asserted that the "security measures" exemption of section 7(1)(v) of the FOIA applied, which exempts " 'security measures *** that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but only to the extent that disclosure *could reasonably be expected to jeopardize* the effectiveness of the measures.' " (Emphasis added.) *Id.* ¶ 7 (quoting 5 ILCS 140/7(1)(v) (West 2016)). The CTA argued that public disclosure of the requested information "could jeopardize the

[2]Chapman argues that the Department forfeited this claim because it failed to raise this theory in response to his motion for summary judgment and only argued it on "the eve of trial." Although the trial court noted that "this defense theory, which is being advanced today for the first time, which is that a 'file layout' or 'source listing' is exempt without regard to *** whether disclosure would jeopardize security of the system," the trial court, nonetheless, ruled "as a matter of law that that theory is at odds with the plain language of the statute." Therefore, the issue has not been forfeited because it was ruled upon by the trial court. See *Village of Palatine v. Palatine Associates, LLC*, 2012 IL App (1st) 102707, ¶ 64 (issues raised for the first time on appeal are waived).

effectiveness of its security cameras." *Id.* Interpreting the language of section 7(1)(v), this court concluded that the statute did "not require an agency to prove, by clear and convincing evidence, that releasing a particular record *would* in fact diminish the effectiveness of its security measures"; rather, "the agency must meet the lesser burden to show that it could reasonably be expected that the release of the record *could* jeopardize the effectiveness of the agency's security measures." (Emphases added.) *Id.* ¶ 44. This court explained that the "General Assembly knew the difference between the use of the term *could* instead of *would*; it had used the word 'would' in other FOIA exemptions." (Emphases in original.) *Id.* ¶ 43.

¶ 36 In this case, unlike in *Chicago Sun-Times*, the legislature used the word "*would*" and not "*could*." Based on *Chicago Sun-Times*, the Department bears the burden of satisfying the higher standard that disclosure of the schema "would" jeopardize the security of the CANVAS system. In other words, the Department must demonstrate by clear and convincing evidence more than the *possibility* of a threat to the security of the CANVAS system.

¶ 37 Under the "clear and convincing evidence" standard, the proof offered by the plaintiff "must 'leave[ ] no reasonable doubt in the mind of the trier of fact as to the truth of the proposition in question.' " *Metropolitan Capital Bank & Trust v. Feiner*, 2020 IL App (1st) 190895, ¶ 39 (quoting *Parsons v. Winter*, 142 Ill. App. 3d 354, 359 (1986)). We will not reverse the trial court's finding of "clear and convincing evidence" unless it is against the manifest weight of the evidence. See *Indeck Energy Services, Inc. v. DePodesta*, 2021 IL 125733, ¶ 56 (trial court's factual findings will not be reversed unless the findings are against the manifest weight of the evidence); *In re Commitment of Tunget*, 2018 IL App (1st) 162555, ¶ 35 (a "clear and convincing evidence" finding warrants reversal if that determination was against the manifest weight of the evidence). A trial court's finding "is against the manifest weight of the evidence only if an opposite conclusion is clearly evident." *DePodesta*, 2021 IL 125733, ¶ 56.

¶ 38 The trial court's finding that the Department failed to demonstrate by clear and convincing evidence that the exemption from disclosure provided in section 7(1)(*o*) applied to Chapman's FOIA request was not against the manifest weight of the evidence. Ptacek testified that the attack of a system would not be facilitated by knowing the schema, the public disclosure of the schema was "not considered a vulnerability in the system," and an attacker knowing the schema would not be substantially less "noisy." Ptacek explained that knowing the source code is valuable to an attacker, not the schema. He also explained that an "incompetently built" system "could be attacked solely with the schema," but Coffing affirmed that the CANVAS system *was* competently built.

¶ 39 With respect to Coffing's testimony, the trial court found that he "summarily testified that if a threat actor knows the name of a field he can more precisely plan and execute an attack without making noise and thereby avoid detection." The trial court also found that "he really didn't go into it more beyond that, as far as explaining how that would work, at least not in a way that the Court found persuasive." Instead, the trial court found "persuasive Mr. Ptacek's argument that the schema is the product of the attack not the predicate of the attack."

¶ 40 Under the FOIA, the Department, not Chapman, had "the burden of proving by clear and convincing evidence" that section 7(1)(*o*) applied to exempt the requested information. 5 ILCS 140/1.2 (West 2018). Although Coffing described the approaches and methods that could hypothetically be employed to plan and initiate an attack of the CANVAS system's security, the trial court's finding that he failed to testify persuasively that disclosure of the schema "*would jeopardize* the security of the system or its data" was not "unreasonable, arbitrary, or not based on the evidence presented" (*Best v. Best*, 223 Ill. 2d 342, 350 (2006)). Construing the exemption narrowly, as we must, and given the high burden imposed on the Department to prove that section 7(1)(*o*) applied by clear and convincing evidence, we agree with the trial court that the information

requested by Chapman was subject to disclosure under the facts of this case. See *In re Appointment of Special Prosecutor*, 2019 IL 122949, ¶ 25. Therefore, the Department must comply with Chapman's FOIA request and disclose "an index of the tables and columns within each table of CANVAS." Disclosure of that information is consistent with the purpose of the FOIA and the presumption that public records are open and accessible to any person. *Id.* Because we find in favor of Chapman, we need not consider his claim that the requested records were also accessible under section 5 of the FOIA (5 ILCS 140/5 (West 2018)), titled "List of records available from public body."

¶ 41 III. CONCLUSION

¶ 42 The Department must provide the information Chapman requested because the information was not exempt from disclosure under section 7(1)(*o*) of the FOIA.

¶ 43 Affirmed.

No. 1-20-0547

Cite as:	*Chapman v. Chicago Department of Finance*, 2022 IL App (1st) 200547
Decision Under Review:	Appeal from the Circuit Court of Cook County, No. 18-CH-14043; the Hon. Sanjay T. Tailor, Judge, presiding.
Attorneys for Appellant:	Celia Meza, Acting Corporation Counsel, of Chicago (Benna Ruth Solomon, Myriam Zreczny Kasper, and Elizabeth Mary Tisher, Assistant Corporation Counsel, of counsel), for appellant.
Attorneys for Appellee:	Joshua Burday, Matthew Topic, and Merrick Wayne, of Loevy & Loevy, of Chicago, for appellee.

I find as an matter of law that that theory is at odds with the plain language of the statute.

I read the statute to mean that qualification language, which is:

"If disclosed would jeopardize security of the system or its data or the security of the material exempt under this section."

Qualifies everything that proceeds it, including "file layouts" and "source listings".

So whether it is a file layout or a source listing does not answer whether its exempt under the statute.

I think I make that finding as a matter of law.

So the only issue then will be, whether disclosure of the information, whatever it is, would jeopardize the security of the system.

MS. NELSON: Your Honor, I would for

more vulnerable to attack, even if somebody considers themselves a civic hacker.

Thank you.

THE COURT: Thank you.

Okay. The City has established by clear and convincing evidence that disclosure of the schema for its CANVAS System, which is an electronic information management system used in administration of the City's citations for violations of the ordinances and law would jeopardize the security of that CANVAS System.

I find that the City has not met its burden of proof on this question under Section 7(1)(o) of FOIA.

I found Mr. Ptacek's -- I'm not sure I'm pronouncing it right -- testimony persuasive on this question.

Mr. Coffing in summary testified that if a threat actor knows the name of a field he can more precisely plan and execute an attack without making noise and thereby avoid

detection.

But he really didn't go into it more beyond that, as far as explaining how that would work, at least not in a way that the Court found persuasive.

Mr. Ptacek testified that knowledge of the schema would not in any way provide a threat actor advantage in attacking a system like CANVAS.

He did testify about SQL Injection attacks and testified that that may occur, for example, when an application allows user input, such as in this case.

Mr. Coffing offered three examples of user input, including for fleet owners, including those seeking payment plan, and there was one other instance which escapes me at the moment.

But that instance, for example, one might enter let's say a citation number, a ticket, and the threat actor could input the number, that number as well as a SQL

instruction, the app could honor the additional SQL instruction that the attacker put in, but only if it was vulnerable to attack in the first instance.

Having the schema, based on the record before me, I find does not make it easier to do a SQL attack.

The schema can be used in conjunction with other information to perform an attack or at least make it easier to perform an attack. It is a source code which is what is necessary to attack the system.

I also find persuasive Mr. Ptacek's argument that the schema is the product of the attack not the predicate of the attack.

That may help guide the hypothetical Latvian threat actor on which system he might want to pursue is really of no moment, because the citation management system such as CANVAS by definition, necessarily has the kind of information that would attract a

threat actor.

But knowledge of the schema in no way makes the system more vulnerable nor the possibility of the zero-day vulnerability in any way is increased by disclosure of the schema.

Nor am I persuaded that the information available on the publically available RFP could in combination with the schema assist the threat actor.

So to conclude, the City has failed to meet its burden on its defense under Section 7(1)(o) of FOIA.

Judgment will be entered in favor of the Plaintiff and against the defendant.

Anything else?

MR. TOPIC: Your Honor, if we could get a date specified by which it would occur, and maybe then a status after that and attorney fees.

THE COURT: 30 days.

MR. TOPIC: Okay.

Order (Rev. 02/24/05) CCG N002

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS

Chapman
v.
Chicago Dept of Finance

No. 18 CH 14043

ORDER

This case before the Court on trial on Defendant's affirmative defense under FOIA Section 7(1)(o) and Plaintiff's FOIA claim against Defendant, judgment is entered for Plaintiff and against Defendant. Defendant is ordered to produce the requested records by Feb. 10, 2020. Case set for status on Feb 4, 2020, at 9:30 AM. for the reasons stated on the record.

Attorney No.: 41295
Name: Matt Topic
Atty. for: Plaintiff
Address: 311 N Aberdeen
City/State/Zip: 60607
Telephone: 312-243-5900

ENTERED:

Dated: _____

ENTERED
Judge Sanjay Tailor-1870
JAN 09 2020
DOROTHY BROWN
CLERK OF THE CIRCUIT COURT
OF COOK COUNTY, IL
DEPUTY CLERK

Judge

Judge's No.

DOROTHY BROWN, CLERK OF THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

MATT CHAPMAN,	)	
	)	
Plaintiff,	)	**No: 18 CH 14043**
v.	)	
	)	**HONORABLE JUDGE TAILOR**
CHICAGO DEPARTMENT OF FINANCE,	)	
	)	
	)	
Defendant.	)	

Q203

ORDER

This matter coming before the Court and the Court being fully advised in the premises, it is hereby ordered:

1) For the reasons set forth in the transcript of proceedings of January 9, 2020, the Court granted judgment for the Plaintiff.

2) The production of all requested records is stayed pending the outcome of appeal.

3) The parties have resolved the issue of attorney's costs and fees, and all other issues having been resolved between the parties, this order and the order of January 9, 2020 are final and appealable.

ENTERED:

DATE:

ENTERED
Judge Sanjay Tailor-1870
MAR 12 2020
DOROTHY BROWN
CLERK OF THE CIRCUIT COURT
OF COOK COUNTY, IL
DEPUTY CLERK

MARK A. FLESSNER, Corporation Counsel
MELANIE K. NELSON, Chief Assistant Corporation Counsel
Legal Information & Prosecutions Division
30 N. LaSalle Street, Suite 1720
Chicago, Illinois 60602
(312)742-0116
Attorney No. 90909

APPEAL TO THE APPELLATE COURT OF ILLINOIS
FIRST JUDICIAL DISTRICT
FROM THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

MATT CHAPMAN,	) Appeal from the Circuit Court
	) of Cook County, Illinois,
Plaintiff-Appellee,	) County Department,
	) Chancery Division
v.	)
	) No. 18 CH 14043
CHICAGO DEPARTMENT OF FINANCE,	)
	) The Honorable
Defendant-Appellant.	) **Sanjay T. Tailor**,
	) Judge Presiding.

NOTICE OF APPEAL

Defendant, CHICAGO DEPARTMENT OF FINANCE, by its attorney, Mark A. Flessner, Corporation Counsel of the City of Chicago, hereby appeals to the Appellate Court of Illinois, First Judicial District, from the order of the Circuit Court of Cook County, Illinois, entered January 9, 2020, entering judgment in favor of Plaintiff and against the Defendant for the reasons stated on the record and ordering Defendant to produce the requested records, and the order of March 12, 2020, which made the order of January 9, 2020 final and appealable.

By this appeal, Defendant will ask the appellate court to reverse the circuit court's judgment and orders, and grant such other relief as Defendant may be entitled to on this appeal.

Respectfully submitted,

MARK A. FLESSNER
Corporation Counsel
of the City of Chicago

By: s/ MYRIAM ZRECZNY KASPER

MYRIAM ZRECZNY KASPER
Chief Assistant Corporation Counsel
30 North LaSalle Street - Suite 800
Chicago, IL 60602
(312) 744-3564
myriam.kasper@cityofchicago.org
appeals@cityofchicago.org
Attorney No. 90909

FILED
3/19/2020 10:56 AM
DOROTHY BROWN
CIRCUIT CLERK
COOK COUNTY, IL
2018CH14043

APPEAL TO THE APPELLATE COURT OF ILLINOIS
FIRST JUDICIAL DISTRICT
FROM THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

MATT CHAPMAN,	) Appeal from the Circuit Court
	) of Cook County, Illinois,
Plaintiff-Appellee,	) County Department,
	) Chancery Division
v.	)
	) No. 18 CH 14043
CHICAGO DEPARTMENT OF FINANCE,	)
	) The Honorable
Defendant-Appellant.	) **Sanjay T. Tailor**,
	) Judge Presiding.

NOTICE OF FILING NOTICE OF APPEAL

TO: Matt Topic
Merrick Wayne
LOEVY & LOEVY
311 North Aberdeen Street, Suite 300
Chicago, Illinois 60607
foia@loevy.com

PLEASE TAKE NOTICE that on March 19, 2020, I electronically filed with the Clerk of the Circuit Court of Illinois, Civil Appeals Division, Richard J. Daley Center, Chicago, Illinois, a **Notice of Appeal**, a copy of which is attached hereto and herewith served upon you.

MARK A. FLESSNER
Corporation Counsel
of the City of Chicago

By: s/ MYRIAM ZRECZNY KASPER
MYRIAM ZRECZNY KASPER
Chief Assistant Corporation Counsel
30 North LaSalle Street - Suite 800
Chicago, IL 60602
(312) 744-3564
myriam.kasper@cityofchicago.org
appeals@cityofchicago.org
Attorney No. 90909

CERTIFICATE OF SERVICE/CERTIFICATE OF FILING

The undersigned certifies under penalty of law as provided in 735 ILCS 5/1-109 that the statements in this instrument are true and correct, and that the attached **Notice of Filing** and **Notice of Appeal** were filed and served electronically via *File & Serve Illinois* at the e-mail address(es) on the accompanying notice on March 19, 2020.

s/ MYRIAM ZRECZNY KASPER
MYRIAM ZRECZNY KASPER

TABLE OF CONTENTS TO THE RECORD ON APPEAL

Common Law Record

Report Of Proceedings

WITNESSES

Bruce Coffing

WITNESSES

Thomas H. Ptacek