Illinois Official Reports

Appellate Court

***Chapman v. Chicago Department of Finance*, 2022 IL App (1st) 200547**

Appellate Court Caption	MATT CHAPMAN, Plaintiff-Appellee, v. THE CHICAGO DEPARTMENT OF FINANCE, Defendant-Appellant.
District & No.	First District, First Division No. 1-20-0547
Filed	February 14, 2022
Decision Under Review	Appeal from the Circuit Court of Cook County, No. 18-CH-14043; the Hon. Sanjay T. Tailor, Judge, presiding.
Judgment	Affirmed.
Counsel on Appeal	Celia Meza, Acting Corporation Counsel, of Chicago (Benna Ruth Solomon, Myriam Zreczny Kasper, and Elizabeth Mary Tisher, Assistant Corporation Counsel, of counsel), for appellant. Joshua Burday, Matthew Topic, and Merrick Wayne, of Loevy & Loevy, of Chicago, for appellee.
Panel	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:
>
> 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.

¶ 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

[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."

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.' " (Emphases 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 Law Group* "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

[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).

> 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 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.