Illinois Official Reports

Supreme Court

***Chapman v. Chicago Department of Finance*, 2023 IL 128300**

Caption in Supreme Court:	MATT CHAPMAN, Appellee, v. THE CHICAGO DEPARTMENT OF FINANCE, Appellant.
Docket No.	128300
Filed	May 18, 2023
Decision Under Review	Appeal from the Appellate Court for the First District; heard in that court on appeal from the Circuit Court of Cook County, the Hon. Sanjay T. Tailor, Judge, presiding.
Judgment	Judgments reversed. Cause remanded with directions.
Counsel on Appeal	Celia Meza, Corporation Counsel, of Chicago (Myriam Zreczny Kasper, Suzanne Loose, Ellen W. McLaughlin, and Elizabeth M. Tisher, Assistant Corporation Counsel, of counsel), for appellant. Matthew Topic, Josh Loevy, Merrick Wayne, and Shelley Geiszler, of Loevy & Loevy, of Chicago, for appellee.

Justices

JUSTICE HOLDER WHITE delivered the judgment of the court, with opinion.

Chief Justice Theis and Justices Neville, Overstreet, Cunningham, Rochford, and O'Brien concurred in the judgment and opinion.

OPINION

¶ 1 Plaintiff, Matt Chapman, filed a request pursuant to the Freedom of Information Act (FOIA) (5 ILCS 140/1 *et seq.* (West 2018)), seeking certain information utilized by defendant, the Chicago Department of Finance. Defendant denied the request, identifying the requested information as exempt from disclosure under section 7(1)(*o*) of FOIA. *Id.* § 7(1)(*o*).

¶ 2 Plaintiff filed a complaint, alleging defendant violated FOIA by failing to disclose the records and asking the Cook County circuit court to order their production. The court agreed with plaintiff and ordered defendant to produce the records. The First District affirmed. 2022 IL App (1st) 200547, ¶ 1.

¶ 3 Now on appeal, defendant argues (1) section 7(1)(*o*) of FOIA expressly exempts the requested records from disclosure and (2) it demonstrated clear and convincing evidence that disclosure would jeopardize the security of its system. We reverse and remand with directions.

¶ 4 BACKGROUND

¶ 5 In August 2018, plaintiff submitted a FOIA request to defendant for certain records pertaining to the Citation Administration and Adjudication System (CANVAS), developed by IBM for the City of Chicago in 2002 for the enforcement of parking, red-light, and speed-camera tickets. After a ticket has been issued, it is loaded into the CANVAS system, which defendant uses to issue notices and for payment purposes.

¶ 6 Specifically, plaintiff sought an "index of the tables and columns within each table of CANVAS" and asked for the "column data type as well." Further, plaintiff's request stated the following:

> "Per the CANVAS specification, 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' "

Plaintiff indicated the requested documents would be made available to the general public and that the request was not being made for commercial purposes.

¶ 7 Defendant denied the request, stating the records were exempt from disclosure pursuant to section 7(1)(*o*) of FOIA (5 ILCS 140/7(1)(*o*) (West 2018)). Section 7(1)(*o*) exempts the following:

> "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." *Id.*

Defendant stated the request for a copy of tables or columns within each table of CANVAS could, if disseminated, jeopardize the security of the systems of the City of Chicago.

¶ 8 In November 2018, plaintiff filed suit, alleging his request concerned nonexempt public records and defendant had willfully and intentionally violated FOIA by failing to produce the requested records. Thereafter, plaintiff filed a motion for partial summary judgment, and defendant filed a cross-motion for summary judgment.

¶ 9 In its cross-motion, defendant argued plaintiff's broad and open-ended request would "provide a detailed roadmap of the entire CANVAS system to the public" and, if released, "would not only provide information about how the CANVAS system was designed but would also facilitate cyber-attacks." The circuit court denied both motions.

¶ 10 In January 2020, the circuit court held a trial on plaintiff's complaint. Before the trial began, defendant argued the information plaintiff requested constituted a "file layout" or "source listing," both of which are expressly exempt from disclosure under section 7(1)(*o*) without regard to whether disclosure would jeopardize the security of the system. The court disagreed "as a matter of law," stating the phrase "if disclosed[,] would jeopardize [the] security of the system or its data or the security of the material[s] exempt under this [S]ection," qualifies every term that precedes it, including "file layouts" and "source listings." Thus, the only issue for trial was whether disclosure of the information would jeopardize the security of the system.

¶ 11 On defendant's behalf, Bruce Coffing testified he was the chief information security officer for the City of Chicago. He indicated his familiarity with the CANVAS system, which contains sensitive information pertinent to constituents who have received tickets relating to parking, speed-light cameras, red-light cameras, booting, and towing. Coffing stated that information includes, among other things, first and last names of the primary and secondary vehicle owners, driver's license numbers, addresses, handicap-parking status, the ticket issuer, and payment method.

¶ 12 Coffing testified he is responsible for protecting the CANVAS system from cyberattacks. One of the ways to defend against such attacks includes limiting the information known about a system, so that hackers have to be "more noisy" when attempting an attack and thereby alerting security defenses that an attack is underway. If an attack is conducted by someone with knowledge of the system, "their activity may blend in and look like normal activity in the system." Coffing stated releasing the requested information would undermine the layer defense strategy by "providing more information for a threat actor to perform [reconnaissance] again to more precisely tailor their attack."

¶ 13 Coffing testified that plaintiff's request concerned file layouts and source listings. He stated file layouts include "table names and column names," which is "the information that the database management system uses to create the structure of the database." "Source listings" include instructions to "the database management system on how to do something to setup the database, the tables, the columns within each of those tables and the data types that those columns represent."

¶ 14 Coffing stated that, if a threat actor knew the file layouts or source listings, he or she could use that knowledge to "perform [reconnaissance] on a target or a system and in this case 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."

¶ 15 Coffing also testified releasing the information requested by plaintiff could facilitate a type of attack known as a structured query language (SQL) injection, which would force the system to do something it is not designed to do. In such an instance, the injection acts as "a window into the system and then it uses this vulnerability to attempt to make the system do something that the threat actor wants the system to do." Coffing stated an SQL injection could be used against the CANVAS system to gain access and modify information, such as payment on a ticket, or delete data to make the system unusable.

¶ 16 On cross-examination, Coffing acknowledged plaintiff's FOIA request did not seek actual data, such as a person's driver's license number, but instead sought a listing of the tables in the CANVAS database and the fields and columns within those tables. However, Coffing explained that disclosure of the requested records would "disclose how the database management system constructs the database that contains the data used, stored and processed by the CANVAS system."

¶ 17 When asked by the circuit court to assume the general public knows what information is being collected, *e.g.*, first and last names, citation number, vehicle information, and date and type of citations, Coffing testified that knowing the specific field name could allow someone to precisely craft an attack to make less noise and go undetected. For example, Coffing stated a field name could be "L underscore name" or "last underscore name," but not knowing which one could lead to inaccurate guesses and thereby alert the system that a threat actor is in the environment.

¶ 18 In plaintiff's case, Thomas Ptacek testified he worked in the field of information and software security. Describing himself as a "vulnerability researcher," he acknowledged he hacks systems for a living. Ptacek understood plaintiff's FOIA request as seeking "the schema of the database that backs the CANVAS application, the tables and the columns of those tables."

¶ 19 Ptacek described "schema" as a term of art referring to "all of the fields and the databases that sit behind these applications." According to Ptacek, "schema information would be of marginal value to an attacker." Moreover, disclosing the requested records would not produce the source code for the CANVAS system, which would provide a collection of instructions that tells the CANVAS application how to function.

¶ 20 Ptacek could not think of a way in which publicly "disclosing the schema would jeopardize the security" of a system or make it easier to carry out an SQL injection attack. Instead, he stated one of the first things he would get from an SQL injection attack would be the schema itself. Ptacek did testify that, if a hacker breached a database, knowledge of the schema would be "of value in that it would allow [the hacker] to select" the application to target. However, he stated that, if the schema is publicly available, it is not considered a vulnerability to the system. He stated "schemas are not file layouts" or source listings.

¶ 21 On cross-examination, Ptacek testified he has never worked with the CANVAS system and he did not know the source code, architecture, or security configurations of the system. He stated that having the schema has some value to the hacker in helping to plan for an attack. For

example, if Ptacek wanted to target Social Security numbers, having the schema would help "isolate the systems" that contained Social Security information so he would not "have to take the time to attack lots of other applications." But he stated knowing the schema would not prevent noise during a hacking attempt, as opposed to knowing the source code, which would help him be "substantially less noisy."

¶ 22 Following closing arguments, the circuit court found defendant had not met its burden of proof under section 7(1)(*o*) of FOIA. The court found persuasive Ptacek's testimony that knowledge of the schema would not in any way provide a threat actor an advantage in attacking a system like CANVAS. The court entered judgment in favor of plaintiff and against defendant. The court also ordered defendant to produce the requested records by February 10, 2020. Following defendant's posttrial motion, the court stayed its order to produce the requested records pending the outcome of an appeal.

¶ 23 On appeal, defendant made no argument that the requested information constituted a "source listing." Instead, defendant maintained 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. 2022 IL App (1st) 200547, ¶ 1. The First District disagreed and affirmed. First, without determining whether the information plaintiff requested was a " 'file layout' " or " 'any other information,' " the court found that, under the plain language of section 7(1)(*o*), the reasonable meaning of " 'if disclosed, would jeopardize' " applies to every item listed, not only to the catchall phrase of " 'and any other information.' " *Id.* ¶ 32. Second, the First District found the circuit court's finding that defendant failed to demonstrate by clear and convincing evidence that the exemption from disclosure provided in section 7(1)(*o*) applied to plaintiff's FOIA request was not against the manifest weight of the evidence. *Id.* ¶ 38. Thus, the court held defendant must provide the information plaintiff requested because the information was not exempt from disclosure under section 7(1)(*o*) of FOIA. *Id.* ¶ 42.

¶ 24 In March 2022, defendant petitioned this court for leave to appeal, and we allowed that petition. Ill. S. Ct. R. 315 (eff. Oct. 1, 2021).

¶ 25 ANALYSIS

¶ 26 Defendant raises two issues on appeal. First, defendant argues the plain language of section 7(1)(*o*) of FOIA expressly exempts the records plaintiff requested from disclosure. Second, defendant argues that section 7(1)(*o*) requires a public body to show only a possibility of harm to a data system's security and that it showed that disclosure of the requested records would jeopardize CANVAS's security.

¶ 27 I. Standard of Review

¶ 28 The first issue requires us to construe section 7(1)(*o*) of FOIA. Issues of statutory interpretation are reviewed *de novo*. *Rushton v. Department of Corrections*, 2019 IL 124552, ¶ 13. " 'The fundamental rule of statutory interpretation is to ascertain and give effect to the legislature's intent, and the best indicator of that intent is the statutory language, given its plain and ordinary meaning.' " *International Ass'n of Fire Fighters, Local 50 v. City of Peoria*, 2022 IL 127040, ¶ 12 (quoting *Dew-Becker v. Wu*, 2020 IL 124472, ¶ 12). In interpreting a statute, this "court may consider the reason for the law, the problems sought to be remedied, the

purposes to be achieved, and the consequences of construing the statute one way or another." *In re Appointment of Special Prosecutor*, 2019 IL 122949, ¶ 23.

¶ 29 A statute must be viewed as a whole, and "this court construes words and phrases not in isolation but relative to other pertinent statutory provisions." *In re Julie M.*, 2021 IL 125768, ¶ 27. Moreover, statutory provisions should be read so that no term is rendered superfluous or meaningless. *Id.* "When the plain language of the statute is clear and unambiguous, the legislative intent that is discernible from this language must prevail, and no resort to other interpretative aids is necessary." *In re Marriage of Kates*, 198 Ill. 2d 156, 163 (2001).

¶ 30 II. The Public Policy Behind FOIA

¶ 31 In conducting our review, we are mindful that, pursuant to FOIA, "public records are presumed to be open and accessible." *Illinois Education Ass'n v. Illinois State Board of Education*, 204 Ill. 2d 456, 462 (2003) (citing *Lieber v. Board of Trustees of Southern Illinois University*, 176 Ill. 2d 401, 407 (1997)). Section 1 of FOIA prescribes the public policy of Illinois and legislative intent of FOIA. 5 ILCS 140/1 (West 2018). Section 1 states, in part, as follows:

> "The General Assembly hereby declares 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. 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.
>
> This Act is not intended to cause an unwarranted invasion of personal privacy, nor to allow the requests of a commercial enterprise to unduly burden public resources, or to disrupt the duly-undertaken work of any public body independent of the fulfillment of any of the fore-mentioned rights of the people to access to information." *Id.*

¶ 32 "All records in the custody or possession of a public body are presumed to be open to inspection or copying." *Id.* § 1.2. A public body must comply with a proper request for information unless one of the statutory exemptions in section 7 applies. *Lieber*, 176 Ill. 2d at 407. This court has noted these "exemptions 'are to be read narrowly.' " *Mancini Law Group, P.C. v. Schaumburg Police Department*, 2021 IL 126675, ¶ 16 (quoting *Lieber*, 176 Ill. 2d at 407). "In the event a public body asserts that a record is exempt from such disclosure, the public body bears the burden of proving by clear and convincing evidence that the record is exempt." *Id.*; 5 ILCS 140/1.2 (West 2018).

¶ 33 III. Section 7(1)(*o*) and File Layouts

¶ 34 Section 7 of FOIA sets forth a series of exemptions to disclosure and provides, in relevant part:

> "(1) When a request is made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt. The public body shall make the remaining information available for inspection and copying. Subject to this requirement, the following shall be exempt from inspection and copying:
>
> * * *

> (*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).

¶ 35 Defendant argues the plain language of section 7(1)(*o*) establishes a *per se* exemption for file layouts. We agree.

¶ 36 We begin by noting this court has found a *per se* rule applies to most of the exemptions set forth in section 7. *Mancini*, 2021 IL 126675, ¶ 30. Thus, "[w]here the public body claims that a requested document falls within one of these specifically enumerated categories and is able to prove that claim, no further inquiry by the court is necessary." *Lieber*, 176 Ill. 2d at 408.

¶ 37 The exemption at issue in section 7(1)(*o*) is narrow in its focus—dealing with administrative or technical information associated with automated data processing operations. The statute specifically lists 10 items that are included within that focus, including file layouts. While the phrase "including but not limited to" indicates the list that follows is illustrative and not exhaustive (*People v. Perry*, 224 Ill. 2d 312, 328 (2007)), the inclusion of these 10 specific items evinces the legislature's intent that they be expressly exempt from disclosure, *i.e.*, the harm that would follow from disclosure of the listed items is presumed. Had the General Assembly intended to require the government agency to show disclosure of information would jeopardize the security of its system, the list of specific items would have been unnecessary.

¶ 38 In addition to listing the specific categories of information that are exempt, the legislature also included the 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*) (West 2018). The catchall phrase simply shows the legislature understood it could not specifically list every item that might fall within the exemption's scope and allowed for the protection of the system should it be proved that disclosure of a nonlisted item, *i.e.*, any other information, would jeopardize its security. See *People v. Newton*, 2018 IL 122958, ¶ 17 (finding the statutory catchall showed the legislature's recognition that it would not be possible to specifically list all places used primarily for religious worship).

¶ 39 In its analysis, the appellate court did not address the entirety of section 7(1)(*o*)'s exemption. However, a plain reading of the exemption as a whole confirms our conclusion that file layouts are expressly exempt. The last part of section 7(1)(*o*) mentions "materials exempt under this Section," thereby indicating the legislature's intent that the previously listed items are indeed exempt. To find otherwise would render the phrase "materials exempt under this Section" superfluous. See *Slepicka v. Illinois Department of Public Health*, 2014 IL 116927, ¶ 14 ("Each word, clause and sentence of a statute must be given a reasonable construction, if possible, and should not be rendered superfluous.").

¶ 40 With the foregoing in mind, the reasonable, commonsense interpretation of section 7(1)(*o*) that gives meaning to the listed items, the catchall, and the entire exemption as a whole leads to the conclusion that file layouts are exempt from disclosure. While it is true that, under FOIA, public records are presumed to be open and accessible, the legislature has specifically provided for a narrow exemption with respect to administrative or technical information associated with

automated data processing operations. The exemption in section 7(1)(*o*) is focused on the security of the government body's data system, and reading the exemption to require a hearing to determine whether disclosure would jeopardize the security of that system every time a file layout is requested would only weaken the specific exemption.

¶ 41 We note section 5 of FOIA requires a public body to "maintain and make available for inspection and copying a reasonably current list of all types or categories of records under its control," which "shall be reasonably detailed in order to aid persons in obtaining access to public records pursuant to this Act." 5 ILCS 140/5 (West 2018). Thus, section 5 provides the public with knowledge of what records are available and what can be obtained. However, the purpose of FOIA is not to put the security of the government's automated data processing operations at risk of unnecessary harm, and section 7(1)(*o*) provides a narrow and reasonable exemption to protect those operations, especially from the harm threatened by cyberattacks. Accordingly, we hold file layouts are *per se* exempt from disclosure.

¶ 42 IV. Plaintiff's Requested Records

¶ 43 Having found that file layouts are expressly exempt from disclosure under section 7(1)(*o*) without a showing that disclosure would jeopardize the security of the system, we need not address defendant's second issue. Instead, the question now becomes whether the records requested by plaintiff constitute file layouts. Plaintiff argues his requested "schema" does not fall within the definition of a file layout. Defendant, however, suggests dictionary definitions establish the requested records fall under the exemption. We agree with defendant.

¶ 44 File layouts are not defined in the statute. In such an instance, "this court has held it is appropriate to refer to a dictionary to ascertain the meaning of otherwise undefined words or phrases." *Skaperdas v. Country Casualty Insurance Co.*, 2015 IL 117021, ¶ 18 (citing *Lacey v. Village of Palatine*, 232 Ill. 2d 349, 363 (2009)); see also *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, ¶ 32 (stating this court may consult dictionaries to ascertain the plain and ordinary meaning of an undefined statutory term).

¶ 45 In his FOIA request, plaintiff sought an "index of the tables and columns within each table of CANVAS" and asked for the "column data type as well." "File layout" has been defined as the "description of the arrangement of the data in a file." McGraw-Hill Dictionary of Scientific & Technical Terms (6th ed. 2003), available at https://encyclopedia2.thefreedictionary.com/file+layout (last visited Apr. 10, 2023) [https://perma.cc/7JRF-MB62]. We find this definition encompasses the records requested by plaintiff.

¶ 46 Plaintiff, however, argues that the records he requested constituted "database schema" and not file layouts. "Schema" is defined as "a structured framework or plan: outline." Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/schema (last visited Apr. 11, 2023) [https://perma.cc/JU96-57T7]. Considering the definitions of both "file layout" and "schema," we find a difference in name only. Just as a file layout is the arrangement of data in a file, a schema is the framework or outline of a database.

¶ 47 As we have found the records requested by plaintiff are file layouts within the meaning of section 7(1)(*o*) of FOIA, those records are exempt from disclosure. Accordingly, the judgments of the circuit court and the appellate court are hereby reversed. We remand the cause to the circuit court for entry of judgment in favor of defendant and against plaintiff.

¶ 48 CONCLUSION

¶ 49 For the foregoing reasons, we reverse the judgments of the circuit court and the appellate court and remand to the circuit court with directions to enter judgment in favor of defendant.

¶ 50 Judgments reversed.

¶ 51 Cause remanded with directions.