

# Illinois Official Reports

## Appellate Court

***Better Government Ass'n v. Zaruba, 2014 IL App (2d) 140071***

Appellate Court Caption	BETTER GOVERNMENT ASSOCIATION, Plaintiff-Appellant, v. JOHN E. ZARUBA, as Sheriff of Du Page County, Defendant- Appellee.
District & No.	Second District Docket No. 2-14-0071
Filed	November 6, 2014
Held <i>(Note: This syllabus constitutes no part of the opinion of the court but has been prepared by the Reporter of Decisions for the convenience of the reader.)</i>	The trial court properly dismissed the complaint of the Better Government Association under the Freedom of Information Act seeking the production of records disclosing the vehicles and persons subjected to Law Enforcement Agencies Data System (LEADS) inquiries by the teenage son of defendant sheriff, pursuant to a course the son took through the Illinois Department of State Police's Learning Management System entitled "LEADS Less Than Full Access" that led to the son being certified as a LEADS operator certified and authorized to access LEADS through a certain date, since plaintiff is not a proper body to investigate an alleged improper use of LEADS but, rather, that task is left to the Illinois Department of State Police in view of the sensitive information involved.
Decision Under Review	Appeal from the Circuit Court of Du Page County, No. 13-MR-958; the Hon. Terence M. Sheen, Judge, presiding.
Judgment	Affirmed.

Counsel on  
Appeal

Paul T. Fox and Gregory E. Ostfeld, both of Greenberg Traurig, LLP,  
of Chicago, for appellant.

Robert B. Berlin, State's Attorney, of Wheaton (Lisa Anne Hoffman  
and Lisa A. Smith, Assistant State's Attorneys, of counsel), for  
appellee.

Panel

JUSTICE ZENOFF delivered the judgment of the court, with opinion.  
Justices Birkett and Spence concurred in the judgment and opinion.

## OPINION

¶ 1 Plaintiff, Better Government Association (BGA), appeals from the dismissal of its complaint seeking production of certain records from defendant, John E. Zaruba, as sheriff of Du Page County (the sheriff), pursuant to the Freedom of Information Act (FOIA) (5 ILCS 140/1 *et seq.* (West 2012)). Specifically, BGA requested records disclosing the vehicles and persons who were the subjects of Law Enforcement Agencies Data System (LEADS) inquiries conducted by Patrick Zaruba, the sheriff's teenage son. The trial court concluded that this information was exempt from disclosure under section 7(1)(a) of the FOIA (5 ILCS 140/7(1)(a) (West 2012)) and that a FOIA response to BGA's inquiries was not possible. For the reasons that follow, we affirm.

### ¶ 2 I. BACKGROUND

¶ 3 On June 28, 2012, BGA filed in the circuit court of Cook County its verified complaint for declaratory and injunctive relief against the sheriff. The case was subsequently transferred to the circuit court of Du Page County on the sheriff's motion.

¶ 4 BGA alleged that on May 29, 2012, it submitted FOIA requests to the sheriff, seeking the following:

“1) Copies of any and all documents relating to Patrick Zaruba's access to LEADS or other law enforcement databases. (Examples of such documents are Patrick Zaruba's LEADS application and other supporting materials.)

2) Copies of documents sufficient to show the names of any and all persons who because of their affiliation with the Du Page County Sheriff's office have become certified to use LEADS even though they're not sheriff's office employees, from Jan. 1, 2010, to present. (Examples of such persons are interns, Explorer scouts and ride-along participants.)

3) Copies of documents sufficient to show any and all written communication between the Illinois State Police and the Du Page County Sheriff's office relating to LEADS and/or Patrick Zaruba, from May 21, 2012, to present. (Examples of such communication include emails and letters.)”

On May 31, 2012, BGA submitted another FOIA request for “[c]opies of documents sufficient to show the vehicles and persons that were the subjects of LEADS inquiries conducted by Patrick Zaruba, from November 2010 to present.”

¶ 5 On June 4, 2012, the sheriff responded as follows to BGA’s requests:

“I am unable to supply any information that is responsive to your Freedom of Information request. LEADS is a system controlled by [the] Illinois State Police. You would need to contact them for information/confirmation of any certified user. You will also need to contact ISP for documentation of what persons/vehicles were the subjects of inquiries [*sic*] made by any certified user. As for written communication between ISP and the Du Page County Sheriff’s Office related to LEADS and or Patrick Zaruba from 5/21/12 to 5/29/12, I do not have information responsive to that request.”

¶ 6 According to the complaint, in violation of section 9 of the FOIA (5 ILCS 140/9 (West 2012)), the sheriff’s response failed to state any statutory basis for denying the first, second, and fourth categories of requests; identify any FOIA exemption; include a detailed factual basis for the application of any exemption; or inform BGA of its rights to judicial review and review by the Public Access Counselor. BGA alleged that it contacted the sheriff’s FOIA officer regarding these purported deficiencies in the sheriff’s response, but was told that the sheriff declined to revisit his position. In count I, BGA sought a declaration of its right to the requested documents, a declaration that the sheriff’s actions were willful, intentional, and done in bad faith, and an award of civil penalties. BGA sought injunctive relief in count II.

¶ 7 On October 2, 2013, the sheriff filed a motion to dismiss the complaint pursuant to section 2-619(a)(9) of the Code of Civil Procedure (Code) (735 ILCS 5/2-619(a)(9) (West 2012)). The sheriff argued that he was “not able to legally comply” with BGA’s requests, invoking section 7(1)(a) of the FOIA, which exempts public bodies from producing “[i]nformation specifically prohibited from disclosure by federal or State law or rules and regulations implementing federal or State law.” 5 ILCS 140/7(1)(a) (West 2012). The sheriff represented that, in addition to his June 4, 2012, response to BGA’s requests, on July 19, 2012, an assistant State’s Attorney had forwarded to BGA copies of (1) an agreement dated March 3, 2008, between the Illinois Department of State Police (Department) and the Du Page County sheriff’s office regarding LEADS access (the Agreement) and (2) Patrick’s certificate of completion for a course entitled “LEADS Less Than Full Access.” Although neither the Agreement nor the certificate is included in the record on appeal, the sheriff represented in his motion to dismiss that section VI of the Agreement provided:

“All data supplied through LEADS is strictly forbidden to be used for personal reasons. It is strictly forbidden to sell any information obtained to any individuals, organization, government agency or corporation. It is strictly forbidden to disseminate any information obtained through LEADS to any individual organization that is not legally authorized to have access to that information.”

The sheriff insisted that he would breach the Agreement if he were to provide the requested records to BGA. Moreover, he argued that disclosure was prohibited by the Department’s regulations, which are codified in the Illinois Administrative Code and provide that “LEADS data shall not be disseminated to any individual or organization that is not legally authorized to have access to the information” (20 Ill. Adm. Code 1240.80(d) (1999)) and that a violation may result in suspension of LEADS service (20 Ill. Adm. Code 1240.110 (1999)). The sheriff

supported his motion with the affidavit of Darlene A. Jacobs, the LEADS statewide coordinator for the Department. She asserted that the information BGA requested, “should it exist,” could not be released by the sheriff in light of the Administrative Code and the Agreement.

¶ 8 In its response to the motion, BGA argued that none of the requests sought either information “obtained through LEADS” or “LEADS data” so as to implicate the Agreement or the Administrative Code. BGA noted that the regulations define “LEADS data” as “all data available through the LEADS computer” (20 Ill. Adm. Code 1240.30(b)(3) (1999)), emphasizing that it was “seeking requests made by Patrick *to* the LEADS system, not personal information or data obtained *from* the LEADS system.” (Emphases in original.) Accordingly, BGA attempted to distinguish between the results of Patrick’s searches, which it recognized would constitute “LEADS data,” and the subjects of Patrick’s LEADS inquiries, which it argued would not. Additionally, BGA argued that the Agreement was not a basis for an exemption under section 7(1)(a) of the FOIA, because the Agreement was neither a law nor a rule or regulation implementing the law. Moreover, BGA argued, the Agreement and the Administrative Code did not specifically prohibit the sheriff from disclosing public records relating to unauthorized LEADS inquiries. In BGA’s words, “[t]he Sheriff cannot hide behind agreements or administrative regulations designed to *prevent* unauthorized access to the LEADS system in order to *conceal* such unauthorized access.” (Emphases in original.)

¶ 9 In his reply brief in support of the motion to dismiss, the sheriff apparently abandoned his argument premised on the Agreement, but continued to insist that he properly withheld “LEADS data” as that term is used in the regulations. He submitted a second affidavit from Jacobs, in which she asserted the following:

“That on November 22, 2010, Patrick Zaruba successfully completed the course entitled ‘LEADS Less Than Full Access’ through the [Department’s] Learning Management System (LMS). As a result of his completion of this course, Patrick Zaruba was LEADS operator certified and authorized to access LEADS through November 22, 2012.

That in order to inquire on a person through the LEADS system, the LEADS operator will submit inquiry identifiers of last name, first name, middle initial, sex, and date of birth and/or their driver’s license number into the LEADS System. Once this information is submitted into the LEADS system it is LEADS data and part of the complete LEADS record maintained by the Illinois State Police.

That through LEADS 2000, the Illinois State Police can only identify a device accessing the LEADS system by its assigned Call Directing Code (CDC) and not the unique identifiers of a certified user accessing the system.

That the Illinois Administrative Code Title 20, Part 1240.80 prohibits the dissemination of LEADS data to any individual and/or organization that is not legally authorized to have access to the information and the Better Government Association is not legally authorized to receive LEADS data.”

Accordingly, the sheriff argued, “the Illinois State Police does not distinguish between information *input* into the LEADS system and any other information contained in the system.” (Emphasis in original.) The sheriff insisted that he could not provide the requested

information to BGA without “intentionally violating the Illinois Administrative Code and thereby subjecting [himself] to a potential suspension of all or a portion of LEADS services.”

¶ 10 The sheriff also contended that Jacobs’ affidavit demonstrated that “the Illinois State Police is not able to confirm what, if any, inquiries were made by Patrick Zaruba,” because “the Illinois State Police can only identify what device the request comes from and not who is using the device.” Finally, the sheriff emphasized that there was no evidence that Patrick had used the LEADS system, let alone for an improper purpose, noting that the Department had not restricted Patrick’s access to the system or suspended the sheriff’s office’s use of the system due to any violation.

¶ 11 On December 18, 2013, the parties appeared before the court for its ruling on the motion to dismiss. During the brief hearing, BGA suggested that there was a question of fact as to whether any of the records responsive to the FOIA requests qualified as “LEADS data.” It also argued that, because Jacobs averred in her second affidavit that the LEADS system could not link specific inquiries to Patrick, BGA did not seek information “available through the LEADS computer.” Therefore, BGA argued, it was entitled to discovery to determine whether there were any responsive records available from the sheriff rather than through the LEADS computer.

¶ 12 In a written order, the court granted the sheriff’s motion to dismiss, concluding that the Administrative Code prohibited the sheriff from disseminating the requested information. The court reasoned that the “broad terms” of the regulations “indicate intent to limit all information in the LEADS system to people with the proper authorization.” Additionally, the court described as “a fallacy” BGA’s argument that Patrick’s input information was not “LEADS data.” The court noted that, according to Jacobs’ second affidavit, “once inquiry identifier information is submitted to LEADS, it is LEADS data and part of the complete LEADS record maintained by the Illinois State Police.” Furthermore, the court explained, interpreting “LEADS data” to include input information was consistent with the intent of the regulations, because the “expansive” definition of “LEADS data” is “not limited to data that can be drawn from the system about a particular subject,” but, instead, is “all data available through the LEADS computer.” The court added: “Assuming it is possible to query who Patrick Zaruba looked up in the system (which no evidence has been submitted to prove this is even possible), one would presumably need to obtain this information by going to a LEADS computer and accessing the system.” Accordingly, the court found that such information was “made available ‘through the LEADS computer’ ” (quoting 20 Ill. Adm. Code 1240.30(b)(3) (1999)).

¶ 13 The court also addressed BGA’s argument that the court’s interpretation would lead to an absurd result. The court explained that, while it was “true that the regulation at issue was created, in part, to prevent use of the LEADS system for personal purposes,” there was “nothing to prevent the appropriate body, properly authorized to access the LEADS system, from investigating any alleged improper uses.” Under the court’s interpretation, “entities such as the BGA are not the proper organizations to undertake such an investigation because the investigation requires access to sensitive information to which the legislative body saw fit to restrict access.” Moreover, the court found that there was “no evidence to suggest that Patrick Zaruba utilized LEADS for an improper purpose,” so “it would be difficult to argue that denying BGA access to the requested records allows the [sheriff] to protect Patrick’s abusive practices by using anti-abuse regulations.”

¶ 14 Finally, the court found that it was not possible for the sheriff to produce records reflecting Patrick’s LEADS inquiries:

“One final salient point noted by the [sheriff] is that the information sought by BGA does not exist. \*\*\* According to Darlene Jacobs, the Illinois State Police can only use the LEADS system to identify a device accessing the LEADS system by its assigned Call Directing Code and not the unique identifies [sic] of a certified user accessing the system. \*\*\* That is, even if the applicable regulations did not operate to deny BGA’s access, the Illinois State Police would not be able to determine which inquiries, if any, were submitted by Patrick Zaruba. As such, a FOIA response to BGA’s inquiries is not possible.”

¶ 15 BGA timely appeals.

## ¶ 16 II. ANALYSIS

¶ 17 On appeal, BGA argues that only LEADS records maintained by the Department, not the sheriff’s public records, are exempt from disclosure. BGA also contends that the term “LEADS data,” as used in the Department’s regulations, encompasses only data available through the LEADS computer, not inquiries submitted to the LEADS computer. Additionally, BGA suggests that the trial court’s interpretation of the regulations had the absurd effect of allowing the state law designed to prevent abuse of the LEADS system to be used to shield such abuses from disclosure. Finally, BGA argues that the court erred in concluding, without allowing BGA to conduct discovery, that the requested records did not exist.

¶ 18 At the outset, we note that BGA has specifically challenged on appeal the trial court’s ruling only as it relates to the request for “[c]opies of documents sufficient to show the vehicles and persons that were the subjects of LEADS inquiries conducted by Patrick Zaruba, from November 2010 to present.” Accordingly, we will not consider the propriety of the trial court’s order as it relates to any of BGA’s other FOIA requests. See Ill. S. Ct. R. 341(h)(7) (eff. Feb. 6, 2013) (points not argued in the appellant’s brief are forfeited).

¶ 19 The purpose of the FOIA is “to open governmental records to the light of public scrutiny.” (Internal quotation marks omitted.) *Watkins v. McCarthy*, 2012 IL App (1st) 100632, ¶ 13. Under the FOIA public records are presumed to be open and accessible (*Heinrich v. White*, 2012 IL App (2d) 110564, ¶ 8), and courts liberally construe the act to achieve the goal of “provid[ing] the public with easy access to government information” (*Southern Illinoisan v. Illinois Department of Public Health*, 218 Ill. 2d 390, 416 (2006)). While “[t]he FOIA may not be used to violate individual privacy rights or disrupt the proper work of a governmental body beyond its responsibilities under the Act,” a public body “must comply with a valid request for information unless one of the narrow statutory exemptions set forth in section 7 of the FOIA applies.” *Watkins*, 2012 IL App (1st) 100632, ¶ 13. It is the public body’s burden to prove by clear and convincing evidence that the requested records fall within any claimed exemption. 5 ILCS 140/11(f) (West 2012). The public body meets this burden by providing “a *detailed* justification for its claimed exemption, addressing the requested documents specifically and in a manner allowing for adequate adversary testing.” (Emphasis in original and internal quotation marks omitted.) *Day v. City of Chicago*, 388 Ill. App. 3d 70, 74 (2009).

¶ 20 This appeal requires us to interpret the term “LEADS data” as defined in section 1240.30(b)(3) of Title 20 of the Administrative Code. We interpret administrative regulations in the same manner that we would interpret a statute. *Arellano v. Department of Human Services*, 402 Ill. App. 3d 665, 673 (2010). “[O]ur primary aim is to give effect to the drafters’ intent, and the best indicator of that intent is the regulation’s language, given its plain and ordinary meaning.” *Arellano*, 402 Ill. App. 3d at 673. Construction of a regulation presents a question of law, which we review *de novo*. *Nelson v. Kendall County*, 2014 IL 116303, ¶ 22. *De novo* review is also appropriate because the trial court dismissed BGA’s complaint pursuant to section 2-619(a)(9) of the Code. *Nelson*, 2014 IL 116303, ¶ 22. “[A] section 2-619 motion admits the legal sufficiency of the claims but raises defects, defenses, or other affirmative matter, appearing on the face of the complaint or established by external submissions, that defeats the action.” (Internal quotation marks omitted.) *Lucas v. Prisoner Review Board*, 2013 IL App (2d) 110698, ¶ 13. In reviewing the trial court’s order, we consider the pleadings and the affidavits in the light most favorable to BGA, as the nonmoving party. *Lucas*, 2013 IL App (2d) 110698, ¶ 14.

¶ 21 The sheriff relies exclusively on section 7(1)(a) of the FOIA, which exempts from disclosure “[i]nformation specifically prohibited from disclosure by federal or State law or rules and regulations implementing federal or State law.” 5 ILCS 140/7(1)(a) (West 2012). This court has held that, even if a statute does not specifically provide that records are exempt from disclosure under the FOIA or otherwise contain an explicit prohibition against public disclosure, records are nevertheless exempt “where the plain language contained in a State or federal statute reveals that public access to the records was not intended.” *Kibort v. Westrom*, 371 Ill. App. 3d 247, 256 (2007). On the other hand, section 7(1)(a) does not apply “where a state or federal statute is ambiguous or silent in regard to the disclosure of public records.” *Kibort*, 371 Ill. App. 3d at 256.

¶ 22 LEADS is “a statewide, computerized telecommunications system designed to provide services, information, and capabilities to the law enforcement and criminal justice community in the State of Illinois.” 20 Ill. Adm. Code 1240.10(a) (1999). “To connect to LEADS, an agency must have computer hardware and computer software, and be connected to a communications link to the LEADS Data Center in Springfield.” 20 Ill. Adm. Code 1240.40(a) (1999). “The Director of the State Police (Director) is responsible for establishing policy, procedures, and regulations consistent with State and federal rules, policies, and law by which LEADS operates.” 20 Ill. Adm. Code 1240.10(b) (1999).

¶ 23 The regulations contemplate either “[f]ull access” or “[l]ess than full access” to “LEADS data and services.” 20 Ill. Adm. Code 1240.30(b)(2), (b)(5) (1999). “LEADS data” is defined as “all data available through the LEADS computer” (20 Ill. Adm. Code 1240.30(b)(3) (1999)), and “LEADS services” refers to “A) providing access to LEADS files; B) processing messages through LEADS; C) providing training and technical support to LEADS users; and D) other LEADS-related services that may become available from the Department” (20 Ill. Adm. Code 1240.30(b)(4)(A)-(D) (1999)). In order to have full access, which is defined as “direct access to all LEADS data and services” (20 Ill. Adm. Code 1240.30(b)(2) (1999)), the candidate organization must qualify under one of the subsections of section 1240.30(c)(1) and enter into a LEADS interagency agreement reflecting the rights and duties of the parties (20 Ill. Adm. Code 1240.30(c)(1), (c)(2) (1999)). In contrast, less than full access refers to “limited access to some LEADS data and services.” 20 Ill. Adm.

Code 1240.30(b)(5) (1999). LEADS agency personnel with either full access or less than full access must undergo mandatory LEADS-user certification administered by the Department. 20 Ill. Adm. Code 1240.90(b)(1), (b)(2) (1999).

¶ 24 Additionally, “[e]ach LEADS participating agency shall comply with the LEADS access security standards established by the Department.” 20 Ill. Adm. Code 1240.50(a) (1999). The regulations specify certain personnel-security requirements, including a “[t]horough background screening” for “terminal operators, programmers, and other persons employed or utilized to effectuate access to or initiate transmission of LEADS and National Crime Information Center (NCIC) information.” 20 Ill. Adm. Code 1240.50(b)(1) (1999). Persons who are not of good character or who have been convicted of a felony are not permitted LEADS access and may not provide maintenance or technical services at or near LEADS equipment. 20 Ill. Adm. Code 1240.50(b)(2), (b)(3) (1999). The regulations provide that “LEADS operators shall use the terminal only for those purposes for which they are authorized” and that “[t]he individual receiving a request for criminal justice information must ensure the person requesting the information is authorized to receive the data.” 20 Ill. Adm. Code 1240.50(b)(4) (1999). Furthermore, “[e]ach LEADS agency must ensure that all LEADS computer devices are placed in a location under the direct control and supervision of authorized criminal justice personnel and are inaccessible to the public or persons not qualified to either operate, view, or possess LEADS and/or NCIC transmitted or received data.” 20 Ill. Adm. Code 1240.50(c) (1999). “The computer site and/or terminal area must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.” 20 Ill. Adm. Code 1240.50(c) (1999).

¶ 25 Section 1240.80 regulates the dissemination of data obtained through LEADS and provides as follows: “a) The LEADS network and LEADS data shall not be used for personal purposes[;] b) Personal or unofficial messages shall not be transmitted[;] c) LEADS data shall not be sold[;] [and] d) LEADS data shall not be disseminated to any individual or organization that is not legally authorized to have access to the information.” 20 Ill. Adm. Code 1240.80(a)-(d) (1999). The regulations provide that “[u]ser certification may be suspended or revoked by the Department for violation or non-compliance with laws, rules, regulations, or procedures.” 20 Ill. Adm. Code 1240.90(b)(9) (1999). The Department also periodically audits each LEADS terminal agency and provides “a written analysis detailing the findings, recommendations, discussions, and requirements for compliance generated by the audit.” 20 Ill. Adm. Code 1240.100(a), (c) (1999). The available sanctions and the required procedures depend on the severity of the violations. 20 Ill. Adm. Code 1240.110 (1999).

¶ 26 BGA argues that the sheriff is not specifically prohibited from disclosing information regarding the subjects of Patrick’s LEADS searches, because such information is not “LEADS data.” BGA focuses primarily on section 1240.30(b)(3), which defines “LEADS data” as “all data available through the LEADS computer.” 20 Ill. Adm. Code 1240.30(b)(3) (1999). From this definition, BGA extrapolates that there is a meaningful difference between search input information (inquiry identifiers) and substantive information available through the system (the results of those inquiries). According to BGA, the Department’s regulations do not specifically prohibit the sheriff from disclosing records falling into the former category. BGA proposes that, had “LEADS data” been intended to encompass inquiries to the LEADS



computer, the Department could have defined the term as information “*submitted to or available through the LEADS computer.*”

¶ 27

Nothing in the regulations suggests that the Department intended to draw such a distinction, and we hold that the regulations specifically prohibit the sheriff from disclosing information regarding the inquiries performed by LEADS users. Even if BGA’s interpretation of “LEADS data” is plausible when considering section 1240.30(b)(3) in isolation, it does not hold up when viewing the regulations as a whole. “A fundamental principle of statutory construction is to view all provisions of a statutory enactment as a whole. Accordingly, words and phrases should not be construed in isolation, but must be interpreted in light of other relevant provisions of the statute.” *Southern Illinoisan*, 218 Ill. 2d at 415. Another provision of the regulations, which the parties do not address, indicates that the Department does not distinguish between information transmitted through LEADS and information stored in the system. Specifically, section 1240.50(c) provides:

“Each LEADS agency must ensure that all LEADS computer devices are placed in a location under the direct control and supervision of authorized criminal justice personnel and are inaccessible to the public or persons not qualified to either operate, view, or possess LEADS and/or NCIC *transmitted or received data*. The computer site and/or terminal area must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the *stored data*.” (Emphases added.) 20 Ill. Adm. Code 1240.50(c) (1999).

The regulations make clear that the public is not entitled to view or possess data that is transmitted through, received through, or stored in LEADS. BGA insists that inquiry identifier information is not “available through” the LEADS computer, because Jacobs’ second affidavit established that “the Illinois State Police can only identify a device accessing the LEADS system by its assigned Call Directing Code \*\*\* and not the unique identifiers of a certified user accessing the system.” However, even if Patrick’s personal search history is not presently *stored in* the LEADS computer, it was, by its very nature, data that was *transmitted through* the system. Section 1240.50(c) makes clear that the Department intended for such information to be treated in the same manner as information received through or stored in the system.

¶ 28

Another provision of the regulations, which the parties likewise do not address, renders BGA’s interpretation of the definition of “LEADS data” questionable. Section 1240.50(b) provides certain personnel-security requirements, including that “[t]he individual receiving a request for criminal justice information must ensure the person requesting the information is authorized to receive the data.” 20 Ill. Adm. Code 1240.50(b)(4) (1999). The regulations do not define “criminal justice information.” However, information about which people or vehicles have been the subjects of LEADS inquiries would seem to fall naturally within the scope of that term. That the Department requires a showing of authority to receive “criminal justice information”—a rather broad and undefined phrase—cuts against BGA’s argument that, by defining “LEADS data” as it did in section 1240.30(b)(3), the Department intended to make LEADS search histories accessible to the public.

¶ 29

The regulations, viewed in their entirety, reflect the Department’s intent to create a law enforcement resource that is not open to public inspection. We cannot agree with BGA that, by defining “LEADS data” as it did in section 1240.30(b)(3), the Department intended to allow the public to know which suspects have been investigated by particular law

enforcement officers. Such a construction of “LEADS data” is neither necessary nor reasonable in the context of regulations designed to prohibit rather than promote public access to the LEADS system. It is readily apparent that public access to inquiry identifier information was not intended and that the regulations do not treat such information differently from other information stored in or accessible through the system.

¶ 30 BGA additionally argues that only LEADS records maintained by the Department, not the sheriff’s public records, are exempt from disclosure as “LEADS data.” BGA claims that, because Jacobs’ second affidavit established that Patrick’s search history cannot be identified by means of the LEADS computer, such information is not “LEADS data.” We disagree with BGA’s assessment. As we have previously explained, the information that BGA seeks—the identities of the subjects of Patrick’s LEADS inquiries—is inherently “LEADS data” prohibited from disclosure. The regulations do not distinguish between information transmitted or received through LEADS and information stored in the system. Nor has BGA brought to our attention any authority that would require a different result. BGA is not entitled to Patrick’s search history, irrespective of whether such information is accessible through the LEADS system or from records that the sheriff possesses.

¶ 31 The reasoning in at least one federal case supports by analogy that LEADS inquiry identifier information is not subject to public disclosure. In *Vazquez v. United States Department of Justice*, 887 F. Supp. 2d 114, 117 (D.D.C. 2012), the plaintiff filed an action under the federal FOIA, seeking a log of NCIC transactions concerning himself. The Department of Justice (DOJ) issued what is known as a “*Glomar* response,” refusing to confirm or deny the existence of any responsive records, because doing so would cause harm cognizable under an exception to the federal FOIA. *Vazquez*, 887 F. Supp. 2d at 116. The DOJ based its response on 5 U.S.C. § 552(b)(7)(E), which exempts law enforcement records from disclosure to the extent that production “would disclose techniques and procedures for law enforcement investigations or prosecutions ... if such disclosure could reasonably be expected to risk circumvention of the law.” (Internal quotation marks omitted.) *Vazquez*, 887 F. Supp. 2d at 116. The DOJ filed a motion for dismissal and summary judgment, supported by the affidavit of Kimberly Del Greco, who described the NCIC as a compilation of “nineteen separate databases, all of which contain material compiled for law-enforcement purposes.” (Internal quotation marks omitted.) *Vazquez*, 887 F. Supp. 2d at 117. She stated that “NCIC transactions [are] performed[ ] in response to queries made by law enforcement agencies regarding an individual” and that “while the public generally knows and understands that law enforcement utilizes the NCIC databases to perform background checks and/or other related checks ... the details of those queries—including how they are executed, what search terms are used, what[ ] passwords and clearances are required, and who has authorization to run such queries[—]are not known to the public.” (Internal quotation marks omitted.) *Vazquez*, 887 F. Supp. 2d at 117. The district court found that Del Greco’s affidavit “established the threshold requirement that the responsive records be compiled for law enforcement purposes” and showed that “utilization of the NCIC database constitutes a ‘procedure[ ] for law enforcement investigations’ covered by exemption 7(E).” *Vazquez*, 887 F. Supp. 2d at 117 (quoting 5 U.S.C. § 552(b)(7)(E) (2006)).

¶ 32 Del Greco additionally explained the nature of the harm from having to confirm or deny the existence of the requested records:

“[P]ublic confirmation of NCIC transactions would alert individuals that they are the subject of an investigation as well as reveal[ ] the identity of the investigative agency. With this information, individuals could modify their criminal behavior, thereby preventing detection by law enforcement agencies and risking circumvention of the law. [Citation.] In other words, persons knowing that they are being investigated by a law enforcement entity, which the requested information would reveal, could reasonably be expected to use the information to circumvent the law. Conversely, a person with knowledge that there have been no NCIC checks run against him, and hence, that he is not on law enforcement’s radar[,] could reasonably be expected to continue to engage in unlawful endeavors with renewed vigor.” (Internal quotation marks omitted.) *Vazquez*, 887 F. Supp. 2d at 117-18.

Based on this affidavit, the district court found that the DOJ justified its assertion of harm from confirming or denying the existence of the requested records, and the court granted summary judgment in favor of the DOJ. *Vazquez*, 887 F. Supp. 2d at 118. The court of appeals summarily affirmed in an unpublished order, concluding that the district court “properly granted the government’s renewed motion for summary judgment with respect to information withheld under Freedom of Information Act exemption 7(E) [citation] and did not abuse its discretion in denying reconsideration of that judgment.” *Vazquez v. United States Department of Justice*, No. 13-5197, 2013 WL 6818207, \* 1 (D.C. Cir. Dec. 18, 2013) (*per curiam*).

¶ 33 According to the Illinois Criminal Justice Information Authority’s website ([http://www.icjia.state.il.us/ijis/public/index.cfm?metasection=strategicplan&metapage=sjis\\_leads](http://www.icjia.state.il.us/ijis/public/index.cfm?metasection=strategicplan&metapage=sjis_leads) (last visited Oct. 6, 2014)), LEADS users are able to access NCIC through LEADS. See also 20 Ill. Adm. Code 1240.50(b)(1) (1999) (requiring background checks for “terminal operators, programmers, and other persons employed or utilized to effectuate access to or initiate transmission of LEADS and National Crime Information Center (NCIC) information”). As federal courts have determined that the public is not entitled to information regarding NCIC inquiries, it makes sense that this same type of information is not accessible to the public through LEADS.

¶ 34 Furthermore, we reject BGA’s argument that our interpretation creates an absurd result by allowing the state law designed to prevent abuse of the LEADS system to be used to shield such abuses from disclosure. The regulations indeed establish, in no uncertain terms, that LEADS users may not use the network or data for personal purposes (20 Ill. Adm. Code 1240.80(a) (1999)) and that such misuse may result in sanctions (20 Ill. Adm. Code 1240.90(b)(9) (1999)). However, as previously explained, the Department periodically audits LEADS terminal agencies, and the Department has implemented sanctions and procedures for addressing noncompliance with its policies. 20 Ill. Adm. Code 1240.110 (1999). As the trial court aptly noted: “There is nothing to prevent the appropriate body, properly authorized to access the LEADS system, from investigating any alleged improper uses. The aforementioned construction merely finds that entities such as the BGA are not the proper organizations to undertake such an investigation because the investigation requires access to sensitive information to which the legislative body saw fit to restrict access.”

¶ 35 Finally, BGA argues that the trial court erred in concluding that “a FOIA response to BGA’s inquiries is not possible” because Jacobs’ second affidavit showed that the Department “would not be able to determine which inquiries, if any, were submitted by

Patrick.” We need not address BGA’s argument on this point in light of our holding that BGA is not entitled to disclosure of the subjects of Patrick’s LEADS searches.

¶ 36

### III. CONCLUSION

¶ 37

The judgment of the circuit court of Du Page County is affirmed.

¶ 38

Affirmed.