PRESENT: Kelsey, McCullough, Chafin, Russell, and Mann, JJ., and Mims, S.J.

MATTHEW KEIL

v. Record No. 240824

JIM O'SULLIVAN, IN HIS OFFICIAL CAPACITY AS SHERIFF OF CITY OF CHESAPEAKE, VIRGINIA

OPINION BY
JUSTICE D. ARTHUR KELSEY
FEBRUARY 12, 2026

FROM THE COURT OF APPEALS OF VIRGINIA

In 2022, the Chesapeake Sheriff's Office demoted Officer Matthew Keil following an internal-affairs investigation. In response, Keil made a request for records pursuant to the Virginia Freedom of Information Act, Code §§ 2.2-3700 to -3715 ("VFOIA"), and the Government Data Collection and Dissemination Practices Act, Code §§ 2.2-3800 to -3809 ("Government Data Act"). Some records were produced; some were not. The circuit court and Court of Appeals rejected Keil's requests for production of the contested records. We agree with the lower courts that Keil has no remedy under the VFOIA. We take a different view, however, of his claim for records under the Government Data Act.

I.

Prior to his demotion, Keil supervised deputies at the Chesapeake City Jail who were involved in a jailhouse incident with an inmate. The Chesapeake Sheriff's Office ("CSO") conducted an internal-affairs investigation of the incident, which resulted in disciplinary actions against several deputies and Keil. Following his demotion, Keil made various requests for documentary and video records under the VFOIA and the Government Data Act.[1] The CSO

[1] Keil also requested documents pursuant to the "Freedom of Information Act (FOIA), 5 U.S.C. section 552." R. at 271. That statute, however, applies only to federal governmental agencies. *See* 5 U.S.C. § 552(f)(1); *see also Department of Homeland Sec. v. MacLean*, 574 U.S. 383, 396 (2015); *Milner v. Department of the Navy*, 562 U.S. 562, 564 (2011). *See generally* 4 Charles H. Koch, Jr., Administrative Law and Practice § 14:24, at 425, 430 (3d ed.

produced Keil's personnel file but denied the VFOIA requests for the internal-affairs records as exempt under Code § 2.2-3706(B)(4) (records related to "persons imprisoned in penal institutions") and Code § 2.2-3706(B)(9) (records, inter alia, of "administrative investigations" of wrongful conduct by law-enforcement officers). For reasons not clear from the record, the CSO never specifically responded to Keil's request for information under the Government Data Act.

Keil filed suit in general district court against Sheriff Jim O'Sullivan, in his official capacity,[2] seeking the withheld records. After receiving an adverse ruling in the district court, Keil appealed to the circuit court seeking a de novo review of his request for all CSO records referencing him "regarding the internal investigation of [the] incident in the jail, including interviews and videotapes." R. at 419.

The circuit court rejected Keil's VFOIA claim because it sought records exempt from disclosure under Code § 2.2-3706(B)(9). The circuit court also denied Keil's requests under the Government Data Act. Such records can be obtained only if the requester "is a 'data subject'" under the Act. *Id.* at 425 (quoting Code § 2.2-3801). Keil was not a statutory "data subject," the court held, because the "internal affairs investigative files" that he requested are "not searchable by employee name" and, instead, are simply "indexed by year and sequential numbering." *Id.* (citations omitted). The court also found that the records are not "indexed" or "search[able]" by using Keil's employee "personal number, or other identifiable particulars." *Id.* at 426 (quoting

---

2010) ("The FOIA applies to *federal* agencies only. The federal FOIA does not apply to state or city agencies. (But all states have their own FOIAs.)" (emphasis in original) (footnote and citation omitted)).

[2] Suing an official in his or her "official capacity" is "functionally" a suit against the entity itself. *See Brooks-Buck v. Wahlstrom*, 304 Va. 470, 482 n.5 (2025) (citing *Kentucky v. Graham*, 473 U.S. 159, 165 (1985)); *see also Kentucky*, 473 U.S. at 165-66 ("Official-capacity suits . . . 'generally represent only another way of pleading an action against an entity of which an officer is an agent.'" (quoting *Monell v. New York City Dep't of Soc. Servs.*, 436 U.S. 658, 690 n.55 (1978))).

Code § 2.2-3801). The court further observed that the records sought are "not part of an employee's personnel file." *Id.* at 425-26.

Keil appealed to the Court of Appeals. In its opinion, the Court of Appeals affirmed the circuit court's holding that the CSO did not violate the VFOIA by failing to separately respond to Keil's overlapping pre-litigation requests. *Keil v. O'Sullivan*, 81 Va. App. 695, 719-21 (2024). The Court of Appeals also agreed with the circuit court that Keil was not a "data subject" under the Government Data Act and thus had no statutory standing to request the internal-affairs records potentially implicating him. *See id.* at 710-19. On these two grounds, the Court of Appeals concluded "that Keil was not entitled to any relief under either VFOIA or the Data Act." *Id*. at 728.

II.

Finding no error in the VFOIA ruling by the Court of Appeals,[3] we limit our review to its analysis of the Government Data Act in this case. On this issue, we hold that the CSO violated the Act by refusing to provide Keil access to the internal-affairs records related to Keil's challenged actions or inactions in his capacity as a supervising deputy sheriff.

A.

Unlike other statutes shielding government information from the public, the Government Data Act "does not make [covered] personal information confidential but establishes certain

[3] We agree with Part II of the opinion of the Court of Appeals, *Keil*, 81 Va. App. at 719-21, with one inconsequential exception. The Court of Appeals stated that "the record does not show that Keil petitioned for mandamus or injunction supported by an affidavit showing good cause, as required by Code § 2.2-3713(A)." *Id.* at 727. Code § 8.01-4.3, however, authorizes an "unsworn written declaration, certificate, verification, or statement, which is subscribed by the maker as true under penalty of perjury" to serve as an affidavit "in any judicial proceeding or administrative hearing" in which an affidavit is required. Keil's "Verified Complaint and Motion for Judgment" was subscribed by Keil with the required certification: "I certify under penalty of perjury that the foregoing is true and correct." R. at 148, 152.

practices which must be followed in the collection, retention, and dissemination of that information." *Carraway v. Hill*, 265 Va. 20, 23 (2003). The Act first appeared in the Code of Virginia with the title, "Privacy Protection Act of 1976." 1976 Acts ch. 597, at 740-44. It was a legislative response to a report from the Virginia Advisory Legislative Council ("VALC"), which observed that the government's "capacity to gather, order and disseminate information has grown tremendously in the past decades. As this capacity has grown, man has become increasingly aware of the potential dangers to individual liberty posed by possible abuse of this capacity." VALC, *Computer Privacy and Security*, S. Doc. No. 27, at 3 (1976).

Our understanding of this statute relied heavily on these concerns in *Hinderliter v. Humphries*, 224 Va. 439, 444 (1982). In that case, a police officer arrested a young woman based upon a "drunk and disorderly" complaint by a local restauranteur. *Id.* at 444-45. In response to a request by the arrestee's mother (who was also a member of the county's board of supervisors), the police department conducted an "internal investigation" and shared its confidential report of that investigation with the mother. *Id.* at 444-46. She considered the report to be "public information" and claimed that "she had the right and obligation to disseminate [its] contents." *Id.* at 446. Confident of that opinion, she then allowed her daughter to obtain a copy of the internal-investigation report prior to her criminal trial on the drunk-and-disorderly charge. *Id.*

Among the questions that we answered in *Hinderliter*, the principal one was whether the internal-investigation report was subject to the Privacy Protection Act of 1976. The report was in paper form stored in file folders in the police department and included within the "officers' personnel files," which were "arranged alphabetically by the individual's name." *Id.* at 445. We held that the officer was a "data subject" because his "personal information" in the internal-

investigation report "is indexed or may be located under his name or other identification in an 'information system.'" *Id.* at 447 (quoting predecessor statute to Code § 2.2-3801).

The "[p]ersonal information" under the Act, we observed, included "all data describing anything about an individual" including "facts relating to . . . [his] employment record." *Id.* (citation omitted). That definition applied to the internal-investigation record in *Hinderliter* because the officer's "personnel file[]" included, among other things, "disciplinary information." *Id.* at 445. The officer asserted that it inaccurately "impute[d] to [him] violations of law and unfitness to perform the duties of a police officer." *Id.* at 446.

We then held that the officers' "personnel records" were included within the Act's definition of an "information system" because that term broadly included "the total components of a record-keeping process, whether automated or manual, containing personal information about a data subject." *Id.* at 447 (citation omitted). Our summary in *Hinderliter* put all of these factors together. The officer

> was a "data subject." "Personal information" was included in the report in question because the contents bore on his employment record and personal traits. And the personnel records kept by the Chief of Police, of which the report became a part, qualified as an "information system" because it was a manual record-keeping process containing personal particulars on a data subject.

Id. It did not matter that the information was recorded in paper documents placed in file folders at the police station. "The term 'information system' means the total components of a record-keeping process, whether automated or manual, containing personal information about a data subject." *Id.* (citation omitted). For these reasons, the officer had a statutory right to review the internal-investigation report to the extent that it directly or indirectly addressed him personally. Consistent with this obligation, the police chief allowed officers to "review" their own personnel records (as well as "disciplinary information" therein) "at any time." *Id.* at 445.

We parted company with the arguments of the officer in *Hinderliter* only on one point. He claimed that the Act also prohibited the police chief and county executive from sharing the internal-investigation report with the arrestee's mother. *See id.* at 448. We disagreed. Given her "official capacity" as a member of the "County Board of Supervisors," we held that they had a "proper purpose" for sharing the report with the mother-qua-supervisor. *Id.* at 448-49. We fully agreed, however, with the officer's claim that she had violated the Act by disseminating the report to her daughter. *Id.* at 449. Doing so "was unnecessary to accomplish any proper purpose of the Board of Supervisors." *Id.* "Rather, the circulation was to serve the private interests of [the mother] and her daughter, either to aid the defense of the criminal charge against the daughter, or perhaps to assist in the prosecution of a civil damage suit against the [officer] as well as other officers involved in the arrests." *Id.* at 449-50.

B.

The Privacy Protection Act of 1976 interpreted in *Hinderliter* has been amended on several occasions in the last 50 years. *See* 1987 Acts ch. 506, at 738; 2001 Acts ch. 844, at 1410-13; 2003 Acts chs. 791, 914, 918, 927, at 1098-99, 1328-31, 1345-48, 1408; 2009 Acts chs. 849, 867, at 2795-98, 2835-38; 2018 Acts chs. 597, 679, at 923-25, 1027-30. Renamed the "Government Data Collection and Dissemination Practices Act" in 2001, the current statute retains all of the previous provisions applicable in *Hinderliter* and includes newer provisions that further strengthen the policies articulated by the General Assembly a half century ago.

Code § 2.2-3801 in the Government Data Act defines "[d]ata subject" as "an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system." This definition tracks word for word the definition in the original 1976 enactment that we interpreted in *Hinderliter*. We held in that case that the police officer was a data subject because the internal-investigation

report, contained in an "information system," included "[p]ersonal information" about "his employment record and personal traits." *Hinderliter*, 224 Va. at 447. The same is true here.

The current statute, unlike the 1976 Act, now includes the phrase "including, but not limited to" — a non-exhaustive, enumerative qualifier[4] — that further broadens the interpretative scope of an already expansive list of analogous matters of "[p]ersonal information," *see* 2008 Acts ch. 840, at 1767. That list includes (as it did in 1976) all "things done by or to such individual." Code § 2.2-3801; *see also* 1976 Acts ch. 597, at 741. As applied to Keil's case, the statutory definition of "[p]ersonal information," *inter alia*, "means all information that (i) describes . . . anything about an individual including, but not limited to, . . . [his] employment record, or (ii) affords a basis for inferring . . . things done by or to such individual." Code § 2.2-3801. The capacious scope of this definition of "[p]ersonal information" covers the internal-affairs-investigation records in Keil's case even more securely that the predecessor provision covered the internal-investigation report in *Hinderliter*.

In its opinion in the present case, the Court of Appeals, however, found *Hinderliter* to be distinguishable because the evidence in that case revealed that the internal-investigation report was found "in the officer's 'personnel file'" with his name on it and thus was "'indexed' by name." *Keil*, 81 Va. App. at 714 n.4 (citation omitted). Unlike in *Hinderliter*, the Court of Appeals observed, no such indexing on any file folders was established in Keil's case. While that distinction is factually correct, we do not find it to be legally dispositive.

The definition of "[d]ata subject" in Code § 2.2-3801 includes two verb phrases stated in the disjunctive: "is indexed or may be located." It is possible that these verb phrases could

---

[4] *See generally Tomlin v. Commonwealth*, 302 Va. 356, 369 (2023) ("[The] 'limited by' principle . . . does not apply when the general words in a statute are expressly said to not be limited by the specific words." (emphasis omitted)).

mean exactly the same thing, but we presume otherwise under settled principles of statutory construction. "Under the conjunctive/disjunctive canon, *and* combines items while *or* creates alternatives." Antonin Scalia & Bryan A. Garner, Reading Law: The Interpretation of Legal Texts 116 (2012).[5]

The preamble of the Privacy Protection Act provides context for this disjunctive phrase. It reveals that the Act was passed because of "the increasing use of computers and sophisticated information technology" that "ha[d] greatly magnified the harm that can occur from these practices," including "the extensive collection, maintenance, use and dissemination of personal information." 1976 Acts ch. 597, at 740. The statute was crafted to address the concern that "the computer is taking an ever-increasing role in our society," and "if unchecked," could "cause grave inroads in the privacy of the individual." VALC, *Computer Privacy and Security*, S. Doc. No. 27, at 3-4 (1976).

Under the "term-of-art canon" of statutory construction, when a statute "addresses a 'technical subject' using words 'obviously transplanted from another legal source,'" *Appalachian Power Co. v. State Corp. Comm'n*, 301 Va. 257, 282-83 (2022) (quoting Scalia & Garner, *supra*, at 73), "we must 'explain them by reference to the art or science to which they are appropriate,'" *id.* at 282 (quoting *Corning Glass Works v. Brennan*, 417 U.S. 188, 201 (1974)). It follows that when evaluating the technical meaning of terms of art, pertaining to computers and information science, courts look to specialized lexicons for guidance. *See, e.g.*, *Van Buren v.*

---

[5] *See Campos-Chaves v. Garland*, 602 U.S. 447, 457 (2024) ("The word 'or' is 'almost always disjunctive.'" (citation omitted)); *Patterson v. Commonwealth*, 216 Va. 306, 307 (1975) (per curiam) (noting that the "ordinary meaning" of "or" is "disjunctive"); *South E. Pub. Serv. Corp. v. Commonwealth*, 165 Va. 116, 122 (1935) (reasoning that "or" is interpreted according to "its ordinary, literal and disjunctive meaning" unless the General Assembly clearly intended for it to be interpreted conjunctively); 1A Shambie Singer, Sutherland's Statutes and Statutory Construction § 21.16, at 113 (8th ed. 2025) ("[T]he word 'or' typically is disjunctive.").

United States, 593 U.S. 374, 388 n.6 (2021) (referencing various specialized dictionaries of computer terms).

In the context of digital information systems, indexing typically employs sub-linear time and tokenized tag searches within computerized retrieval systems and databases. *See generally* Christopher D. Manning, Prabhakar Raghavan, & Hinrich Schütze, Introduction to Information Retrieval 5-6 (2008) (discussing the operations of an inverted index and user queries).[6] Doing so "avoid[s] linearly scanning the texts for each query," *id.* at 3, by operating a "scalar value that allows direct access into a multi-element data structure such as an array without the need for a sequential search through the collection of elements," Microsoft Computer Dictionary 269 (5th ed. 2002).[7]

In the context of non-digital records, an "index" describes a listing of key search words for finding information in a larger corpus of records. *See* Black's Law Dictionary 918 (12th ed. 2024); *see also* Joan M. Reitz, Online Dictionary for Library and Information Science, https://odlis.abc-clio.com/odlis_i.html (last visited Feb. 4, 2026) (defining an index as "[a]n alphabetically arranged list of headings consisting of the personal names, places, and subjects treated in a written work, with page numbers to refer the reader to the point in the text at which information pertaining to the heading is found").

---

[6] *See generally* Microsoft Computer Dictionary 511 (5th ed. 2002) (defining a tag as "a key or an address that identifies a record and its storage location in another file"); *id.* at 522 (defining a token as "[a] unique structured data object or message that circulates continuously among the nodes of a token ring and describes the current state of the network"); *id.* at 464 (defining scalar as "[a] factor, coefficient, or variable consisting of a single value (as opposed to a record, an array, or some other complex data structure)").

[7] *See also* A Dictionary of Computer Science 266 (Andrew Butterfield & Gerard Ekembe Ngondi Abraha eds., 7th ed. 2016); Charles J. Sippl & Roger J. Sippl, Computer Dictionary 235 (3d ed. 1980); Microsoft Encarta College Dictionary 732 (2001).

These digital and non-digital definitions of "indexed" serve as contrasts to the disjunctive verb phrase — "may be located" — used in the definition of "[d]ata subject" in Code § 2.2-3801. The phrase "may be located" implies no custom search methodology or specialized search terms. Its plain meaning is simple: Look in this file cabinet, in that drawer, in those folders, or wherever — so long as it is reasonable to believe that looking in those places "may" (not "will") locate any requested personal information identified "under" the name, number, or "other identifiable particulars" of the data subject. Code § 2.2-3801. If a record can reasonably be found using this information, it should be found.[8] It is no excuse to say that the individual's name, number, or other identifiable particular is not printed on a file folder label, sticky note, bookmark, index card, or color-coded tag.[9]

The practical point of placing this broad "may be located" provision as an alternative to relying exclusively on the employer's organized systems of indexed documents is illustrated by the facts of Keil's case. The Sheriff testified that "many years ago" he decided not to continue placing internal-affairs records in the "personnel file" for the officer being investigated. R. at 469-70. "[N]o eyes can see" internal-affairs records, he testified, "except for me and the undersheriff and the investigator that did it." *Id.* at 469. Keeping these records out of an

---

[8] We acknowledge the reliance the Court of Appeals placed on *Neal v. Fairfax County Police Department*, 295 Va. 334 (2018) (*Neal I*), and *Neal v. Fairfax Cnty. Police Dep't*, 299 Va. 253 (2020) (*Neal II*). We agree that both cases support the view that "'[i]dentifiable particulars' are unique identifying details about the person who is the subject of the data." *Keil*, 81 Va. App. at 714. The issue in Keil's case, however, is not the definitional scope of "[i]dentifiable particulars" but rather the scope of the "may be located" search required by Code § 2.2-3801.

[9] Under the Federal Privacy Act, the Court of Appeals observed, "it is not enough that an agency has a record with identifying information about an individual; that record must exist within a 'system of records' *indexed* according to unique personal characteristics." *Keil*, 81 Va. App. at 718 (emphasis added). The words "index" or "indexed," however, are not used in the Federal Privacy Act, 5 U.S.C. § 552a. Code § 2.2-3801 of the Government Data Act, however, mentions "indexed" personal information and immediately thereafter decouples it from the same information that "may be located" without an indexing system.

individual's personnel file, the Sheriff explained, made sure that any adverse finding "doesn't hurt that person further in [his] career." *Id.* at 470. When asked "why" internal-affairs records are "kept at all," the Sheriff said that they would be helpful in the event "a lawsuit pops up." *Id.*; *see also id.* at 472.[10]

The Government Data Act's expansive "may be located" provision cannot be so easily sidelined. In both Keil's case and *Hinderliter*, the investigatory records were physically located in a file cabinet or drawer or maybe lying on the Sheriff's desk. Neither case involved a digital information system executing computational operations on structured, machine-readable data. There was no need for some sophisticated indexing function to pore through searchable databases. Locating the internal-investigation records in *Hinderliter* involved looking into the officer's personnel file. *See* 224 Va. at 447. Locating the internal-affairs records in Keil's case simply involves finding the "secret" internal-affairs files, R. at 450-51, 467-69, and looking for the records mentioning Keil's name, personal number, or other identifiable particulars. The text of Code § 2.2-3801 covers both scenarios.

III.

In sum, we affirm the judgment of the Court of Appeals dismissing Keil's VFOIA claims and reverse the judgment of the Court of Appeals upholding the circuit court's dismissal of Keil's claims under the Government Data Act. We remand this case to the Court of Appeals for further remand to the circuit court to review in camera the records withheld by the CSO to determine if anything in those records contains "personal information" subject to Keil's "[r]ights

[10] During his testimony, the Sheriff volunteered that he knew of "potential litigation" against Keil arising out of the investigated incident. *See* R. at 473. The Sheriff's "position" nonetheless remained steadfast — he "could share the information" in the internal-affairs-investigation records "with Matt Keil that is about him relating to a potential lawsuit but [he did not] have to." *Id.*

of data subjects" under Code § 2.2-3806.[11] Matters within those records that do not directly or indirectly contain "personal information," Code § 2.2-3801, about Keil should be redacted by the circuit court prior to review or access by Keil. With respect to any ancillary matters necessary to bring this case to closure, the circuit court retains authority to adjudicate them.

Affirmed in part,
reversed in part,
and remanded.

[11] In addition to the internal-affairs documents, Keil requested "body camera footage," "audio or video recordings," and "photographs" from the inmate incident. *Id.* at 271. The appellate record indicates that the internal-affairs material may contain "videotape[s]" as well as the reports and notes concerning the incident at the jail. *Id.* at 482, 487, 530, 532-33. The Government Data Act applies to the videos and images as well as the documents to the extent that they meet the definition of "[p]ersonal information." Code § 2.2-3801 (defining "all information that . . . affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual" as "[p]ersonal information"); *see also Neal I*, 295 Va. at 350 (holding that pictures can qualify as "personal information").