ALEX ROSETTI, Plaintiff-Respondent, v. RAMAPO-INDIAN HILLS REGIONAL HIGH SCHOOL, BOARD OF EDUCTION, Defendants-Appellants.	SUPREME COURT OF NEW JERSEY DOCKET NO.: 090375 Civil Action On Petition for Certification from a Final Judgment of the Appellate Division, Docket No. A-1466-23 Sat Below: Hon. Thomas W. Sumners, P.J.A.D. Hon. Ronald Susswein, J.A.C. Hon. Stanley L. Bergman, Jr. (t/a)

BRIEF OF AMICUS CURIAE MATTHEW J. PLATKIN, ATTORNEY GENERAL OF THE STATE OF NEW JERSEY

Jeremy M. Feigenbaum
Solicitor General

Benjamin M. Shultz
Christopher Weber
Raymond R. Chance, III
Assistant Attorneys General
Of Counsel

Sara M. Gregory (027252010)
Assistant Attorney General
Of Counsel and On the Brief

Ivonnely Colon-Fung (033642008)
Deputy Attorney General
On the Brief

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY
Richard J. Hughes Justice Complex
25 Market Street
P.O. Box 112
Trenton, New Jersey 08625
(609) 696-4262
ivonnely.colon-fung@law.njoag.gov
Attorney for Amicus Curiae

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

PRELIMINARY STATEMENT

This appeal addresses a recurring issue under New Jersey's Open Public Records Act (OPRA), N.J.S.A. 47:1A-1 to -13: whether a public agency must retrieve or generate email logs from personal, non-government accounts hosted on third-party servers, if the accounts are used for official business on at least one occasion. To be clear, all—including the Attorney General—agree that government emails on such servers are "government records" subject to OPRA just as if they were on the government's servers. But the Appellate Division's decision goes further, requiring agencies to take the unprecedented step of generating email logs too, even where the accounts are outside the agency's custody or technical control, and even where the requests fail to identify any discrete or limited subject matter for the emails the requestor is seeking. This is at odds with OPRA's text, threatens significant intrusions on public employees' privacy interests, and interferes with the ability of officials to respond to OPRA requests and perform other duties. This Court should reverse.

As an initial matter, the Appellate Division erred in finding that the email logs at issue here were "government records." When Plaintiff submitted his request in 2023, OPRA defined a "government record" to include any "paper," "document," or "information stored or maintained electronically," that was "made, maintained or kept on file in the course of his or its official business by"

a government official or agency. See N.J.S.A. 47:1A-1.1 (2022). Context, logic, and consideration of underlying privacy interests all make clear that when something is a government record solely because it is "electronic information stored or maintained electronically," the storage or maintenance must be done by the government itself. So, when an email system is private, the information contained in the corresponding email logs (that is, the metadata in email header fields like "sender," "date," and "recipient") is not information that is "stored or maintained electronically" within OPRA's meaning, and that information is not a "government record." Otherwise, agencies would face the technically difficult task of combing through unfamiliar private email servers, like Gmail, Yahoo, or other personal accounts, to obtain the metadata contemplated by the Appellate Division's opinion. And they would have to do so in a way that threatens privacy interests that did not apply to government servers and that this Court did not have to confront in Paff v. Galloway, 229 N.J. 340 (2017).

In any event, even if the email logs constitute "government records" under the version of OPRA then in effect, the Court should still clarify that the OPRA request was overbroad. Plaintiff sought email logs for all accounts used by every current and former Board member over a multi-month period, without identifying a discrete or limited subject matter, and without limiting the request

to systems maintained by the Board. That sweeping request runs headlong into the longstanding principle that requestors must specify the records sought with "reasonable clarity" by identifying a discrete subject matter. Burke v. Brandes, 429 N.J. Super. 169, 174 (App. Div. 2012). That, too, requires reversal.

To be clear, the Attorney General does not suggest that emails sent or received in the official course of business are themselves outside OPRA's reach just because they reside on private servers. "[D]ocuments" that are "made" by a public employee in their official course of business—even if the electronic version of that document is stored or maintained by a third party—are well within OPRA's reach. See Burnett v. Cnty. of Gloucester, 415 N.J. Super. 506, 517 (App. Div. 2010). But as explained below, under the pre-2024 version of OPRA, an agency is not obligated to retrieve or generate underlying metadata from personal accounts beyond that agency's custody or control, and certainly not where the request lacks a discrete subject matter. (And going forward, due to the Legislature's 2024 amendments to OPRA, requests for metadata will be governed by a materially different version of the statute than this Court confronted in Paff v. Galloway.) Because this metadata is on a private server, and given the breadth of this request, the court below should not have compelled the production of these logs.

PROCEDURAL HISTORY AND STATEMENT OF FACTS[1]

The Attorney General relies on and incorporates the statement of facts in the Appellate Division's opinion, Rosetti v. Ramapo-Indian Hills Regional Board of Education, 481 N.J. Super. 1 (App. Div. 2025), adding the following:

In January 2023, Plaintiff–Respondent Alex Rosetti submitted an OPRA request to the Ramapo–Indian Hills Regional Board of Education ("the Board") and its Business Administrator/Records Custodian, Thomas Lambe. Id. at 5. In relevant part, the request sought:

> Email logs of all past and current Board members for all email accounts in which they have conducted or discussed Board of Education matters or business during the time frame of November 1, 2022 through to the date of the response. The email log should contain the sender, recipient, those copied ("cc") or blind copied ("bcc"), the date, time, subject and identify the existence and name of any attachment.
>
> [Ibid.[2]]

[1] These sections are combined for the Court's convenience.

[2] The request also sought "[a]ll comments submitted by the public comments form received by the Board from August 1, 2022 through to the date [for] the response . . . [including] the name, email, town and the question or comment of the sender." Ibid. This request was resolved between the parties through the proceedings below and is not at issue in this appeal.

After the Board did not respond within OPRA's statutory timeframe, Plaintiff filed a verified complaint and order to show cause in Superior Court on March 14, 2023. Ibid.; see also (Pa1-4).[3] Through counsel, the parties resolved the request to the extent it pertained to email logs from the Board's municipal-issued email addresses, with the Board producing the redacted email logs from the relevant government–issued accounts (i.e., @rih.org addresses). (Dca22-374). After those logs showed communications between Board members' government-issued accounts and their personal email addresses, as well as instances where members forwarded Board business to themselves at personal accounts, ibid., the parties agreed to preserve for judicial determination a single, discrete issue: whether OPRA required the custodian to obtain or generate email logs from Board members' private, non-government accounts used for public business. Rosetti, 481 N.J. Super. at 5-6.

Before the trial court, the Board did not dispute that the Board members' private email addresses had been used for public business. Ibid. Instead, it relied heavily on a certification filed by the Board's Director of Technology,

[3] "Dcb" refers to Defendants' petition for certification; "Dca" refers to the appendix to their petition. "Db" refers to Defendants' Appellate Division brief; "Da" refers to the appendix to that brief. "Pb" refers to Plaintiff's Appellate Division brief, and "Pa" refers to the appendix to that brief. "Pcb" refers to Plaintiff's brief in opposition to the petition for certification.

John Chang. Id. at 6. Chang certified that while he could readily and accurately generate logs from the school district's Google Workspace accounts, doing so for personal email services—ranging from Gmail and Yahoo to encrypted providers such as ProtonMail—was "difficult if not impossible" in many cases. (Pa17). Chang further certified that most personal email users lack administrative privileges to generate logs in the requested format, that capabilities vary widely among providers, and that even with usernames and passwords, the Board could not ensure the integrity of any data retrieved from private servers. (Pa17-18). Chang emphasized the stark difference between extracting data from the district's controlled environment and attempting to access privately-maintained systems over which the district had no legal authority or control. (Pa18).

The trial court agreed with the Board, holding that OPRA does not compel a custodian to obtain email logs from personal, non-government accounts, and that nothing in Paff v. Galloway extended its rationale to third-party email platforms outside agency control. Rosetti, 481 N.J. Super. at 6-7. The trial court also found that producing the requested logs would require Defendants to "manually compile and collate information to create a log" for accounts beyond

their custody or control—an "arduous task" the court deemed unauthorized by OPRA. Ibid.

Plaintiff appealed. On January 27, 2025, in a published decision, the Appellate Division reversed the trial court's decision. Id. at 4. The decision found that the email logs "are government records under OPRA because they relate to Board business even though they are on Board members' private servers and not maintained nor controlled by the Board." Id. at 11. In support of this conclusion, the Appellate Division cited Paff v. Galloway for the proposition that an email log is "'electronically stored information extracted from an email,' 'not the creation of a new record or new information.'" Id. at 12. It also cited Simmons v. Mercado, 247 N.J. 24 (2021), as support for the conclusion that "even though the email logs are not kept on Board servers, they are nonetheless government records because they reference Board business," Rosetti, 481 N.J. Super. at 12, as well as its decision in Association for Governmental Responsibility, Ethics, and Transparency (AGREAT) v. Borough of Mantoloking, 478 N.J. Super. 470 (App. Div. 2024), cert. granted, 260 N.J. 597 (2025), which held that "'OPRA's broad reach can include emails concerning government business, sent to or from personal accounts of government

officials—if the emails fall within the definition of government records[,]'" Rosetti, 481 N.J. Super. at 11.

The Appellate Division also rejected the trial court's finding that the Board had established that the production would be unduly burdensome, and ultimately concluded a remand was necessary so the Board could substantiate its claims that there are unfeasible burdens to produce the logs and to allow Plaintiff an opportunity to respond. Id. at 14-15. The panel remanded with instructions for each Board member to search their personal accounts, submit Paff[4]-style certifications detailing the search, and—if necessary—participate in a fact-finding process to determine whether production would impose an undue burden. Id. at 16.

On June 16, 2025, this Court granted the Board's petition for certification.

ARGUMENT

POINT I

THE REQUESTED EMAIL LOGS ARE NOT "GOVERNMENT RECORDS" UNDER OPRA.

OPRA's reach only extends to "government record[s]." N.J.S.A. 47:1A-5(g). Thus, if the specific email logs at issue do not meet OPRA's definition of

[4] Paff v. N.J. Dep't of Labor, 392 N.J. Super. 334, 341 (App. Div. 2007). In all other instances in this brief, Paff refers to Paff v. Galloway.

a "government record," the records custodian was not required to produce them in response to Plaintiff's OPRA request. That principle resolves this case: Under the version of OPRA in effect at the time Plaintiff submitted his request, the email header information at issue did not meet the definition of "government record," as it was not stored or maintained by any government entity operating in his or its official capacity. That said, this Court should take care in its opinion to warn lower courts that their decisions may be different when they confront similar requests for email logs after 2024, because intervening amendments by the Legislature have excluded essentially all email header information (whether maintained on private or public email servers) from OPRA's definition.

A. Email Header Information Residing On Private Email Servers Does Not Fall Within OPRA's Definition Of "Government Record."

The term "government record" under OPRA is statutorily-defined. Both at the time of Plaintiff's January 2023 request—and continuing after the 2024 amendments—OPRA defined a "government record" as:

> any paper, written or printed book, document, drawing, map, plan, photograph, microfilm, data processed or image processed document, information stored or maintained electronically or by sound-recording or in a similar device, or any copy thereof, that has been made, maintained or kept on file in the course of his or its official business by any officer, commission, agency or authority of the State or of any political subdivision

> thereof, including subordinate boards thereof, or that has been received in the course of his or its official business by any such officer, commission, agency, or authority of the State or of any political subdivision thereof, including subordinate boards thereof.
>
> [N.J.S.A. 47:1A-1.1 (2022) (emphasis added).]

As this provision's plain text establishes, OPRA distinguishes between treatment of "paper[s], written or printed book[s], document[s], drawing[s], map[s], plan[s], photograph[s], microfilm[s], [and] data processed or image processed document[s]," on the one hand, and "information stored or maintained electronically or by sound-recording or in a similar device," on the other. N.J.S.A. 47:1A-1.1 (2022). The former (i.e., books, documents, etc.) appear without any immediate reference to how they are stored or maintained, but the last item, "information," is qualified: its mechanism of storage or maintenance matters, because information can only constitute a "government record" if it is "stored or maintained electronically or by sound-recording or in a similar device." Ibid.

To determine when information is "stored or maintained electronically or by sound-recording or in a similar device," this Court should look to statutory context. See, e.g., C.R. v. M.T., 257 N.J. 126, 139 (2024) (explaining that statutory interpretation proceeds by reading terms "in context with related

provisions so as to give sense to the legislation as a whole") (internal quotation marks omitted); State v. Carter, 247 N.J. 488, 513 (2021) (explaining that this Court does not review words "in isolation," and instead carefully accounts for broader context). In a statute defining the term "government records," the individual or entity doing the maintaining or storing of the information necessarily must be the government, rather than some private person or entity.

Indeed, that contextual point explains how to read OPRA's later reference to things that have been "made, maintained or kept on file in the course of [a government official or entity's] official business." N.J.S.A. 47:1A-1.1 (2022). For listed items that do not depend on how they are stored and maintained (such as documents and papers), that phrase is sensibly read so that those items can be government records if they meet any of three listed conditions: being "made," "maintained," or "kept on file" by someone from the government acting in an official capacity. But for "information," whose very inclusion on the list does depend on how it is "stored or maintained," ibid., it would be odd to think the Legislature would treat that information as a "government record" solely because the government was that information's original source. The much more sensible interpretation is that for this category, only the "maintained" and "kept on file" parts of the statute are relevant. And so electronically-stored

information can only qualify as a government record if it is "maintained or kept on file" in the course of a government entity's official duties.

Any contrary interpretation would lead to bizarre results. The Appellate Division appeared to believe that so long as information is "made" by someone performing official government business, it would become a government record if later stored anywhere in an electronic medium. See Rosetti, 481 N.J. Super. at 10-11. But if that were true, a citizen's personal recording of a public official's speech, or portions of a purely private email chain quoting a government official, would have to be "government records" as well since they contain "information" originally "made" by someone officially performing government business. That surely cannot be what the Legislature intended. The more sensible reading is that when it comes to pure information maintained electronically, status as a government record turns on whether the government is the one maintaining it in an electronic medium.

Applying that understanding leads to the straightforward conclusion that an email log of emails on private servers is not a government record. As this Court found in Paff v. Galloway, email logs are compilations of certain "fields of information" from individual emails, including the sender, recipient, date, and subject fields commonly used in email programs. 229 N.J. at 354-55.

Irrespective of whether that information was originally "made" by someone performing official government business, if information is stored only on private servers it is not a government record because the information is not "maintained or kept on file" in the course of a government entity's official duties.

This interpretation also avoids a potential state constitutional problem. See DeSimone v. Springpoint Senior Living, Inc., 256 N.J. 172, 187 (2024) (recognizing the Court's "duty to interpret a statute to avoid running afoul of constitutional protections"). Article I, Paragraph 1 of the New Jersey Constitution protects against unwarranted invasions of privacy. See, e.g., Hennessey v. Coastal Eagle Point Oil Co., 129 N.J. 81, 95-96 (1992). Yet if Plaintiff's interpretation were accepted, government agencies would regularly be forced to perform intrusive electronic searches of their employees' personal email accounts to determine whether a given piece of information qualified as a record. Cf. Lipsky v. N.J. Ass'n of Health Plans, Inc., 474 N.J. Super. 447, 473 (App. Div. 2023) (recognizing the "strong privacy interests associated with the contents[] of individuals' personal electronic devices, which often include an extraordinary amount of confidential and even privileged information," and overturning a discovery order that required employees in the Department of Health to turn their personal electronic devices over for forensic evaluation in

response to a subpoena). And the logic of Plaintiff's position would not stop there: even private citizens can be in possession of electronic "information" originally made by a government official, and Plaintiff's position implies that those purely personal devices should be searched as well.

This privacy concern is further highlighted by the fact that Plaintiff's email log request was not even facially limited to the individual emails sent or received by Board members in their official course of business. Instead, he sought logs "for all email accounts in which [Board members] have conducted or discussed Board of Education matters or business." Rosetti, 481 N.J. Super. at 5 (emphasis added). This would seem to encompass the many, many purely personal emails that almost certainly exist on Board members' personal email servers, and which would inevitably be implicated by generating a log of those servers. This request is thus akin to asking the Board to "search the entire contents of a house merely because some items in the house might be relevant." Lipsky, 474 N.J. Super. at 473 (quoting Carlson v. Jerousek, 68 N.E3d 520, 537 (Ill. Ct. App. 2016)).

Furthermore, since its inception, OPRA itself has expressed concern with protecting individual privacy, warning in its opening section that "a public agency has a responsibility and an obligation to safeguard from public access a

citizen's personal information with which it has been entrusted when disclosure thereof would violate the citizen's reasonable expectation of privacy."[5] N.J.S.A. 47:1A-1. As this Court recognized over a decade ago, OPRA's "Section 1 is neither a preface nor a preamble." Burnett v. Cnty. of Bergen, 198 N.J. 408, 422 (2009). Rather, it imposes a substantive obligation on agencies to ensure that when maximizing transparency, they are not simultaneously disclosing personal information that "run[s] contrary to reasonable privacy interests." Id. at 423. That provides yet more indication that the term "government records" in OPRA does not have the definition Plaintiff ascribes.

It is no answer to these privacy concerns to suggest, as the Appellate Division apparently did, that the email logs should only contain information from individual emails that qualify as "government records." See Rosetti, 481 N.J. Super. at 12 ("Based on the record before us, we hold the email logs of the Board members' private servers sought by Plaintiff are subject to OPRA because the emails discuss Board business and were made by the Board members."). That does not explain how private emails should be redacted or removed from

[5] The 2024 amendments signaled an increased attention to privacy concerns, including by, inter alia, adding a comprehensive definition of "personal identifying information." See N.J.S.A. 47:1A-1.1.

those logs—nor by whom.[6] And, even putting aside public release, permitting anyone other than the employee at issue to examine the contents of a personal account is itself a significant invasion of privacy, potentially exposing deeply personal communications wholly unrelated to public business. See Lipsky, 474 N.J. Super. at 473-74 ("Unlike [in this case, other] courts have not mandated that the employees turn over their personal electronic devices for search by a third party (someone other than the employees themselves), nor have they found any requirement that public entities undertake extraordinarily extensive or intrusive searches of their employees' personal accounts and devices.").

Nor does Simmons compel a contrary result. There, the requestor sought access to specific documents called "CDR-1s" that were generated whenever local police officers issued complaint-summonses. Simmons, 247 N.J. at 31. Although the Judiciary's electronic system stored the summonses, this Court observed that the substantive content was created entirely by police officers in the course of their official duties. Id. at 43–44. So the Court found that the

[6] Although the Appellate Division discussed Paff-style certifications submitted by Board members when ordering a remand, it only contemplated that such certifications would be appropriate in the event the email logs were unavailable, or if producing them would be a burden. Rosetti, 481 N.J. Super. at 4. Its decision did not address the separate harm caused by the preliminary disclosure of private emails to a third-party.

entire document—"the actual completed official document," id. at 40,—was a "government record" under OPRA since the document was "made in the course" of the officer's official business. Ibid.; see also ibid. ("Pursuant to OPRA's definition of 'government record,' there is no question that CDR-1s are documents that are made in the course of a law enforcement officer's official business." (emphasis added)). That basic holding is fully consistent with the point above that a "document" (but not "information") can be a government record under OPRA solely because it was "made" by a government official in the course of his official duties. And, to the extent any portions of Simmons suggest the same is true of pure information, those portions are dicta. Indeed, given the nature of the request at issue, Simmons did not confront a situation where the distinction between a "document" and "information" mattered for purposes of something "made" but not "maintained" by a government agency.

Finally, it bears emphasizing that the Attorney General fully agrees that an underlying email itself falls within OPRA's reach if sent or received from a personal email account in the course of official business. As already explained above, a "document" can be considered a government record under OPRA if it was "made" by a government official performing his official business. And a complete email (such as might appear if one simply printed a copy of an email

residing on a computer server) can comfortably fit within the term "document." Accord Paff v. Galloway, 229 N.J. at 353 (describing a "document" as a compilation of "information," and implying that underlying emails count as a "document" under OPRA). So adopting amicus's position does not mean that public officials can escape scrutiny by ferreting public business to private email servers. The point is simply that when the putative record at issue is "information" contained within an email or other digital item, rather than a "document," "paper," or the like, that digital "information" will not qualify as an OPRA record if it is only kept and maintained on a private server.

B. In Crafting Its Opinion In This Case, This Court Should Be Aware That The 2024 Amendments To OPRA Changed The Laws Governing Email Logs.

As explained above, this case can and should be resolved on the ground that the requested email logs are not "government records" under the version of OPRA in effect at the time Plaintiff submitted his request. But even if the Court does not agree on that point, the Court should take care to recognize that the 2024 OPRA amendments have since materially changed the definition of the term "government record" to exclude Paff v. Galloway-style email logs.

Under N.J.S.A. 47:1A-1.1, as amended in 2024, the definition of a "government record" expressly excludes "structured reference data that helps to

sort and identify attributes of the information it describes, referred to as metadata, or any extrapolation or compilation thereof, which shall include the SMTP header properties of emails, except that portion that identifies authorship, identity of editor, and time of change[.]" The import of this amendment follows from its plain text, which excludes both "metadata," and "any extrapolation or compilation thereof[.]" Ibid. This is exactly the information that Plaintiff and others seeking email logs are trying to obtain. See (Pcb6) (describing the core of Paff v. Galloway's holding to be that "metadata . . . is in fact a 'government record' subject to disclosure under" OPRA); Pressler & Verniero, Current N.J. Court Rules, Official Comment on R. 4:10-2(f)(1) (Aug. 1, 2016) (explaining that metadata is "embedded information in electronic documents"); Grenig, Electronic Discovery & Records & Info. Mgmt. Guide § 15:18 (2024) (listing as examples of metadata "information in email files about the email's author, creation date, attachments, and identities of all recipients"); see also Paff v. Galloway, 229 N.J. at 353 (treating the request at issue, which sought email logs, as seeking compilations of "electronically stored information extracted from an email").

Furthermore, to avoid any doubt, the Legislature specifically added that this excluded category "shall include the SMTP header properties of emails."

N.J.S.A. 47:1A-1.1 (emphasis added). "SMTP" is the acronym for the Simple Mail Transfer Protocol, the standard protocol governing the transmission of email messages over the Internet. Natl. Inst. of Standards and Tech., Computer Security Resource Center, Simple Mail Transfer Protocol, csrc.nist.gov/glossary/term/simple_mail_transfer_protocol (last visited Sept. 12, 2025). And under standard internet message formatting, an email "header" is the portion of an email that "contains the vital information about the message including origination date, sender, recipient(s), delivery path, subject, and format information." Natl. Inst. of Standards and Tech., Special Publication 800-45, Version 2, Guidelines on Electronic Mail Security (Feb. 2007), §2.1;[7] see also Internet Engineering Task Force, RFC 5321 – Simple Mail Transfer Protocol (Oct. 2008), § 2.3.1 (explaining that the SMTP protocol has a "header section [that] consists of a collection of header fields . . . structured as in the message format specification . . . RFC 5322");[8] Internet Engineering Task Force, RFC 5322 – Internet Message Format (Oct. 2008), § 3.6 (defining the format of various email header fields, including origination date, sender, to, cc, bcc, and

[7] Available at nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45ver2.pdf (last visited Sept. 12, 2025).

[8] Available at datatracker.ietf.org/doc/html/rfc5321#section-2 (last visited Sept. 12, 2025).

subject). This email header information is therefore unquestionably the kind of information sought in a Paff v. Galloway-type email log. See 229 N.J. at 344 (including "Sender," "Recipient," "Date," and "Subject" as the fields in the email log).

To be clear, Plaintiff's OPRA request predated the 2024 amendments. So the Attorney General does not contend that this new definition of "government record" applies to this case, and the Court need not definitively resolve how that definition applies on these facts. The Court also need not determine here the precise meaning of the new language allowing requestors to seek the portion of metadata "that identifies authorship, identity of editor, and time of change." N.J.S.A. 47:1A-1.1. Amicus simply urges this Court to recognize that, going forward, requests for email logs will require a substantially different analysis than had been the case for requests predating the 2024 amendments.

POINT II

PLAINTIFF'S OPRA REQUEST FAILED TO MEET THRESHOLD REQUIREMENTS BECAUSE IT WAS OVERBROAD.

Entirely distinct from whether the requested email logs are "government records" is a separate but dispositive issue: whether Plaintiff's OPRA request was facially proper to begin with. Although the parties and the panel below did

not address this, the answer to this important question is "no." Because Plaintiff's request failed to limit itself to a discrete and limited subject matter, this failure was sufficient for the Board to deny Plaintiff's request, whether not the request was seeking "government records."

OPRA establishes "a comprehensive framework for access to public records." Mason v. City of Hoboken, 196 N.J. 51, 57 (2008). That framework reflects a careful balance—honed over more than two decades of Legislative amendment, implementation, and construction—between "maximiz[ing] public knowledge about public affairs," Bozzi v. City of Jersey City, 248 N.J. 274, 283 (2021) (quotation omitted), and guarding against disclosures that would be contrary to "the public interest," Mason, 196 N.J. at 65 (quoting N.J.S.A. 47:1A-1). See also Burnett, 198 N.J. at 414 (describing "OPRA's twin aims" as "ready access to government records and protection of a citizen's personal information"). Similarly, OPRA strikes a delicate balance between the needs of requestors and agencies, who are "expected to work together toward [the goal of transparency] by accommodating one another." Mason, 196 N.J. at 78. While the public has a right to request and receive government records, that right comes with whatever limits the Legislature ultimately chooses to provide. Educ. Law Ctr. v. N.J. Dep't of Educ., 198 N.J. 274, 284 (2009).

One important limit, emanating from OPRA's earliest case law, is the requirement that requestors identify records with reasonable clarity by articulating a discrete and limited subject matter. Indeed, in 2005, just a few years after OPRA was passed, the Appellate Division recognized that OPRA forbids "overbroad" requests. MAG Entm't, LLC v. Div. of Alcohol Beverage Control, 375 N.J. Super. 534, 547-50 (App. Div. 2005). After surveying various authorities, the court concluded that "[u]nder OPRA, agencies are required to disclose only 'identifiable' governmental records not otherwise exempt" and that "OPRA does not countenance open-ended searches of an agency's files." Id. at 547-49. The Appellate Division then quickly reaffirmed this rule in Bent v. Twp. of Stafford Police Dep't, 381 N.J. Super. 30 (App. Div. 2005), noting that "OPRA does not authorize unbridled searches of an agency's property." Id. at 37. Subsequent cases are in accord. See, e.g., N.J. Builders Ass'n v. N.J. Council on Affordable Hous., 390 N.J. Super. 166, 178 (App. Div. 2007) (noting that OPRA contemplates short turnaround times for responding to requests, which does not leave custodians time to do things like "speculate about what the requestor seeks," conduct research, or "survey agency employees to determine what they considered or used"); Spectraserv, Inc. v. Middlesex Cnty. Utils. Auth., 416 N.J. Super. 565, 576 (App. Div. 2010) (recognizing that OPRA "does

not countenance [w]holesale requests for general information," and instead requires that a requestor "specifically describe the document sought" (internal quotation marks omitted).

This well-established rule has been synthesized into the principle that a requestor must describe the records sought with "the requisite specificity," with the scope of his inquiry limited to "a discrete and limited subject matter." Burke, 429 N.J. Super. at 177-78. This Court approvingly cited that rule in Simmons, quoting Burke for the proposition that the request had to be restricted to a "discrete and limited subject matter." 247 N.J. at 43. And in Paff v. Galloway itself, this Court specifically recognized that a "records request must be well defined so that the custodian knows precisely what records are sought. The request should not require the records custodian to undertake a subjective analysis to understand the nature of the request." 229 N.J. at 355.[9]

[9] The Legislature likewise recognized this preexisting principle in the 2024 OPRA amendments. L. 2024, c. 16, § 2. Those amendments, in relevant part, explicitly codified the established requirement that requestors identify records they are seeking with particularity, including that the request include "a specific subject matter" and be "confined to a reasonable time period." N.J.S.A. 47:1A-5(g). The Governor's signing statement expressly noted that the OPRA amendments "codif[y] a number of judicial decisions," and specifically mentioned Burke as one such decision. Governor's Statement to S. 2930 3 (June 5, 2024). The signing statement also expressly declared that under the new version of OPRA "the manner by which [OPRA] requests are made and the specificity required for such requests" will be "consistent with current practice." Id. at 4

There are a range of reasons why courts and the Legislature alike have always required requestors to limit themselves to a discrete and limited subject matter. Agencies and municipalities have finite resources, and the time they spend responding to any one OPRA request can come at the expense of the time they spend responding to other OPRA requests or performing other important public duties. Moreover, because public officials must spend time not just figuring out which records are responsive to an OPRA request, but also whether information within them falls into the specific exemptions the Legislature has provided (and hence must be redacted or withheld), overbroad OPRA requests can detrimentally draw resources away from public agencies in multiple stages.

But the OPRA request at issue in this case flatly failed to limit itself to a discrete and limited subject matter, and it should have accordingly been rejected for that independent reason. In pertinent part, the request sought:

> Email logs of all past and current Board members for all email accounts in which they have conducted or discussed Board of Education matters or business during the time frame of November 1, 2022 through to the date of the response. The email log should contain the sender, recipient, those copied ("cc") or blind copied ("bcc"), the date, time, subject and identify the existence and name of any attachment.
>
> [Rosetti, 481 N.J. Super. at 5.]

Plaintiff did not identify any subject matter at all to aid the Board in conducting its search and producing records. Instead, read literally, the request sought email logs for entire email accounts of every single past and present Board member who had ever used his or her personal email account to transact Board business (even just once). That is in no way a limited request. Cf. Lipsky, 474 N.J. Super. at 473 (discussing requests akin to "'search[ing] the entire contents of a house merely because some items in the house might be relevant.'" (quoting Carlson v. Jerousek, 68 N.E3d 520, 537 (Ill. Ct. App. 2016)).

Even interpreting Plaintiff's request as limited to logs of just those emails used to transact public business, the request was still overbroad. If Plaintiff had been requesting only emails conducting Board business from the official Board email accounts for the at-least three-month period at issue, his request would surely still be deemed overbroad. That is not much different than asking for all emails over an extended date range, and is akin to a prohibited "[w]holesale request[] for general information," Spectraserv, 416 N.J. Super. 565, 576. And the fact that Plaintiff was seeking email logs, rather than emails, does not change this conclusion. While generating an email log from an official account could in some circumstances take only a few minutes with the right technology, it "take[s] considerably longer" for a public agency to "determine whether the

requested information in each email may intrude on privacy rights or raise public-safety concerns." Paff v. Galloway, 229 N.J. at 357. Inevitably, that requires not just review of the "fields" generated in the log, but also an examination of the emails themselves to discharge the agency's responsibility to properly assess potential privileges and exemptions under OPRA. After all, whether an email pertains to the existence of non-public investigations; employee grievances; confidential labor relations; student records (particularly in this case); or even information pertaining to victims is not always apparent from one line of an email log.

These problems are compounded when emails reside on private servers. Unsurprisingly, Chang certified that this posed nearly-insurmountable technical challenges when it came to logs of the Board members' personal accounts—as distinct from government accounts. (Pa18). Moreover, even if those technical challenges could be overcome by someone who learns the appropriate skills and immerses themselves in the technical details of the various private email systems, at minimum this will require additional research and learning. And on top of that, the request raised the host of privacy concerns discussed above. Thus, if Plaintiff's request should be considered overbroad when it comes to

official email accounts (and it should), the request is even more clearly overbroad as applied to private email accounts.

It also makes good sense that requestors must identify a specific subject matter when seeking email logs—just as they must do for other OPRA requests. Requiring such precision enables agencies to assess, at the outset, whether a request implicates confidentiality concerns. It also prevents sweeping demands for logs of every message an official may send or receive in a given day—requests that could transform OPRA from a transparency tool into a mechanism for monitoring internal communications. By maintaining OPRA's "specific and discrete" limitation, courts preserve the Legislature's intended balance: ensuring robust public access to records while safeguarding the candid exchange of thoughts, ideas, and deliberations that is essential to effective government, and allowing agencies to devote their limited resources to addressing targeted requests rather than combing through thousands of unrelated emails. In short, a requirement that requestors identify a specific subject matter when requesting email logs is not just consistent with longstanding OPRA case law and OPRA's 2024 amendments, but it also will serve OPRA's underlying goal of maximizing access to specific government records as quickly as possible.

Nor does Paff v. Galloway require any other result. The requestor there sought an email log, for a two-week period, covering emails between two discrete public officials using their official accounts. 229 N.J. at 344. The custodian denied the request, asserting that it would improperly require the town to create a new record. Id. at 344-45. The issue contested in the case, and the Court's actual holding, was that the underlying information was itself a "record" and hence could be obtained under OPRA. Id. at 352-56. While the Court also purported to distinguish MAG and noted that the requestor had "circumscribed his request to a two-week period and identified the discrete information he sought," 229 N.J. at 356, the Court was considering solely the issue of government records and not the separate discrete and limited subject matter inquiry.

Indeed, Paff v. Galloway made abundantly clear that its decision did "not end the inquiry." Id. at 357. Noting that OPRA "carves out thirty exceptions to the definition of government record . . . and lists multiple exemptions to the right to access[,]" the decision cautioned that "[t]his Court is not the proper forum to resolve whether exceptions or exemptions apply to the information requested, and we offer no opinion on the issue." Id. at 358. Thus, if the Township wished "to contest the disclosure of the information on grounds other than those raised

in this appeal, it must present evidence and arguments to the trial court, and Paff must be given the opportunity to respond." Ibid. In this same vein, the Court also recognized that while it might take an IT specialist "two or three minutes" to create the log, it would take the custodian "considerably longer" to determine whether release of the information in the log "may intrude on privacy rights or raise public-safety concerns." Id. at 357. In short, because the record in Paff v. Galloway was not sufficiently fulsome to address any issues outside of the question of whether the log required Galloway Township to create a record, this Court expressly did not do so. Id. at 358.

In any event, Paff v. Galloway's narrowly-confined discussion concerned a request relating to emails for only a two-week period, and for only a single pair of officials. That in no way compels the conclusion that public agencies are obligated to: (1) more broadly search their systems for all emails conducting public business, or (2) extract information from third-party, private systems over which they have no custody or control. Indeed, Paff v. Galloway involved a request for metadata fields stored on a municipality's own servers, and which consisted solely of information that already was "maintained" by the public agency. 229 N.J. at 343. And while the Court held that extracting readily-available discrete fields of data from a system under the municipality's control

did not require creation of a record, id. at 347–49, 353, nothing in Paff v. Galloway requires agencies to intrude into private servers or engineer technical workarounds to collect data that necessarily includes indisputably-personal information.

CONCLUSION

For these reasons, this Court should reverse the Appellate Division's decision. The Court should also clarify that in determining whether a request for email logs seeks "government records," the analysis will differ for requests governed by the 2024 OPRA amendments.

Respectfully submitted,

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY

By: /s/Ivonnely Colon-Fung
Ivonnely Colon-Fung
Deputy Attorney General

Dated: September 16, 2025