SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-3769-20

FRAN BROOKS and
STUART BROOKS,

Plaintiffs-Appellants,

v.

TOWNSHIP OF TABERNACLE
and ELAINE B. KENNEDY, in
her capacity as Municipal Clerk
and Records Custodian of the
TOWNSHIP OF TABERNACLE,

Defendants-Respondents.

———————————————————

Argued July 11, 2022 – Decided March 29, 2023

Before Judges Currier, DeAlmeida and Enright.

On appeal from the Superior Court of New Jersey, Law Division, Burlington County, Docket No. L-0676-21.

Walter M. Luers argued the cause for appellants (Cohn Lifland Pearlman Herrmann & Knopf LLP, attorneys; Walter M. Luers, on the briefs).

William R. Burns argued the cause for respondents (Kalavruzos, Mumola, Hartman, Lento & Duff, LLC,

attorneys; William R. Burns, of counsel; Stephen J. Colianni, on the brief).

The opinion of the court was delivered by

DeALMEIDA, J.A.D.

At issue is whether, in the circumstances presented here, members of the public have an objectively reasonable expectation in the privacy of their names and email addresses sufficient to protect them from disclosure under the Open Public Records Act (OPRA), N.J.S.A. 47:1A-1 to -13. We conclude that when members of the public engage in email communications with municipal elected officials and employees about public business, they cannot objectively reasonably expect that their names and email addresses will not be subject to public disclosure as part of a log of emails sent and received by those officials and employees.

I.

The facts are undisputed. Plaintiff Fran Brooks is a resident of defendant Township of Tabernacle. Defendant Elaine B. Kennedy is the township's municipal clerk and records custodian.

On February 17, 2021, Brooks submitted a written request under OPRA and the common law right of access for a log showing the sender, recipient, date, subject line, persons copied, and persons blind-copied for each email to or from

sixteen township elected officials and employees for the period December 1, 2020 to December 31, 2020. Brooks did not request disclosure of the contents of the emails.

On March 1, 2021, Kennedy provided Brooks with the log she requested in the form of a spreadsheet with thousands of lines of data. Because the information in the log was taken from the township's server, every email listed was sent to, received from, or copied to a township email address. Kennedy redacted all email addresses that did not have a commercial, governmental, or institutional domain name, marking them as "private." The redactions also removed the names associated with the email addresses. At least 855 pieces of data were redacted from the log. Kennedy later conceded that commercial email addresses from domains ordinarily associated with private individuals and the names associated with those email addresses were subject to disclosure.

On March 26, 2021, Brooks filed a complaint in the Law Division. She alleged that Kennedy's redactions from the email log violated both OPRA and the common law right of access.[1]

[1] By analyzing the email log, Brooks determined that the mayor and two members of the township committee had used their private email addresses, which had been redacted, to communicate with township officials or employees about public business. The trial court found that defendants violated OPRA by

On July 16, 2021, the trial court issued an oral opinion upholding defendants' claims that the requested information is protected from disclosure. The court found that Kennedy made a colorable claim that release of the redacted names and email addresses would violate an objectively reasonable expectation of privacy, see N.J.S.A. 47:1A-1, because "the average citizen generally does not understand OPRA or what its parameters might be or that . . . their communications could be caught up in an OPRA request." In addition, the court found the emails at issue "are with public officials but they may involve private citizen concerns where there is no expectation on the part of that citizen about dissemination or warning [of] dissemination of personal data information." The court found that members of the public expect government officials to safeguard private information conveyed to them in their official capacities.

Applying the factors adopted in Burnett v. Cnty. of Bergen, 198 N.J. 408, 427 (2009), the trial court concluded that: (1) the information sought is personal data and (2) contains names and email addresses of members of the public; (3) the potential harm from disclosure is "in subsequent nonconsensual

---

redacting those private email addresses, found Brooks to be a prevailing party, and awarded her attorney's fees. The trial court's decision on this point is not before us, but, as will be illustrated below, is relevant to our analysis of the need for access to the requested information and the public interest in disclosure.

disclosure[;]" (4) communications with municipal officials will be deterred by disclosure; (5) there are no safeguards to prevent further unauthorized disclosure; (6) Brooks did not establish a need for access to the requested information; and (7) public policy militates against disclosure. On balance, the court concluded, the privacy interest in the names and email addresses outweighs any need for disclosure. The trial court did not consider whether Brooks was entitled to disclosure of the names and email addresses under the common law right of access. A July 16, 2021 order memorializes the court's decision.

This appeal followed. Brooks argues the trial court erred when it found an objectively reasonable expectation of privacy in the requested information. In addition, she argues that the public interest in detecting conflicts of interest, improper influence, and violations of OPRA and the Open Public Meetings Act (OPMA), N.J.S.A. 10:4-6 to -21, outweighs any interest in non-disclosure.

After Brooks filed her initial brief, the trial court issued a written amplification of its decision. In the amplification, the court found that release of the requested information would not only disclose the names and email addresses of members of the public, but also "identify a group of citizens and information about their communication with their local government." In other

words, disclosure would reveal not only names and email addresses but also the fact that the people identified by that information communicated with municipal officials and employees about public business. The court found that disclosure posed the danger of undermining public confidence in local government and deterring communication with municipal officials and employees. The court reasoned that although Brooks does not seek the contents of the emails, the specter of release of names and email addresses was sufficient to chill future communications.[2]

II.

We review de novo trial court decisions regarding the applicability of OPRA and whether statutory exclusions from public disclosure of information in government records have been met. O'Shea v. Twp. of W. Milford, 410 N.J. Super. 371, 379 (App. Div. 2009); Asbury Park Press v. Cty. of Monmouth, 406

[2] Pursuant to Rule 2:5-1(d), within thirty days of service of a notice of appeal a trial court may file an amplification of its prior opinion. Here, the trial court, without explanation, filed its amplification almost five months after service of the notice of appeal and, more importantly, forty-four days after Brooks filed her initial brief with this court. We discourage the late filing of amplifications, particularly after a party has filed its merits brief with this court. Brooks did not have the benefit of the trial court's amplification when she drafted her initial brief, an advantage defendants had when they drafted their responding brief. However, because Brooks addressed the amplification in her reply brief, she does not appear to have been unduly harmed by the late amplification.

N.J. Super. 1, 6 (App. Div. 2009). "The purpose of OPRA is to maximize public knowledge about public affairs in order to ensure an informed citizenry and to minimize the evils inherent in a secluded process." O'Shea, 410 N.J. Super. at 379 (quoting Times of Trenton Publ'g Corp. v. Lafayette Yard Community Dev. Corp., 183 N.J. 519, 535 (2005) (internal quotations omitted)). The statute "shall be construed in favor of the public's right of access . . . ." N.J.S.A. 47:1A-1. The records custodian has the burden to show that its denial of access was authorized by law. N.J.S.A. 47:1A-6; Lagerkvist v. Off. of Governor, 443 N.J. Super. 230, 234 (App. Div. 2015).

N.J.S.A. 47:1A-1 provides that "government records shall be readily accessible for inspection, copying, or examination . . . with certain exceptions, for the protection of the public interest . . . ." N.J.S.A. 47:1A-1. A "[g]overnment record" includes

> any . . . information stored or maintained electronically . . . that has been made, maintained or kept on file in the course of . . . official business by any officer . . . of the State or of any political subdivision thereof . . . or that has been received in the course of . . . official business by any such officer . . . .
>
> [N.J.S.A. 47:1A-1.1.]

There is no dispute that the email log requested by Brooks is a government record created with information maintained by officers of the municipality in

the course of official business. See Paff v. Twp. of Galloway, 229 N.J. 340 (2017) (electronic fields of information covering sender, recipient, date, and subject in emails sent by township police chief and township clerk over two-week period constituted government records under OPRA).

Defendants argue, however, that names and email addresses of members of the public that appear on the log are excluded from public disclosure because of privacy concerns. The statute expressly excludes email addresses in public government records from disclosure in three circumstances. "A government record shall not include[:]" (1) "personal identifying information received by the Division of Fish and Wildlife . . . in connection with the issuance of any license authorizing hunting with a firearm" including the "email address . . . of any applicant or licensee . . . [;]" (2) "information received by a member of the Legislature from a constituent . . . including . . . information . . . contained in any e-mail or computer data base . . . [;]" and (3) a "[p]ersonal firearms record," which includes the "email address . . . of any applicant, licensee, registrant or permit holder." N.J.S.A. 47:1A-1.1. These exclusions do not apply here.

In addition, N.J.S.A. 47:1A-5(a) provides that

> [p]rior to allowing access to any government record, the custodian thereof shall redact from that record any information which discloses the social security number, credit card number, unlisted telephone number, or

> driver license number of any person, or . . . the home address, whether a primary or secondary residence, of any active, formerly active, or retired judicial officer, prosecutor, or law enforcement officer, or . . . any immediate family member thereof . . . .[3]

The statute, which was amended several times in the recent past to expand protection of personal information, L. 2020, c. 125 § 1 (excluding home addresses of judicial officers from public disclosure); L. 2021, c. 19, § 18 (excluding records of certain marijuana convictions from public disclosure); L. 2021, c. 37 § 10 (excluding home addresses of immediate family members of judicial officers and others from public disclosure), does not include names and email addresses of people who email municipal officials and employees about public business.

To justify their redactions, defendants rely on a provision of OPRA that concerns personal information more generally. N.J.S.A. 47:1A-1 provides 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 . . . ."

---

[3] The statute permits, in some circumstances, disclosure of social security numbers when they appear in documents required to be made, maintained or kept on file by a public agency. N.J.S.A. 47:1A-5(a).

This provision requires government records custodians, when reviewing a request for disclosure, to apply "a balancing test that weighs both the public's strong interest in disclosure with the need to safeguard from public access personal information that would violate a reasonable expectation of privacy." Burnett, 198 N.J. at 427. The Supreme Court adopted the multi-factor framework set forth in Doe v. Poritz, 142 N.J. 1, 88 (1995), to determine whether the public interest justifies disclosure of personal information in a government record. Those factors are:

> (1) the type of record requested; (2) the information it does or might contain; (3) the potential for harm in any subsequent nonconsensual disclosure; (4) the injury from disclosure to the relationship in which the record was generated; (5) the adequacy of safeguards to prevent unauthorized disclosure; (6) the degree of need for access; and (7) whether there is an express statutory mandate, articulated public policy, or other recognized public interest militating toward access.
>
> [Burnett, 198 N.J. at 427 (quoting Doe, 142 N.J. at 88).]

Three recent Supreme Court opinions apply the Doe factors to requests for government records that public agencies argued contain private information.

Burnett involved a request for disclosure of documents relating to real property, such as mortgages, deeds, construction liens, and releases from judgment that had been filed with a county clerk over a twenty-two-year period.

Id. at 415. The requestor intended to compile the documents in an easily searchable electronic database to which it would sell access. Ibid. The records, which were otherwise "plainly subject to disclosure," id. at 428, contained social security numbers (SSNs), implicating the privacy provision of OPRA. Id. at 416. The custodian sought to redact the SSNs pursuant to N.J.S.A. 47:1A-1, arguing that the parties whose SSNs appeared in the documents had an objectively reasonable expectation they would not be disclosed to the public. Ibid.

With respect to the first two Doe factors, the Court recognized the public interest in the availability of records relating to realty, given that "[t]he very purpose of recording and filing them 'is to place the world on notice of their contents.'" Id. at 429 (quoting Dugan v. Camden Cnty. Clerk's Off., 376 N.J. Super. 271, 279 (App. Div. 2005)). "Potential buyers and creditors rely on the records to establish and protect their ownership interests." Ibid. (citing N.J.S.A. 46:22-1). In addition, the Court noted that SSNs are not required on the documents in question and were likely added by lenders and others who prepared them for filing. Ibid. Thus, the Court observed, it was unlikely that people realized their SSNs were on documents subject to public inspection or would be

included in a computerized database available to be searched by anyone willing to pay for access to their information. Id. at 429-30.

In addition, the Court observed that while SSNs might be available in other public settings, that fact alone was not sufficient to erase the interest in limiting dissemination of that information. Id. at 430. The Court also found an elevated privacy interest because the SSNs appeared on the records along with other personal information, such as names, addresses, marital status, and mortgage details, ibid., and because the requestor intended to compile the information in an easily searchable database. Id. at 430-31.

As for the potential harm from disclosure, the Court found of "particular concern" the "significant risk of identity theft from disclosure of vast numbers of SSNs." Id. at 431. This is so, the Court found, because "SSNs are unique identifiers. They are closely tied to a person's financial affairs and their disclosure presents a great risk of harm." Ibid. "'[A]rmed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on the person's checking account, obtain credit cards, or even obtain that person's paycheck . . . .'" Ibid. (quoting Greidinger v. Davis, 998 F.2d 1344, 1354-55 (4th Cir. 1993) (citations and footnote omitted)).

With respect to factor five, the Court found that there were no safeguards against unlimited disclosure of the SSNs once released. Id. at 434. The Court also noted that the requestor had no demonstrated need for the SSNs and could fulfill its objective without access to the SSNs. Ibid. The Court held,

> [a]s a general rule, we do not consider the purpose behind OPRA requests. See [Michelson v. Wyatt, 379 N.J. Super. 611, 620 (App. Div. 2005)]. An entity seeking records for commercial reasons has the same right to them as anyone else. However, when legitimate privacy concerns exist that require a balancing of interests and consideration of the need for access, it is appropriate to ask whether unredacted disclosure will further the core purposes of OPRA: "'to maximize public knowledge about public affairs in order to ensure an informed citizenry and to minimize the evils inherent in a secluded process.'" [Mason v. City of Hoboken, 196 N.J. 51, 64 (2008) (quoting Asbury Park Press v. Ocean Cnty. Prosecutor's Off., 374 N.J. Super. 312, 329 (Law Div. 2004))]; see also Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 172 [(2004)] (noting that under [the Freedom of Information Act], to give effect to exemptions protecting personal privacy of citizens, "the usual rule that the citizen need not offer a reason for requesting the information must be inapplicable").
>
> [Id. at 435.]

The Court concluded that "[n]either of OPRA's goals is furthered by disclosing SSNs that belong to private citizens to commercial compilers of computer databases. Were a similar request made by an investigative reporter or public

interest group examining land recording practices of local government, this factor would weigh differently in the balancing test." Ibid.

Finally, the Court noted that the Legislature had "expressed increasingly strong concerns against disclosure of SSNs in recent years" through the enactment of statutes prohibiting the inclusion of SSNs on documents filed with a county recording authority. Id. at 435-36. The Court held that

> [o]n balancing the above factors, we find that the twin aims of public access and protection of personal information weigh in favor of redacting SSNs from the requested records before releasing them. In that way, disclosure would not violate the reasonable expectation of privacy citizens have in their personal information.
>
> [Id. at 437.]

In Brennan v. Bergen Cnty. Prosecutor's Off., 233 N.J. 330, 333 (2018), a county prosecutor's office held a public auction to sell sports memorabilia it had previously seized. All bidders submitted a registration form that included their names, addresses, telephone numbers, and email addresses. Ibid. There were thirty-nine successful bidders. Id. at 334. After a news report raised questions about the authenticity of the items, the prosecutor's office offered the successful bidders refunds. Ibid.

Brennan submitted an OPRA request for the contact information for each winning bidder. Ibid. The prosecutor's office produced receipts issued to the

winning bidders "that did not include the buyers' names or addresses." Ibid. Brennan filed suit in the Law Division, alleging a violation of OPRA.

After applying the Doe factors, the trial court ordered release of the unredacted records. Ibid. The court found the privacy interest "limited" because the buyers' names and addresses were already publicly available from various sources. Ibid. The court also concluded that the risk of harm from disclosure was "relatively miniscule." Ibid. We reversed. We also applied the Doe factors, but concluded that the privacy interest was significant because the release of the buyers' names and addresses would reveal that they are collectors of valuable memorabilia, which might make them targets for theft. Ibid. In addition, we reasoned that the interest in government accountability was not served by disclosure because the buyers "were not responsible for any government actions in connection with the auction." Id. at 336. We, therefore, found that Brennan was not entitled to the release of unredacted versions of the records. Ibid.

The Supreme Court reversed. The Court emphasizes that Burnett does not "require[] courts to analyze the Doe factors every time a party asserts that a privacy interest exists." Id. at 341. As the Court explained,

> [i]n Asbury Park Press v. County of Monmouth, for example, the Court ordered disclosure of a settlement agreement between the County of Monmouth and an employee. 201 N.J. 5, 6 (2010). The employee had

> filed a lawsuit claiming sex discrimination, harassment, retaliation, and a hostile work environment. Id. at 6. The County relied on OPRA's privacy clause to try to prevent disclosure of the agreement. Id. at 6-7.
>
> Noting that the case was "a far cry from Burnett," the Court quickly dispensed with the argument. Ibid. The Court explained that "OPRA's privacy clause has no application here because this case does not implicate the concerns raised in Burnett." Id. at 7. The Court also saw "no reason to analyze the Doe factors" when "a former county employee chose to file a public action – a complaint against the County which was available to the public" – and the matter would have unfolded in open court had the case not settled. Ibid. Disclosure of the settlement, the Court observed, "would not violate any reasonable expectation of privacy." Ibid.
>
> [Ibid.]

The Court clarified its holding in Burnett, as it was interpreted in Asbury Park Press: "before an extended analysis of the Doe factors is required, a custodian must present a colorable claim that public access to the records requested would invade a person's objectively reasonable expectation of privacy." Id. at 342. When the custodian does "not present a colorable privacy claim at the outset . . . there is no need to resort to the Doe factors." Ibid.

Applying that standard, the Court concluded that the custodian at the prosecutor's office did not present a colorable claim of privacy in the names and addresses of the successful bidders. As the Court explained, "[t]he bidders knew

that they were participating in a public auction" and "that they were bidding on seized property forfeited to the government." Ibid. In addition, the Court noted, "[f]orfeiture proceedings and public auctions of forfeited property are not conducted in private." Ibid. Statutes require the filing of a complaint before property can be forfeited and public notice in advance of the auction. Ibid. The Court concluded:

> [a]ll of those circumstances undermine the notion that a bidder could reasonably expect the auction in this case to be cloaked in privacy. Viewed objectively, it was unreasonable for a buyer to expect that the information requested would remain private. If anything, the sale of government property at a public auction is a quintessential public event that calls for transparency. To guard against possible abuses, the public has a right to know what property was sold, at what price, and to whom. OPRA's plain terms call for disclosure of that type of recorded information, including the names and addresses of successful bidders. To hold otherwise would jeopardize OPRA's purpose . . . .
>
> [Id. at 343.]

Recently, in Bozzi v. City of Jersey City, 248 N.J. 274, 278 (2021), the owner of an invisible fence installation business submitted an OPRA request for a copy of Jersey City's dog license records. He noted that the city may "redact information relating the breed of the dog, the purpose of the dog – if it is a service or law enforcement animal – and any phone numbers associated with the

records. He sought only the names and addresses of the dog owners." Ibid. He intended to use the information to solicit customers for his business. Id. at 277.

The city denied the request, asserting that disclosure of the names and addresses of dog license applicants would violate their objectively reasonable expectations of privacy. Id. at 278. In addition, the city noted that disclosure "may jeopardize the security of both dog-owners' and non-dog-owners' property, as well as potentially put the dogs themselves at risk for theft." Ibid.

After the requestor filed suit alleging a violation of OPRA, the city submitted a certification from its Police Chief, expressing "exceptional[] concern[]" about release of the information. Ibid. He certified that

> those residing at addresses known not to have dogs on the premises may be exposed as more vulnerable to robbery or burglary. Further, disclosure may expose the locations of victims who have fled from threats, stalking, and other harm. And finally, knowing an address has a dog may encourage wrongdoers to bring a weapon.
>
> [Ibid.]

A second certification stated there were five reported dog thefts in the city in the year preceding the request. Id. at 279.

The trial court concluded that the information was not excluded from public disclosure. Ibid. We affirmed. Id. at 279-80.

On appeal, the Supreme Court noted that there is no express statutory exemption from public disclosure for names and home addresses appearing in dog license applications. Id. at 284. Thus, the Court observed, the requested information could be protected from disclosure only if it fell within the more general privacy provision of N.J.S.A. 47:1A-1. Id. at 285.

As the Court held, "[i]t is . . . the ownership and licensing of a dog that would have to provide a reasonable expectation of privacy for Jersey City to make . . . a colorable claim. And it is here that Jersey City's claim fails, because we find no reasonable expectation of privacy in owning or licensing a dog." Id. at 286. The Court found that

> [o]wning a dog is, inherently, a public endeavor. Owners – and the dogs themselves – are regularly exposed to the public during daily walks, grooming sessions, and veterinarian visits. Many owners celebrate their animals on social media or bumper stickers, inherently public platforms. Some people put up signs stating that there is a dog at the residence; others frequent certain parks or establishments specifically made for dogs and dog owners. Some owners even enter their dogs into public shows, events, and competitions. Dog owners who continually expose their dogs to the public cannot claim that dog ownership is a private undertaking. Just like the participants in the public auction in Brennan, dog owners are fully aware of the public exposure of their actions.
>
> [Ibid.]

Because it concluded that the Jersey City custodian did not state a colorable claim that public disclosure of the requested information would violate an objectively reasonable expectation of privacy, the Court did not apply the Doe factors to determine if disclosure was permitted. Id. at 287.

We have carefully considered the record in light of these precedents and conclude that the trial court erred when it found that the requested information is protected from public disclosure.

We agree with the trial court that no provision of OPRA expressly excludes from public disclosure the names and email addresses of members of the public who email municipal officials and employees about public business. As detailed above, the Legislature identified three circumstances in which email addresses in government records are categorically excluded from disclosure. None of those circumstances apply here. We think it significant that N.J.S.A. 47:1A-1.1 expressly protects from disclosure information received via email by members of the Legislature, but does not extend that protection to email communications with municipal officials. The Legislature appears to have drawn a deliberate distinction between themselves and municipal officials and employees with respect to information received from the public. Moreover, N.J.S.A. 47:1A-5(a) contains a detailed list of personal information in

government records that must be redacted before disclosure. That list does not include email addresses. Unlike in Burnett, the Legislature has not enacted a statute expanding protection for names and email addresses.[4]

The only provision under which the information requested here arguably may be protected from disclosure is the personal information privacy provision of N.J.S.A. 47:1A-1. At the outset of our analysis, it is essential that we identify the information sought by Brooks. While Brooks, in a minimal sense, seeks only names and email addresses, it is the context in which that information appears in the township's records that is crucial to assessing the asserted privacy interest. By virtue of their appearance in the email log, the names and email addresses convey the fact that the identified persons communicated with a municipal official or employee about public business. When combined with the

[4] The significance of the omission of email addresses from N.J.S.A. 47:1A-5(a) must be considered in light of the 2004 report from the Privacy Study Commission, created by Governor McGreevey in 2002, through Executive Order No. 21. The Commission recommended that for purposes of OPRA, email addresses be treated in the same manner as unlisted telephone numbers, which are protected from disclosure in N.J.S.A. 47:1A-5(a). See Privacy Study Commission, Final Report 12 (2004). The Legislature has not adopted that recommendation. The Supreme Court found legislative inaction with respect to a recommendation of the Commission "strongly cautions against creating a judicial exception" that effectuates the unadopted recommendation. Bozzi, 248 N.J. at 284-85 (citing Brennan, 233 N.J. at 339).

subject line matter entry on the email log, the requested information also identifies the topic about which those people communicated.

We agree with the trial court's finding that the custodian make a colorable claim that disclosure of the requested information would invade the reasonable expectations of privacy of members of the public. Arguably, N.J.S.A. 47:1-1.1 puts the public on notice that information in emails only with members of the Legislature, and not municipal officials and employees, are protected from public disclosure. We agree, however, that it is at least colorable that a member of the public would expect that their name, email address, the fact that they communicated with a municipal official or employee, and the subject matter of that communication would not be readily subject to public disclosure.

We disagree, however, with the trial court's conclusion that an expectation of privacy in these circumstances is objectively reasonable and outweighs what we find to be the significant public interest advanced by disclosure of the requested information. We apply the Doe factors in turn:

(1) As we explained, the information sought is the names and email addresses of members of the public who communicated via email with municipal officials and employees;

(2) The requested information contains names and email addresses, both of which are generally widely publicly disclosed and, in this instance, were readily sent by the involved parties to a municipal official or employee at an address on the municipality's server, to discuss public business. The context in which this information appears in the municipality's records, however, conveys additional information: that a member of the public, who is identified by name and email address, communicated with a municipal official or employee about public business and the subject matter of that communication;

(3) We see little evidence in the record of harm from the disclosure of the requested information. Defendants speculate that the members of the public to whom the names and email addresses belong may be annoyed, harassed, or subject to intrusion, presumably by unsolicited emails or inquiries about their communications with municipal officials and employees. Brooks, however, does not intend to use the names and email addresses for commercial purposes or to contact the members of the public identified in the email log. Her intent is to monitor the activities of municipal officials and employees, to identify who is influencing decision making in her municipality, and to detect conflicts of interest, corruption, and potential violations of OPRA and OPMA. While Brooks would have a conduit to contact those persons whose information is in

the email log, they could easily filter, screen, or block communications from her if they so desire;

(4) We also find no support in the record for the trial court's conclusion that disclosure of the requested information will chill communications with municipal officials and employees. Engaging in discussions with municipal officials and employees about public business is an inherently public activity. It is not reasonable, or in accord with the legislative intent to promote transparency in government through OPRA, for a member of the public, or a municipal official or employee, to believe they have a right to cloak their contacts relating to public business in secrecy. To the extent that disclosure inhibits secret communications between members of the public and municipal officials and employees about public business, the purpose of OPRA will be advanced. Emails with public officials and employees about public business, contrary to defendants' arguments, are not a "closed loop" shielded from public scrutiny;

(5) While there is no practical way to prevent Brooks, once she is in possession of the requested information, from further distributing that information, we also find no support in the record that she intends to do so;

(6) We disagree with the trial court's finding that Brooks made no showing of need for the requested information. As Brooks points out, there is no mechanism in place to review the use of email by municipal officials and employees to discuss public business. Disclosure of the unredacted email log allows Brooks to review the information to identify corruption, conflicts of interest, and those who are influencing decision making in her municipality. The names and emails of those engaging in electronic discussions of public business with municipal officials and employees is necessary for public oversight of this crucial avenue of communication. As the record demonstrates, Brooks's analysis of the email log, even in its redacted form, revealed that the mayor and two members of the governing body were using their personal email addresses to discuss public business with township employees, possibly in violation of record retention policies. The trial court found that defendants' redaction of those email addresses violated OPRA and subjected them to the award of attorney's fees;

(7) Contrary to the trial court's conclusion, we find that the public interest weighs heavily in favor of disclosure. The purpose of OPRA is to facilitate transparency in government. It is readily apparent that the information sought by Brooks furthers that objective by exposing to public scrutiny the

names and emails of members of the public who have contacted municipal officials and employees about public business. Whatever interest members of the public have in preventing the public disclosure of their names, email addresses, and the subject of their communications, is outweighed by their decision to engage in email exchanges with municipal officials and employees about public business. The record contains no evidence that the people whose information is subject to disclosure received assurances from the municipality that their information would remain confidential.

We conclude that in the circumstances presented here, the limited interest in privacy associated with shielding the names and email addresses from public disclosure is outweighed by the public's interest in transparency in the email communications of municipal officials and employees about public business. The trial court erred when it permitted defendants to withhold categorically the names and email addresses with private domain addresses in the email log.

We offer no opinion with respect to whether the contents of the emails, which have not been requested by Brooks, would be protected from disclosure under OPRA or the common law right of access. Nor does our decision preclude the records custodian from applying the Doe factors to determine if the disclosure of the name and email address associated with any particular email is

protected from disclosure pursuant to N.J.S.A. 47:1A-1. See Scheeler v. Off. of the Governor, 448 N.J. Super. 333, 348-49 (App. Div. 2017). As was the case in Scheeler, we do not discount the possibility that an individualized assessment under Doe of a particular email or series of emails might result in a determination that release of the name and email address of a member of the public would violate an objectively reasonable expectation of privacy.

Paragraph 2 of the June 16, 2021 order is reversed. The matter is remanded for further proceedings consistent with this opinion.[5] We do not retain jurisdiction.

[5] Brooks requests that we remand "for an award of attorney's fees and costs for the work performed by counsel for [Brooks] on this appeal, and for the consideration of an award of additional counsel fees for the work performed" in the trial court. Should Brooks wish to seek attorney's fees, she must do so through the filing of a timely motion in this court and/or the trial court on remand.