State of New York
Court of Appeals

OPINION

No. 6
In the Matter of James C. Russell,
Respondent,
v.
Town of Mount Pleasant, New York,
Appellant.

Darius P. Chafizadeh, for appellant.
James C. Russell, for respondent.
New York State Association of Towns, New York State Conference of Mayors & Municipal Officials, New York Coalition for Open Government, Inc., amici curiae.

RIVERA, J.:

The issue on appeal is whether respondent Town of Mount Pleasant (the Town) properly denied a request under the Freedom of Information Law (FOIL) to disclose the individual names and corresponding email addresses of all subscribers to the Town's online

news alert system. We conclude that the Town established that the privacy interests in keeping the information confidential are weighty, and that disclosure of the requested records would serve no public interest. Accordingly, the Town properly denied the FOIL request on the basis that disclosure would constitute an unwarranted invasion of personal privacy. Therefore we reverse the Appellate Division's order.

I.

The Town uses a notification system called "E-news" to send subscribers email alerts regarding news, updates, or announcements relating to the Town. Petitioner James Russell submitted a FOIL request to the Town seeking disclosure of the names and email addresses of all residents of the Town who subscribe to E-news. Petitioner's FOIL request relied on the Appellate Division's decision in *Matter of Livson v Town of Greenburgh*, which held that a neighboring town was required under FOIL to disclose a similar email subscriber list for its electronic news service because the town had failed to "articulate any privacy interest that would be at stake" (*see* 141 AD3d 658, 661 [2d Dept 2016]). Petitioner's request also stated that he would not reproduce, redistribute, or circulate the names or email addresses or use the information contained therein for solicitation, fundraising, or any commercial purpose—the same conditions that the court imposed in *Livson* (*see id.* at 659).[1]

[1] Relatedly, Public Officers Law § 89 (2) (b) (iii) exempts from FOIL disclosure "lists of names and addresses if such lists would be used for solicitation or fund-raising purposes."

The Town initially denied the request on the ground that it did not possess the requested records. Petitioner administratively appealed and the Town Supervisor, serving in his role as Records Access Appeals Officer, replied, expressing discomfort with disclosing the requested records without the consent of the people who signed up to receive emails and stating that he would look into the request and wait for a legal opinion. After the Town failed to render a decision on his administrative appeal, petitioner commenced this CPLR article 78 proceeding seeking to compel disclosure and for an award of litigation costs. The Town responded that the records are exempt from disclosure under FOIL because disclosure would constitute an unwarranted invasion of personal privacy, as the residents' privacy interests outweigh any public interest in releasing the information. In support, the Town submitted an affidavit from the Town Supervisor, which described a "Consent Form" that the Town sent out to E-news subscribers and digitally published. According to the Town Supervisor, 218 of the 220 respondents stated that they did not consent to the disclosure of their email addresses to others. The Town also submitted an affidavit from its cybersecurity manager, who had 11 years of experience managing the Town's information technology needs. He averred that disclosure of the requested records could expose E-news subscribers to "unnecessary cybersecurity risks," including spoofing, by which someone with malicious intent could email them pretending to be the Town and seek to take advantage of them, exposing them to potential identity theft, account hacking, or a computer virus. He also stated that the Town maintains added security measures employed to protect, among other things, email addresses provided to the Town from unauthorized access by third parties, and expressed concern that a member of the public

with access to private email addresses may not take the same level of security precautions. Supreme Court granted the petition, ordered disclosure of the records subject to the same conditions as in *Livson*, and denied petitioner's request for litigation costs. The Town appealed.

The Appellate Division affirmed Supreme Court's order, holding that the Town failed to demonstrate that the privacy interests at stake outweighed the public interest in disclosure (227 AD3d 1083, 1083-1084 [2d Dept 2024]). The Court concluded that the Town's asserted cybersecurity risks were "speculative, as the Town failed to show that disclosure . . . under the conditions imposed . . . would make the E-news subscribers or the Town more susceptible to such risks than they ordinarily would be" (*id.* at 1085). We granted the Town leave to appeal (42 NY3d 912 [2025]).

II.

The Town claims that disclosure of the requested records would constitute an unwarranted invasion of personal privacy and is therefore exempt under FOIL. We agree.[2]

[2] On this appeal, petitioner argues, for the first time, that the Town's invocation of FOIL's statutory privacy exemption is unpreserved. We disagree. First, petitioner's FOIL request relied solely on *Livson*, which balanced the private and public interests at stake and concluded that the list of names and email addresses in that case was not exempt under FOIL (141 AD3d at 661). Second, although the Town Supervisor did not expressly rule on petitioner's FOIL request, resulting in a constructive denial, he responded to petitioner's administrative appeal by relaying his concern about the E-news subscribers' privacy interests in their personal information. Thus, under the circumstances of this case, we conclude that the Town adequately preserved its privacy arguments.

A.

The Legislature enacted FOIL to "promote open government and public accountability" (*Matter of Gould v New York City Police Dept.*, 89 NY2d 267, 274 [1996]) and to "encourage public awareness and understanding of and participation in government" (*Matter of Beechwood Restorative Care Ctr. v Signor*, 5 NY3d 435, 440 [2005] [internal quotation marks omitted]). Our FOIL "imposes a broad duty on government to make its records available to the public" (*Gould*, 89 NY2d at 274; *Matter of Data Tree, LLC v Romaine*, 9 NY3d 454, 462 [2007]). All government records are presumptively available for disclosure, unless the requested records fall within one of the enumerated exemptions set forth in Public Officers Law § 87 (2) (*Gould*, 89 NY2d at 274-275; *Matter of Abdur-Rashid v New York City Police Dept.*, 31 NY3d 217, 225 [2018]). We must narrowly construe such FOIL exemptions to ensure maximum public access to government records (*Gould*, 89 NY2d at 275; *Matter of Town of Waterford v New York State Dept. of Envtl. Conservation*, 18 NY3d 652, 657 [2012]).

In a CPLR article 78 proceeding to compel production of records pursuant to FOIL, the government has the burden of establishing the applicability of its asserted exemption (*Gould*, 89 NY2d at 275; *Data Tree*, 9 NY3d at 462-463). Blanket denials are impermissible and government records cannot be withheld if they are disclosable in redacted form (*see* Public Officers Law § 89 [2] [a], [c] [i]; *see also Gould*, 89 NY2d at 275 ["(B)lanket exemptions for particular types of documents are inimical to FOIL's policy of open government"]; *Matter of New York Civ. Liberties Union v Office of Ct. Admin.*, — NY3d —, — , 2025 NY Slip Op 05784, *1 [2025] ["(The agency) is not entitled to a blanket

exemption for all potentially responsive documents based on a sweeping invocation of attorney-client privilege"]; *Matter of Reclaim the Records v New York State Dept. of Health*, — NY3d —, — , 2025 NY Slip Op 03102, *9 [2025] ["(The agency) may only redact portions of records if it shows with particularity and specificity that a FOIL exemption applies"]; *Data Tree*, 9 NY3d at 464 ["(E)ven when a document subject to FOIL contains . . . private, protected information, agencies may be required to prepare a redacted version with the exempt material removed"]).

Among its various exemptions to disclosure, FOIL provides that an "agency may deny access to records or portions thereof that . . . if disclosed would constitute an unwarranted invasion of personal privacy under [Public Officers Law § 89 (2)]" (Public Officers Law § 87 [2] [b]). Public Officers Law § 89 (2) (b), in turn, provides a non-exhaustive list of specific types of exempt information that does not expressly include names and email addresses submitted to obtain governmental correspondence, other than when such information is provided for tax purposes under Real Property Tax Law § 104 (*see* Public Officers Law § 89 [2] [b] [vii]). As the parties recognize, no enumerated type of information applies here. Accordingly, as the Court held in *Matter of New York Times Co. v City of N.Y. Fire Dept.*, when none of the enumerated forms of unwarranted invasions of personal privacy apply, we must "balanc[e] the privacy interests at stake against the public interest in disclosure of the information" (4 NY3d 477, 485 [2005]). The balancing of the interests at issue here lands squarely in favor of the subscribers' privacy interests.

B.

1.

On one side of the scales, the subscribers have a strong privacy interest in keeping their names and email addresses confidential to avoid unwanted and unwelcome communications, and to minimize the risk of cybersecurity threats resulting from disclosure of such information. An email address, and the corresponding holder's name, are commonly treated as personally identifying information (PII). For example, New York's Stop Hacks and Improve Electronic Data Security Act includes email addresses, in combination with a password or security question and answer that would permit access to an online account, as an example of protected information which—if accessed or acquired without valid authorization—triggers notification to the affected persons (General Business Law § 899-aa [1] [b] [ii]; *see also* Rules of Ct of Appeals [22 NYCRR] § 500.5 [d] [providing that "sensitive material," including email addresses, should be "omitted or redacted from public documents" prior to filing with the Court]; 9 NYCRR 540.6 [b] [defining "personal information" as including "e-mail address(es)" for purposes of confidentiality regarding electronic signatures]; Administrative Code of City of NY § 23-1201 [New York City's Identifying Information Law, protecting "identifying information" including "email address(es)"]). Similarly, federal law enforcement considers a personal email address and corresponding name to be PII (*see e.g.* FBI, *How We Can Help You: Identity Theft Resources* [Sept. 5, 2025], available at https://www.fbi.gov/how-we-can-help-you/victim-services/seeking-victim-information/identity-theft-victim-resources [last accessed Jan. 28, 2026]).

Generally, individuals share their email address with people they know, or in exchange for a particular benefit or information that they consent to receive. They assume and rely on a common understanding that those with whom they share their email address will maintain that information private from third parties and the public at large, unless otherwise agreed or implied. The fact that public and private repositories of names and corresponding email addresses customarily publish privacy policies or other notices regarding how they may use that information, including any potential disclosure as required by law or for governmental purposes, confirms that individuals assume their email addresses will be kept confidential by the government unless disclosure is legally mandated or consented to.

The subscribers' privacy concerns also reflect the ubiquitous use of email as a means of communicating highly sensitive private information. One's email account generally contains a large amount of personal data. For example, medical records, job applications, consumer purchase histories, tax returns, and credit card, bank account, and social security numbers are often embedded in emails, or in documents attached to emails. In addition, people often use their email addresses as a username or user ID to log in to many different websites or access online services (*see* Microsoft Support, *What to do if your email address is leaked*, available at https://support.microsoft.com/en-us/topic/what-to-do-if-your-email-address-is-leaked-e85361c2-024d-43f6-93f6-aea41cf48073 [last accessed Jan. 28, 2026]). Moreover, email permits a sender to intrude upon the recipient with correspondence that may be unwelcome or intended to facilitate cyberattacks. Unsurprisingly, the Town Supervisor's affidavit confirmed that this common understanding of the private nature of

email addresses was held by the vast majority of the Town's survey respondents, who indicated that they did not want their email addresses disclosed to petitioner or the public.

Contrary to the Appellate Division's conclusion, the Town's assertions regarding the potential risks to E-news subscribers whose names and email addresses are disclosed were not speculative. The pervasive use of email in our society—and the potential for identity theft and account hacking—makes email addresses highly sought after for nefarious purposes (*see e.g.* New York State Attorney General, *Phishing Information*, available at https://ag.ny.gov/resources/individuals/consumer-issues/technology/phishing-information [last accessed Jan. 28, 2026]). When a person's email address is made available on the Internet or in the public domain, someone with malicious intent can send an email to that person pretending to be either someone they trust or a sender from whom they expect to receive communication—such as their bank, employer, or insurance provider—and then take advantage of them to acquire otherwise private information (*see id.*; FBI, *How We Can Help You: Spoofing and Phishing*, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing [last accessed Jan. 15, 2026]). The Town's cybersecurity manager specifically expressed concern that disclosure of the email list to petitioner could expose subscribers to an increased risk of spoofing, which in turn can lead to account hacking, identity theft, and computer viruses (*see* New York State Attorney General, *Phishing Information*, available at https://ag.ny.gov/resources/individuals/consumer-issues/technology/phishing-information [last accessed Jan. 28, 2026]; FBI, *How We Can Help You: Spoofing and*

Phishing, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing [last accessed Jan. 28, 2026]).

Due to these risks, the government and other large institutions often employ various cybersecurity measures that most people may not have access to or cannot afford, in order to protect against the misuse of email addresses. Without the protection of this heightened security, a person whose email address is disclosed may face an enhanced risk from cyber threats.

Lastly, we note that the federal judiciary shares our view that disclosure of email addresses implicates weighty privacy interests. "Given that our [FOIL] statute was modeled after [the federal Freedom of Information Act (FOIA)], we have repeatedly looked to federal precedent when interpreting FOIL" (*Abdur-Rashid*, 31 NY3d at 231; *see Matter of Lesher v Hynes*, 19 NY3d 57, 64 [2012], citing *Matter of Fink v Lefkowitz*, 47 NY2d 567, 572 n [1979]). Public Officers Law § 89 (2) (b)'s privacy exemption "was modeled" after "the analogous [federal] provision," set forth in FOIA Exemption 6 (*see Matter of Hanig v State of N.Y. Dept. of Motor Vehs.*, 79 NY2d 106, 111 [1992], citing 5 USC § 552 [b] [6]).[3] Thus, the federal district courts' treatment of email addresses as personal information that implicates a cognizable privacy interest under FOIA Exemption 6, provides further support for our conclusion (*see e.g. New York Times Co. v Fed. Communications Commn.*, 457 F Supp 3d 266, 273 [SD NY 2020] [interpreting FOIA

[3] Under FOIA Exemption 6, the federal government is not required to disclose "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" (5 USC § 552 [b] [6]).

Exemption 6 to cover "a person's date of birth, place of birth, social security number, blood type, place of residence, names of family members(,) . . . religious affiliation(,) . . . (and) email address( )"]; *Hall & Assoc. v U.S. Envtl. Protection Agency*, 2020 WL 4673411, *5 [DDC Aug. 12, 2020] ["Courts in this District have routinely held that release of privately held email addresses would implicate a privacy interest (for purposes of FOIA Exemption 6)"]).

2.

On the other side of the scales, there is no public interest served by disclosure here. Petitioner argues only that disclosure will increase public engagement on issues of community concern. This argument is unpersuasive for several reasons. First, it is more likely that disclosure will have either no or a negative effect on public engagement, as people across the State would be hesitant to sign up for their municipality's email alerts due to privacy and security concerns if they knew their email address might be disclosed to third parties upon request and without their consent. Second, the Town's E-news service provides only one-way communications, and its existing subscribers may have no interest in political discourse. Indeed, those who do not want to be contacted by petitioner or anyone other than the Town likely will unsubscribe from E-news, thus reducing rather than maintaining or improving public engagement.[4] The result would therefore undermine the

[4] As petitioner acknowledges, recipients can simply delete any email from him without engaging with him at all, or with anyone else.

animating purpose of FOIL to make the workings of government transparent and accessible to the public. Nothing is gained by the public from disclosure of these subscribers' email addresses and accompanying names. Lastly, petitioner concedes that there are other ways he can attempt to reach Town residents using social media. In sum, there is no public interest served by disclosure of the E-news subscribers' names and email addresses.

In reaching a contrary decision, the Appellate Division misapplied our balancing test (*see City of N.Y. Fire Dept.*, 4 NY3d at 485). First, the Court did not discuss the privacy interests at stake or how it balanced those interests against the public interest in disclosure (227 AD3d at 1084-1085). Second, the Court employed the wrong standard in concluding that the Town's asserted cybersecurity risks were speculative because "the Town failed to show that disclosure . . . under the conditions imposed . . . would make the E-news subscribers or the Town more susceptible to such risks than they ordinarily would be" (*id.* at 1085). Although cybersecurity threats are risks faced by any email user, the Town needed only to establish that the subscribers' interest in maintaining their information private outweighed any public interest in its disclosure (*see City of N.Y. Fire Dept.*, 4 NY3d at 485). For the reasons discussed, we conclude that the Town demonstrated that disclosure would constitute an unwarranted invasion of personal privacy.

III.

In sum, the Town established that the names and email addresses of Town residents who subscribe to E-news are exempt from disclosure under FOIL. The balance tips in only

one direction: in favor of the privacy interest. Accordingly, the Appellate Division order should be reversed, with costs, and the petition dismissed.

Order reversed, with costs, and petition dismissed. Opinion by Judge Rivera. Chief Judge Wilson and Judges Garcia, Singas, Cannataro, Troutman and Halligan concur.

Decided February 19, 2026