No. S218066

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

City of San Jose, *et al.*,
Defendants and Petitioners Below,
vs.
Superior Court of the State of California,
Respondent.

Ted Smith,
Plaintiff, Real Party in Interest, and Petitioner Here.

Amicus Curiae Brief in Support of Plaintiff-Petitioner Ted Smith

After Decision by the Court of Appeal
Sixth Appellate District, Case No. H039498
Santa Clara County Superior Court, Case No. 1-09-CV-150427

MICHAEL T. RISHER (191627)
mrisher@aclunc.org
MATTHEW T. CAGLE (286101)
mcagle@aclunc.org
CHRISTOPHER J. CONLEY (290747)
cconley@aclunc.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
Phone: (415) 621-2493

PETER BIBRING (223981)
pbibring@aclusocal.org
PETER ELIASBERG (189110)
peliasberg@aclusocal.org
AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA, INC.
1313 West 8th Street
Los Angeles, CA 90017
Phone: (213) 977-9500

JENNIFER LYNCH (240701)
jlynch@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333

DAVID LOY (229235)
davidloy@aclusandiego.org
AMERICAN CIVIL LIBERTIES UNION OF SAN DIEGO & IMPERIAL COUNTY, INC.
2750 5th Avenue #300
San Diego, CA 92101
Phone: (619) 232-2121

No. S218066

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

City of San Jose, *et al.*,
Defendants and Petitioners Below,
vs.
Superior Court of the State of California,
Respondent.

Ted Smith,
Plaintiff, Real Party in Interest, and Petitioner Here.

Amicus Curiae Brief in Support of Plaintiff-Petitioner Ted Smith

After Decision by the Court of Appeal
Sixth Appellate District, Case No. H039498
Santa Clara County Superior Court, Case No. 1-09-CV-150427

MICHAEL T. RISHER (191627)
mrisher@aclunc.org
MATTHEW T. CAGLE (286101)
mcagle@aclunc.org
CHRISTOPHER J. CONLEY (290747)
cconley@aclunc.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
Phone: (415) 621-2493

PETER BIBRING (223981)
pbibring@aclusocal.org
PETER ELIASBERG (189110)
peliasberg@aclusocal.org
AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA, INC.
1313 West 8th Street
Los Angeles, CA 90017
Phone: (213) 977-9500

JENNIFER LYNCH (240701)
jlynch@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333

DAVID LOY (229235)
davidloy@aclusandiego.org
AMERICAN CIVIL LIBERTIES UNION OF SAN DIEGO & IMPERIAL COUNTY, INC.
2750 5th Avenue #300
San Diego, CA 92101
Phone: (619) 232-2121

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Cases

Federal Statutes

State Statutes

Rules

Regulatory Authorities

Constitutional Provisions

No. S218066

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

City of San Jose, *et al.*,
Defendants and Petitioners Below,
vs.
Superior Court of the State of California,
Respondent.

Ted Smith,
Plaintiff, Real Party in Interest, and Petitioner Here.

Amicus Curiae Brief in Support of Plaintiff-Petitioner Ted Smith

After Decision by the Court of Appeal
Sixth Appellate District, Case No. H039498
Santa Clara County Superior Court, Case No. 1-09-CV-150427

MICHAEL T. RISHER (191627)
mrisher@aclunc.org
MATTHEW T. CAGLE (286101)
mcagle@aclunc.org
CHRISTOPHER J. CONLEY (290747)
cconley@aclunc.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
Phone: (415) 621-2493

PETER BIBRING (223981)
pbibring@aclusocal.org
PETER ELIASBERG (189110)
peliasberg@aclusocal.org
AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA, INC.
1313 West 8th Street
Los Angeles, CA 90017
Phone: (213) 977-9500

JENNIFER LYNCH (240701)
jlynch@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333

DAVID LOY (229235)
davidloy@aclusandiego.org
AMERICAN CIVIL LIBERTIES UNION OF SAN DIEGO & IMPERIAL COUNTY, INC.
2750 5th Avenue #300
San Diego, CA 92101
Phone: (619) 232-2121

No. S218066

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

City of San Jose, *et al.*,
Defendants and Petitioners Below,
vs.
Superior Court of the State of California,
Respondent.

Ted Smith,
Plaintiff, Real Party in Interest, and Petitioner Here.

Amicus Curiae Brief in Support of Plaintiff-Petitioner Ted Smith

After Decision by the Court of Appeal
Sixth Appellate District, Case No. H039498
Santa Clara County Superior Court, Case No. 1-09-CV-150427

MICHAEL T. RISHER (191627)
mrisher@aclunc.org
MATTHEW T. CAGLE (286101)
mcagle@aclunc.org
CHRISTOPHER J. CONLEY (290747)
cconley@aclunc.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
Phone: (415) 621-2493

PETER BIBRING (223981)
pbibring@aclusocal.org
PETER ELIASBERG (189110)
peliasberg@aclusocal.org
AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA, INC.
1313 West 8th Street
Los Angeles, CA 90017
Phone: (213) 977-9500

JENNIFER LYNCH (240701)
jlynch@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333

DAVID LOY (229235)
davidloy@aclusandiego.org
AMERICAN CIVIL LIBERTIES UNION OF SAN DIEGO & IMPERIAL COUNTY, INC.
2750 5th Avenue #300
San Diego, CA 92101
Phone: (619) 232-2121

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Cases

Federal Statutes

State Statutes

Rules

Regulatory Authorities

Constitutional Provisions

Other Authorities

APPLICATION TO FILE *AMICUS* BRIEF

All three California affiliates of the American Civil Liberties Union and the Electronic Frontier Foundation urge the Court to reverse the Court of Appeal. That court's holding violates both the letter and spirit of the California Public Records Act (PRA) and Article I, section 3 of the California Constitution by holding that emails relating to official business are outside the PRA merely because they are sent and received using non-governmental accounts. And the court's reasoning would allow government officials and employees to circumvent the PRA simply by opening a new browser window and logging into a personal web-based email account as they sit at their government-owned computers. The result would be to curtail if not eliminate public access to informal emails between individual officials and employees and with industry and special interests that provide critical insights into governmental operations beyond the often sanitized contents of formal memoranda and bulletins: not just *what* the government is doing but *why* it is doing it and at whose behest. These types of emails have provided the public with information on subjects ranging from California's implementation of its capital punishment laws to the apparently politically motivated closure of the George Washington bridge on the East Coast to the work of the U.S. Department of State, all of which represent vital information that the public otherwise would never have obtained.

INTERESTS OF AMICI

Proposed Amici are the California affiliates of the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF). The ACLU is a national, nonprofit, nonpartisan civil liberties organization with more than 500,000 members dedicated to the principles of liberty and equality embodied in both the United States and California constitutions

and our nation's civil rights law. It has three California affiliates: The ACLU of Northern California, the ACLU of Southern California, and the ACLU of San Diego & Imperial Counties.

Since their founding, both the national ACLU and California ACLU affiliates have had an abiding interest in the promotion of the guarantees of liberty and individual rights embodied in the federal and state constitutions, including the freedom of speech and freedom of the press guaranteed by the First Amendment to the United States Constitution and the Liberty of Speech Clause of the California Constitution.

EFF is a San Francisco-based, donor-supported, nonprofit civil liberties organization working to protect and promote fundamental liberties in the digital world. Through direct advocacy, impact litigation, and technological innovation, EFF's team of attorneys, activists, and technologists encourage and challenge industry, government, and courts to support free expression, privacy, and transparency in the information society.

Amici believe in—and have long advocated for—both governmental transparency and also personal privacy, both of which are expressly protected by our state constitution.[1]

Because of these interests, *amici* respectfully request that this Court allow them to submit this brief addressing the state constitutional issue. *See* Rule of Ct. 8.520(f).

---

[1] Amici and their counsel have advocated for open government under the PRA in cases such as *Sierra Club v. Superior Court*, 57 Cal. 4th 157 (2013); *Am. Civil Liberties Union Found. v. Deukmejian*, 32 Cal. 3d 440 (1982); *Am. Civil Liberties Union of N. Cal. v. Superior Court*, 202 Cal. App. 4th 55 (2011); *N. Cal. Police Practices Project and ACLU v. Craig*, 90 Cal. App. 3d 116, 118 (1979). They have advocated for privacy under article I § 1 of the California Constitution in cases including *Sheehan v. San Francisco 49ers, Ltd.*, 45 Cal. 4th 992 (2009); *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1 (1994); *Brown v. Shasta Union High Sch. Dist.*, C061972, 2010 WL 3442147 (Cal. Ct. App. Sept. 2, 2010).

No person or entity other than *amici* and their counsel authored the attached brief or made any monetary contribution to its preparation.

Dated: July 22, 2015

Respectfully submitted,

By: _____
Michael T. Risher

By: _____
Matthew T. Cagle

American Civil Liberties Union
Foundation of Northern California, Inc.

Attorneys for *Amici Curiae*

AMICUS BRIEF

1. INTRODUCTION AND SUMMARY OF ARGUMENT

In California, "information concerning the conduct of the people's business is a fundamental and necessary right of every person." Gov't Code § 6250. Our constitution specifically provides that "the writings of public officials and agencies shall be open to public scrutiny." CAL. CONST. art. I, § 3(b)(1). To ensure that these rights are not diluted by executive or judicial decisions, every provision of law must be "broadly construed if it furthers the people's right of access." *Id.* § 3(b)(2); *see also Sierra Club v. Superior Court*, 57 Cal. 4th 157, 175 (2013). The PRA, like all statutes, should be read in light of what it is meant to accomplish and in order to "result in wise policy rather than mischief or absurdity." *People v. Zambia*, 51 Cal. 4th 965, 972 (2011).

The fundamental error the City makes is that it advances an arguable, but cramped, reading of the statutory language, rather than adopting the more plausible and broader reading that is required under article I § 3(b)(1) of the California Constitution. The City's claim that the PRA's definition of "local agency" cannot cover individual officers or employees because it does not expressly list them ignores not just the expansive purpose of the PRA but also the fact that the definition is not meant to be exclusive: the PRA states that the term "'local agency' *includes*" the listed bodies and that the term "public records" *includes* the enumerated categories of writings. § 6252(a), (e) (all unlabeled statutory references are to the Government Code). This Court has long held that the Legislature's use of the term "[i]ncludes" is "ordinarily a term of enlargement rather than limitation." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 774 (2002) (citation omitted). Both the mandate of article I § 3(b)(1) and the Legislative intent behind the PRA require that the provision be read to include work-related emails of

government officials, regardless of whether they use official or private accounts to send or receive them.

Contrary to the City's claims, this reading of the PRA will not infringe upon the personal privacy of government employees. The CPRA only applies to documents "relating to the conduct of the public's business." § 6252(e). Moreover, the statute contains exceptions that protect employee privacy; employees, public agencies, and courts can ensure that responsive records are identified and released without allowing any government access to accounts or to personal information that is unrelated to the public's business. As the experiences of other states and the federal government demonstrate, it is entirely feasible to ensure that the people of this state have access to a local government official's emails relating to the public business and maintained on private devices or accounts, without compromising that official's personal privacy.

Finally, the City's proposed rule would create perverse incentives for public officials to use private accounts for public business in a manner that raises digital-security concerns. Under the City's interpretation of the CPRA, officials seeking to shield their correspondence from public scrutiny know they can do so simply by switching to a personal account or device to conduct government business. Not only does this violate the statutory and constitutional open-records provisions, it undermines the government's ability to oversee and manage the digital security of public records, including sensitive records related to public health, educational institutions, and criminal investigations.

2. ARGUMENT

2(A) The City's proposed rule is inconsistent with the statutory definition of a public record.

In arguing that the statutory definition of public records excludes messages sent or received using non-governmental accounts, the City relies heavily on the fact that the PRA's definition of state agency, but not local agency, specifically includes an "officer." *See* § 6250(a), (f). But this argument is flawed for two reasons: (1) the statutory text shows that the definition of a local agency, unlike the definition of a state agency, is not meant to be exhaustive; and (2) inclusion of the word "officer" in the state definition is necessary to include elected state executive officers who are not part of any state agency, a consideration that simply does not apply with respect to local agencies and officers.

First, the statutory definition of "local agency" states that the term "*includes*" counties, cities, and other listed entities. § 6252(a). Similarly, the term "Public records" "*includes*" writings relating to the "public's business prepared, owned, used, or retained" by local or state agencies. § 6262(c) (emphasis added). This Court has repeatedly held that, as used in California statutes, the term "[i]ncludes" is "ordinarily a term of enlargement rather than limitation," and that a "statutory definition of a thing as 'including' certain things does not necessarily place thereon a meaning limited to the inclusions." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 774 (2002) (citing *Ornelas v. Randolph, Inc.*, 4 Cal. 4th 1095, 1101 (1993) and *People v. W. Air Lines*, 42 Cal. 2d 621, 639 (1954)). Thus, for example, it has held that provisions in the Public Utilities Code defining "common carriers" to "include[]" 18 enumerated types of corporations also cover other types of transportation companies that are not listed, because that expansive interpretation is more consistent with the statute's purpose. *W. Air Lines*, 42 Cal. 2d at 639. Here, reading the definitions of local

agency and public records to include work-related emails that government officers and employees send or receive using private accounts furthers the purposes of the PRA and the constitutional right to information about the public business; indeed, because a government agency "can act only through its officers and employees," a contrary would frustrate the purpose of these statutory and constitutional provisions.[2]

The use of the term "includes" in the definition of *local* agency is particularly significant here because the PRA's statutory definition of *state* agency uses more restrictive language: "'State agency' *means* every state office ...." § 6252(f) (emphasis added). Similarly, the definition of "public record" also contains a more restrictive aspect relating to gubernatorial records: "'Public records' in the custody of, or maintained by, the Governor's office means any writing prepared on or after January 6, 1975." § 6252(e). The use of two different words—"means" vs. "includes"—in the same statute shows that the Legislature intended two different meanings. *See Briggs v. Eden Council for Hope and Opportunity*, 19 Cal. 4th 1106, 1117 (1999). The Legislature's decision to use "includes" in some definitions and the restrictive "means" in others confirms that it did not intend the definitions of local agencies and public records to be limited to the enumerated bodies and types of writings.

Second, that the definition of "state agency"—but not of "local agency"—specifically lists "officers," does not suggest any legislative intent to exempt local public officials from complying with the PRA.

---

[2] *Suezaki v. Superior Court of Santa Clara Cnty.*, 58 Cal. 2d 166, 174 (1962); *see Dearborn v. Grand Lodge A.O.U.W.*, 138 Cal. 658, 663 (1903) ("[A]n artificial person .... cannot sit down and write its name. It acts through its members, or officers, or agents."). The drafters of the PRA are presumed to have crafted the law with these principles in mind. *See People v. Scott*, 58 Cal. 4th 1415, 1424 (2014); *People v. Superior Court (Zamudio)*, 23 Cal. 4th 183, 199 (2000).

Instead, this different language simply reflects the fact that elected state constitutional officers such as the Governor, Lieutenant Governor, Secretary of State, and Treasurer may not be part of any state agency. *See generally* CAL. CONST. art. V, §§ 1, 9, 11. The Legislature therefore needed to specifically include state officers in order to ensure that there are no gaps in the PRA's coverage. No such language is needed in the definition of "local agency" because the comprehensive definition of that term already includes all local employees; neither the California Constitution nor any statute creates any local officials that are not part of a local agency as defined under the PRA. *See generally* CAL. CONST. art. XI, § 1(b) (county officers), § 2 (cities); Gov't Code § 24000 (listing county officers); §§ 34903, 36501 (city officers).

Third, even if it is possible to read the definitions of "local agency" and "public records" more narrowly, article I § 3 commands that the statute be read broadly so as to promote access, particularly in light of its command that "the writings of public officials…shall be open to public scrutiny."

In light of these constitutional mandates, the PRA's reference to "writings … prepared, owned, used, or retained by any … agency," therefore must include documents relating to government business that the agency's officials and employees have prepared, used, or retained as part of their employment. To hold otherwise would create an exception that swallows the rule.

2(B) The City's proposed rule would improperly prevent critical access to information about how our government is working.

Under the City's cramped reading of the PRA, it is perfectly lawful for government officials and employees to conduct public business in secret, even as they sit in their government offices in front of their

government computers, simply by logging on to a non-governmental email account.[3] This result would frustrate the PRA's goal of ensuring public access to "every conceivable kind of record that is involved in the governmental process," other than those specifically exempted. *Sander v. State Bar of Cal.*, 58 Cal. 4th 300, 322 (2013) (citation omitted). "Only purely personal information unrelated to 'the conduct of the public's business," *id.*, such as "the shopping list phoned from home, the letter to a public officer from a friend which is totally void of reference to governmental activities" is excluded from the definition of a public record. *California State Univ. v. Superior Court*, 90 Cal. App. 4th 810, 825 (2001) (citation omitted). This means that public records include not just official memoranda, bills, and directives, but also a government official's or employee's emails to colleagues about official business, notes they have taken at meetings, and communications with lobbyists and other members of the public, all of which must be disclosed unless they are exempt. Government officials cannot be allowed to circumvent the disclosure requirements merely by using non-governmental accounts to conduct public business.

---

[3] Web-based email accounts accessed through a web browser commonly leave no local copy of outgoing or incoming emails unless the user installs a separate program or browser plug-in to allow offline access; messages are kept only on the provider's servers. Although the records request in this case involved only messages sent using private devices, the Court of Appeal's reasoning applies equally to all records that are "not stored on [government] servers and are not directly accessible by the [government]." Court of Appeal Opn., Slip. Op. at 2; *see, e.g., id.* at 19 ("the issue presented here [is] whether a writing that undisputedly is related to official business is subject to disclosure when it is outside the public body's electronic communication system.").

This is particularly important because these less-formal emails and notes are often the most revealing materials released under the PRA. For example, when the ACLU was investigating how the state had obtained execution drugs from other states, many of the records it obtained from the CDCR were copies of emails between individual employees that they could easily have sent using non-government accounts.[4] These included records relating to the CDCR's decision to trade execution drugs with other states, in what officials described as a "secret … mission" that would be done "very discreetly."[5] These emails were widely covered in the media and have contributed to the continuing public debate over capital punishment.[6]

---

[4] *See, e.g.*, Records of E-mail Between Employees Regarding Secret Mission to Arizona, ACLU OF NORTHERN CALIFORNIA (Sept. 29, 2010), https://www.aclunc.org/sites/default/files/secret_mission_to_arizona.pdf; *see generally Documents from the CDCR*, ACLU OF NORTHERN CALIFORNIA (April 7, 2011), https://www.aclunc.org/blog/documents-cdcr.

[5] Records of E-mail Between Employees Regarding Secret Mission to Arizona, *supra* note 5. The reference to "a secret and important mission" and the promise that "it will be done very discretely" appear on the first page of this set, which is Bates stamped LI000859/ACLU PRA 000991.

[6] *See, e.g.*, Gregg Zoroya, *Death penalty spurs Wild West scramble for drugs*, USA TODAY (Mar. 17, 2014), *available at* http://www.usatoday.com/story/news/nation/2014/03/09/executions-lethal-injection-drugs-prisons-death-penalty/5866947/ ("California launched a 'secret mission' to swap some of its muscle relaxant for vials of Arizona's sodium thiopental in 2010…..Scott Kernan, a California prison executive at the time, exulted over the mission's success in an e-mail that became grist for Comedy Central's Colbert Report: 'You guys in AZ are life savers. By (sic) you a beer next time I get that way.'"); John Schwartz, *Seeking Execution Drug, States Cut Legal Corners*, N.Y. TIMES (April 13, 2011), *available at* http://www.nytimes.com/2011/04/14/us/14lethal.html?_r=0 (discussing these same emails). *See generally Am. Civil Liberties Union of N. Cal. v. Superior Court*, 202 Cal. App. 4th 55, 64 (2011) (describing litigation over these documents and holding that the CDCR must release additional documents).

And, although it involves New Jersey rather than California officials, the famous email that led to the politically motivated partial closure of the George Washington Bridge in 2013 is a perfect example of how government officials may use non-governmental accounts to try to hide unsavory aspects of how they are exercising their official powers: "Time for some traffic problems in Fort Lee," one official wrote from her Yahoo account to another official's Gmail account, as they cooked-up a near-shutdown of one of New York City's main access points.[7] Because no California law requires government officials or employees to use their official email accounts to conduct public business, the City's position would allow public officials to send these sorts of emails in complete secrecy; the public would have no access to them at all. This result cannot be what the legislature or the voters intended when they passed the PRA and amended the state constitution to ensure public access to information about how, why, and on whose behalf our government is using its authority. *See* VOTER INFORMATION GUIDE FOR 2004, GENERAL ELECTION 14 (2004) (argument in favor of Proposition 59).[8]

---

[7] *Christie administration traffic jam correspondence*, MOTHER JONES: DOCUMENTS, *available at* http://www.motherjones.com/documents/1003323-christie-administration-traffic-jam-correspondence. *See generally* Kate Zernike, *Christie Faces Scandal on Traffic Jam Aides Ordered,* N.Y. TIMES (Jan. 8, 2014), *available at* http://www.nytimes.com/2014/01/09/nyregion/christie-aide-tied-to-bridge-lane-closings.html. The documents on the Mother Jones website show that this was just one of the many messages about the closures sent by public officials using private accounts.

[8] *Available at* http://repository.uchastings.edu/cgi/viewcontent.cgi?article=2236&context=ca_ballot_props

2(C) The Court of Appeal's categorical rule barring access is not needed to protect privacy.

Of course, both the PRA and Article I § 3 both recognize the importance of protecting privacy, as do amici. Californians do not forfeit their state and federal rights to privacy when they enter government service. *See O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (plurality); *Long Beach City Emps. Assn. v. City of Long Beach*, 41 Cal. 3d 937, 951 (1986). But the City's categorical rule denying access to all relating to official business sent using non-governmental accounts is not needed to protect employee privacy. Standard procedures and protocols for complying with PRA and discovery requests—ones that are enshrined in the policies of other states and the federal government—ensure that public access to official records stored in non-governmental accounts does not infringe on privacy.

In responding to PRA requests, state and local agencies do not rifle through the desks, briefcases, and filing cabinets of every employee who might have responsive records; indeed, in part because employees often keep personal items in these areas, agencies would likely be prohibited from doing so. Nor do agencies typically need to send a technician to search the local drives of each employee's computer to locate responsive records so long as employees properly cooperate with a records search. Rather, they work with employees who might know about responsive records to locate them, whether those records are on paper or in electronic form, and whether they are stored in an employee's office, in a storage room, or in her home office or briefcase. The City itself notes that it "generally relies on [its employees'] integrity to comply with CPRA requests." City of San Jose Brief at 29 (March 27, 2015). It could do the same here and require these employees to search non-governmental accounts and disclose work-related emails, as they would in responding to a discovery request. This would not require employees to disclose any private

emails to their employer or to the public because records unrelated to the public's business are simply not covered by the CPRA, regardless of where they are stored. *See* § 6252(e); *San Gabriel Tribune v. Superior Court*, 143 Cal. App. 3d 762, 774 (1983). The City's claim that employees somehow have a right to refuse to cooperate in retrieving work-related records is unsupported and wrong as a matter of law. *See Spielbauer v. Cnty. of Santa Clara*, 45 Cal. 4th 704, 725 (2009) ("a public employee may be required—on pain of dismissal—to answer questions 'specifically, directly, and narrowly relating to the performance of his official duties.'") (quoting *Long Beach City Emps. Assn.*, 41 Cal. 3d at 947).

The federal Electronic Communications Privacy Act (ECPA) does not change this because it simply does not apply here. ECPA—and more specifically, the part of it called the Stored Communications Act (SCA)—generally prohibits the Government from obtaining electronic communications *from email providers* without following specific procedures. *See Juror No. One v. Superior Court*, 206 Cal. App. 4th 854, 860-62 (2012). But the law does not prohibit the City from requiring its employees to provide it with copies of emails relating to public business. *See id.* at 864-65, 868 (court could order juror to disclose Facebook postings even if it could not obtain them directly from Facebook under SCA/ECPA); *see also O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 1446 (2006) ("Where a party to the [electronic] communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions," even though SCA prohibited obtaining emails from provider); *Mintz v. Mark Bartelstein & Assocs., Inc.*, 885 F. Supp. 2d 987, 994 (C.D. Cal. 2012) (defendant could

use discovery to obtain text messages directly from plaintiff even though SCA prohibited obtaining them from provider).[9]

Nor will this procedure infringe on employees' personal privacy. Employees who want to avoid the burden of having to comply with requests that they search for and disclose business-related emails that they sent or received using private accounts can simply refrain from using non-governmental accounts to conduct official business, or can forward copies of any work-related messages to their government accounts (just as employees who are concerned about their privacy refrain from using their work email accounts for personal purposes). In fact, this is how the federal government ensures that official records are preserved for public oversight even where they are held within personal accounts, without invading the privacy of federal employees. Since 2009, federal law has required agencies that allow employees to use non-agency email accounts to ensure those records are preserved as agency records:

> Agencies that allow employees to send and receive official electronic mail messages using a system not operated by the agency must ensure that Federal records sent or received on such systems are preserved in the appropriate agency recordkeeping system.
>
> 36 C.F.R. § 1236.22(b).

The Office of Management and Budget and the National Archives thus instruct agencies that "Email sent on personal email accounts

---

[9] This would not, as the City suggests at pages 17-18 of its brief, violate Government Code § 6270. That section simply prohibits the government from selling or otherwise transferring public records to a private entity in a way that would prevent the government from maintaining control over those records so that it can comply with the PRA.

pertaining to agency business and meeting the definition of Federal records must be filed in an agency recordkeeping system."[10]

Under this regulatory scheme, federal agencies must maintain specific policies and procedures for official use of personal email accounts and the retention of official records. For example, the Environmental Protection Agency (EPA) requires that employees who send or receive official messages using a private account forward copies to their official account and delete them from the non-official account. ENVIRONMENTAL PROTECTION AGENCY, NO. CIO 2155.2, INTERIM RECORDS MANAGEMENT POLICY (2013).[11] The Department of Energy (DOE) also requires that the agency "[c]apture and manage records created or received via websites and portals, or from personal email used for Departmental business." U.S. DEPARTMENT OF ENERGY, OFFICE OF INFORMATION RESOURCES, DOE ORDER 243.1B, ADMIN CHG 1, RECORDS MANAGEMENT PROGRAM, (2013).[12]

---

[10] Davis S. Ferriero, NARA BULLETIN 2014-06, GUIDANCE ON MANAGING EMAIL, NATIONAL ARCHIVES (Sept. 15, 2014), *available at* http://www.archives.gov/records-mgmt/bulletins/2014/2014-06.html; Davis S. Ferriero, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES AND INDEPENDENT AGENCIES, GUIDANCE ON MANAGING EMAIL, OFFICE OF MANAGEMENT AND BUDGET (Sept. 15, 2014), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-16.pdf (incorporating Bulletin 2014-06).

[11] ENVIRONMENTAL PROTECTION AGENCY, NO. CIO 2155.2, INTERIM RECORDS MANAGEMENT POLICY, (2013), *available at* http://www.epa.gov/irmpoli8/policies/CIO-2155.2.pdf.

[12] U.S. DEPARTMENT OF ENERGY, OFFICE OF INFORMATION RESOURCES, DOE ORDER 243.1B, ADMIN CHG 1, RECORDS MANAGEMENT PROGRAM, (2013), *available at* https://www.directives.doe.gov/directives-documents/200-series/0243.1-BOrder-b-admchg1.

In accordance with these regulations and policies, Congress recently amended federal law to establish a straightforward and non-invasive rule governing all the use of personal email accounts for official business by all executive employees. Under the Presidential and Federal Records Act Amendments Of 2014, government employees may only use personal mail accounts for official business if they either copy an official e-mail account in sending the message or later forwards that message to an official e-mail account:

> An officer or employee of an executive agency may not create or send a record using a non-official electronic messaging account unless such officer or employee-
> (1) copies an official electronic messaging account of the officer or employee in the original creation or transmission of the record; or
> (2) forwards a complete copy of the record to an official electronic messaging account of the officer or employee not later than 20 days after the original creation or transmission of the record.

44 U.S.C. § 2911(a).[13]

These established policies and the new statute demonstrate that government employees may use personal email accounts while at the same time ensuring that records in those accounts that relate to government business are preserved for the public, without providing the government

---

[13] *See also H.R. 1233—Presidential and Federal Records Act Amendments of 2014*, CONGRESS.GOV (Nov. 26, 2014), https://www.congress.gov/bill/113th-congress/house-bill/1233/text (bill amending 44 U.S.C. § 2911).

with actual access to private accounts or private messages contained on them or otherwise infringing on the privacy of government employees.[14]

Finally, it is important to remember that the PRA has exemptions that protect privacy. The government can withhold records—or parts of records—if the public interest in non-disclosure clearly outweighs the public interest in disclosure. § 6255(a); *see* §§ 6253(a), 6254(c). Thus, the government may, when appropriate, redact an employee's private email address to protect privacy[15] and may, in appropriate circumstances, withhold messages—or, under § 6253(a), parts of messages—that do not relate to official business. *Cf. Am. Civil Liberties Union of N. Cal. v. Superior Court*, 202 Cal. App. 4th 55, 81-82 (2011) (allowing agency to redact portions of documents that are not responsive to request under § 6253(a)). The City's categorical rule that emails relating to public business sent or received using private accounts are beyond the scope of the PRA is simply not needed to protect employee's privacy.

---

[14] Although most if not all federal agencies allow their employees to use private email accounts if they follow these protocols, they also encourage them to use their official accounts when conducting official business. *See* EPA Interim Records Management Policy CIO 2155.2 (June 28, 2013), *available at* http://www.epa.gov/irmpoli8/policies/CIO-2155.2.pdf ("[O]fficial agency business should first and foremost be done on official EPA information systems"); U.S. DEPARTMENT OF ENERGY, OFFICE OF INFORMATION RESOURCES, DOE ORDER 243.1B, ADMIN CHG 1, RECORDS MANAGEMENT PROGRAM, (2013), *available at* https://www.directives.doe.gov/directives-documents/200-series/0243.1-BOrder-b-admchg1.

[15] Amici take the position that in such cases the government should only partially redact these addresses, leaving the domain name (the part after the "@") so that the public can see whether the employee is using a private or an official account to conduct official business.

2(D) The experience of other states shows that Plaintiff's proposed rule is workable.

Judicial and administrative decisions from numerous other states make official emails sent and received by personal accounts subject to public records laws. These decisions rest on interpretations of public records laws that focus on the nature of the record and seek to ensure that the public's right to know is not eliminated simply because officials use non-official channels to conduct the people's business. And while the specific text of public records laws varies from state to state, many of these states that allow public access to emails sent or received from private accounts have open records laws with provisions that, like the provisions here at issue, do not specifically refer to local officials.

Numerous courts have held that official emails sent and received via personal accounts are subject to state open records laws, regardless of whether those statutes specifically refer to individual officers or employees and regardless of whether the locality possessed the requested record itself. *See Mollick v. Twp. of Worcester*, 32 A.3d 859, 872-73 (Pa. Commw. Ct. 2011) (holding that emails located in private accounts could qualify as a "record" if it pertained to public business, even though statute only refers to agencies); *Vining v. Dist. of Columbia*, No. 2013CA8189B (D.C. Super. Ct. July 9, 2014) (ordering the District of Columbia to produce emails from an official's personal e-mail account even though the District's public records law does not refer to records created by individual councilmembers or commissioners);[16] *Smith v. NY State Attorney General*, No. 3670-08, NYLJ 1202555064972, at *3 (N.Y.

---

[16] *Vining v. Dist. of Columbia*, No. 2013CA8189B (D.C. Super. Ct. July 9, 2014), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1235901/234984443-mcmillan-vining-v-dc-final-order-2014.pdf.

Sup. Ct., April 30, 2012), *rev'd on other grounds*, 973 N.Y.S.2d 404 (N.Y. App. Div. 2013) (for public's "maximum access" to agency records, "the [Office of the Attorney General] has both the responsibility and the obligation to gain access to the private e-mail account of former Attorney General Spitzer...."); [17] *cf. McLeod v. Parnell*, 286 P.3d 509, 514-15 (Alaska 2012) (allowing officials to use private email to conduct official business because employees would have duty to preserve those emails as public records); [18] *Bradford v. Dir., Emp't Sec'y Dep't*, 128 S.W.3d. 20, 28 (Ark. Ct. App. 2003) (rejecting an interpretation of the state's Freedom of Information Act that would exclude emails about the public's business sent over private accounts). In the above decisions, the public interest in the records at issue took precedence over the fact that the official rather than the agency possessed them.

In addition, Attorneys General interpreting public records statutes that do not refer to individual actors have decided that official emails sent on personal accounts are "public records" and subject to disclosure. *See* Inspection of Public Records Act Complaint—Mr. Joey Peters, Op. N.M. Att'y Gen. (Feb. 5, 2013) (interpreting "public records" under N.M Stat. Ann. § 14-2-6(E) and concluding that"[i]f email is used to conduct public business, the email is a public record, without regard to whether the email

---

[17] *Smith v. NY State Attorney General*, No. 3670-08, NYLJ 1202555064972, at *3 (N.Y. Sup. Ct., April 30, 2012), *available at* https://www.dos.ny.gov/coog/pdfs/smith_v_oag(spitzer).pdf.

[18] The Alaska Public Records Act defines "public records," in relevant part, as those "that are developed or received by a public agency, or by a private contractor for a public agency, and that are preserved for their informational value or as evidence of the organization or operation of the public agency." ALASKA STAT. § 40.25.220(3) (2015).

is created or maintained on a public or private email account."); [19] File No. 12-R-116; Gage Co. Board of Supervisors; Beatrice Daily Sun, Op. Neb. Att'y Gen. (July 2, 2012) (examining "public records" as defined at Neb. Rev. Stat. § 84-712.01(1) and finding that county "Board members…have an obligation to search for such records on members' personal email accounts."); [20] Public Access Opinion No. 11-006 at 5, Op. Ill. Att'y Gen. (Nov. 15, 2011) (interpreting 5 Ill. Comp. Stat. § 140/2(c) and holding that a city council's text messages pertaining to public business were subject to the state's FOIA law); [21] Op. Tenn. Open Records Counsel (Feb 8, 2011) (interpreting "public records," Tenn. Code Ann. Section 10-7-503(a), to include official emails sent and received on a personal device).[22] The above decisions focused on the content of specific email messages rather than the format by which they were sent and recognized that official bodies create public records through their respective members.

More generally, Attorneys General and other officials in at least half a dozen other states have issued opinions and guidance subjecting official emails on personal accounts and devices to public records laws. *See* Op.

---

[19] Inspection of Public Records Act Complaint – Mr. Joey Peters, *Op.* N.M. Att'y Gen. (Feb. 5, 2013), *available at* https://docs.google.com/viewer?a=v&pid=sites&srcid=bm1hZy5nb3Z8cHVibGljLXJlY29yZHMtcHJvamVjdHxneDo2OTViNGJlYzhmMzliZmY1.

[20] File No. 12-R-116; Gage Co. Board of Supervisors; Beatrice Daily Sun, Op. Neb. Att'y Gen. (July 2, 2012), *available at* https://bloximages.chicago2.vip.townnews.com/beatricedailysun.com/content/tncms/assets/v3/editorial/0/47/0477c440-ce89-5a81-9465-7542c00d5ed2/4ff7740f3130e.pdf.pdf.

[21] Public Access Opinion No. 11-006 at 5, Op. Ill. Att'y Gen. (Nov. 15, 2011), *available at* http://foia.ilattorneygeneral.net/pdf/opinions/2011/11-006.pdf.

[22] Op. Tenn. Open Records Counsel (Feb 8, 2011), *available at* http://tcog.info/files/2014/01/11-01CityOfClarksville.pdf.

Tx. Att'y Gen. No. 2012-06843 (May 9, 2012) (e-mails and text messages maintained in connection with transaction of official business in personal accounts are subject to open government act);[23] Op. Okla. Att'y Gen. No. 09-12 (May 13, 2009) (records of government business are subject to the state's Open Records Act even if they were created using a private email account or smart phone);[24] Op. Wis. Att'y Gen. (Sept. 25, 2006) (emails sent or received on personal email accounts by the Elections Board are subject to the state's public records law and suggesting the Board consider creating official email accounts to avoid the issue);[25] Op. N.D. Att'y Gen. No. 2008-O-15 (July 1, 2008) (official emails stored on the home computers of a school district's agents are subject to the state's open records law);[26] Op. Fl. Att'y Gen. No. 2008-07 (Feb. 26, 2008) (emails and web postings sent and received via personal accounts are a "public record" under Florida law);[27] Policy Dep't Maine Sec'y of State (advising state employees that "[I]f you are sending work emails using your personal email account, your account could become subject to Public Information Requests").[28]

---

[23] Op. Tx. Att'y Gen. No. 2012-06843 (May 9, 2012), *available at* https://www.texasattorneygeneral.gov/opinions/openrecords/50abbott/orl/2012/pdf/or201206843.pdf.

[24] Op. Okla. Att'y Gen. No. 09-12 (May 13, 2009), *available at* http://media.okstate.edu/faculty/jsenat/foioklahoma/09-12.PDF.

[25] Op. Wis. Att'y Gen. (Sept. 25, 2006), *available at* http://www.wisfoic.org/agopinions/2006_09_25%20dunst.pdf.

[26] Op. N.D. Att'y Gen. No. 2008-O-15 (July 1, 2008), *available at* http://www.ag.nd.gov/Opinions/2008/OR/2008-O-15.pdf.

[27] Op. Fl. Att'y Gen. No. 2008-07 (Feb. 26, 2008), *available at* http://www.myfloridalegal.com/ago.nsf/Opinions/B4D1320C99E9E532852573FB00726034.

[28] Policy Dep't, Maine Sec'y of State, *available at* http://www.maine.gov/sos/arc/records/state/emailguidebasic.doc.

That so many jurisdictions subject official emails to public records scrutiny regardless of where they were created or stored belies the City's claims that doing so is unworkable.

2(E) The government's position creates perverse incentives for public officials to use private accounts to conduct public business, even though they are less secure.

Creating an incentive to use private accounts to conduct public business poses a threat to the security of those communications, because private accounts create fundamental security risks that could be avoided by the use of a single well-planned communications network.

At the highest level, the use of private accounts undermines what is perhaps the most important security protocol for email: establishing and securing a single email system for all of an agency's employees. *See* NAT'L INST. OF STANDARDS & TECH., GUIDELINES ON ELECTRONIC MAIL SECURITY (Version 2 2007) (describing the process of implementing and maintaining a secure email infrastructure).[29] In fact, the use of personal accounts makes it impossible even to effectively identify all of the technologies that are used for communications, let alone evaluate and address potential security vulnerabilities. Moreover, the consensus of security experts is that internal networks are much easier to secure than the cloud-based services and similar products that most consumers use. CYBEREDGE GRP., 2015 CYBERTHREAT DEFENSE REPORT: NORTH AMERICA & EUROPE (2015).[30]

---

[29] NAT'L INST. OF STANDARDS & TECH., GUIDELINES ON ELECTRONIC MAIL SECURITY (Version 2 2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf.

[30] CYBEREDGE GRP., 2015 CYBERTHREAT DEFENSE REPORT: NORTH AMERICA & EUROPE (2015), *available at* http://www.brightcloud.com/pdf/cyberedge-2015-cdr-report.pdf.

The use of private accounts also hinders or precludes numerous specific security best practices. For example, end-to-end email encryption—which ensures that no intermediary can read the contents of an email—is relatively straightforward to implement on a single mail system but much more difficult to implement if government employees use their own private email accounts. *See* JIANGSHAN YU ET AL., CHALLENGES WITH END-TO-END EMAIL ENCRYPTION, WORLD WIDE WEB CONSORTIUM (2014).[31] Even email providers that encrypt email in transit, such as Google's Gmail,[32] can typically access the email themselves.[33] There are many other security practices that can be implemented on a single internal network that would be difficult if not impossible to implement across numerous private accounts, including:

- Access controls to limit access to specific devices or locations.
- Threat detection tools to identify and respond to unusual activity.
- Filters to detect and protect against malware and phishing emails.
- Identity verification based on direct personal relationship.

Many private email providers simply do not offer these tools that could be deployed to secure the government's internal email system. Moreover, even if a private account did offer the same security features as the government's own service, it would be much more difficult to ensure that each user properly implemented these features. A 2015 survey indicated

---

[31] JIANGSHAN YU ET AL., CHALLENGES WITH END-TO-END EMAIL ENCRYPTION, WORLD WIDE WEB CONSORTIUM (2014), *available at* https://www.w3.org/2014/strint/papers/08.pdf.

[32] *See Google Transparency Report, Email Encryption in Transit*, GOOGLE, https://www.google.com/transparencyreport/saferemail/.

[33] *See Terms of Service*, GOOGLE (Apr. 14, 2014), http://www.google.com/intl/en/policies/terms/ ("Our automated systems analyze your content (including emails) ....").

that 78 percent of security professional consider negligent or careless employees to be the greatest threat to email and network security. PONEMON INST. LLC, 2015 STATE OF THE ENDPOINT REPORT: USER-CENTRIC RISK 3.[34] Providing an incentive for government employees to create, configure, and use their own private accounts to conduct government business magnifies the risk of these types of security problems. Instead, government employees should be encouraged to use standard government accounts that allow greater opportunities for training and account management.

3. CONCLUSION

When the people of California overwhelmingly voted to enact Proposition 59, they made clear the importance that they attach to their "right of access to information concerning the conduct of the people's business." CAL. CONST. art. I § 3. The City's unduly narrow reading of the PRA's definition of "public record" is not mandated by the statutory text, violates the constitutional imperative that the law be read broadly so as to increase public access to information about the people's business, and will gut public disclosure law by allowing government officials and employees to circumvent the PRA. It is not necessary to protect privacy. This Court should hold that emails and other electronic communications relating to official business that government officials and employees send and receive are covered by the PRA, regardless of whether they are sent using official or private accounts.

---

[34] PONEMON INST. LLC, 2015 STATE OF THE ENDPOINT REPORT: USER-CENTRIC RISK 3, *available at* http://www.ponemon.org/local/upload/file/2015%20State%20of%20Endpoint%20Risk%20FINAL.pdf.

Dated: July 22, 2015

Respectfully submitted,

By: _____
Michael T. Risher

By: _____
Matthew T. Cagle

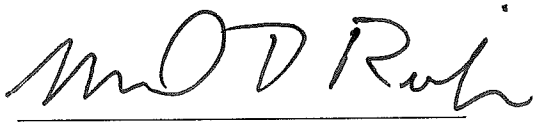
American Civil Liberties Union
Foundation of Northern California, Inc.

Attorneys for *Amici Curiae*

CERTIFICATE OF COMPLIANCE

I certify that the text in the attached Brief contains 5,869 words, as calculated by Microsoft Word, including footnotes but not the caption, the table of contents, the table of authorities, signature blocks, or this certification. *See* Rule of Court 8.204(c)(1), (3).

Dated: July 22, 2015



Michael T. Risher
American Civil Liberties Union
Foundation of Northern California, Inc.

DECLARATION OF SERVICE BY MAIL

I, the undersigned, declare that I am over 18 years of age and not a party to the within cause. I am employed in the County of San Francisco, State of California. My business address is 39 Drumm Street, San Francisco, CA 94111. My electronic service address is ihernandez@aclunc.org. On July 22, 2015, I served a true copy of the attached,

Amicus Curiae Brief in Support of Plaintiff Ted Smith

on each of the following, by placing same in an envelope(s) addressed as follows:

Richard Doyle
Nora Frimann
Margo Laskowska
OFFICE OF THE CITY ATTORNEY
200 E. Santa Clara Street, 16th Floor
San Jose, CA 95113

Clerk of the Court
SIXTH DISTRICT COURT OF APPEAL
333 W. San Carlos Street, Suite 1060
San Jose, CA 95113

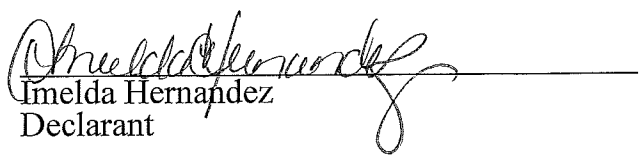
Karl Olson
RAM OLSON CEREGHINO & KOPCZYNSKI
555 Montgomery Street, Suite 820
San Francisco, CA 94111

Clerk of the Superior Court
SANTA CLARA COUNTY SUPERIOR COURT
191 N. First Street
San Jose, CA 95113

James McManis
Matthew Schechter
Christine Peek
Jennifer Murakami
MCMANIS FALKNER
50 W. San Fernando Street, 10th Floor
San Jose, CA 95113

Each said envelope was sealed and the postage thereon fully prepaid. I am familiar with this office's practice of collection and processing correspondence for mailing with the United States Postal Service. Under that practice each envelope would be deposited with the United States Postal Service in San Francisco, California, on that same day in the ordinary course of business.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on July 22, 2015, at San Francisco, California.



Imelda Hernandez
Declarant