MEMORANDUM

TO: Commissioners and Observers, ULC Drafting Committee on Redaction of Personal Information from Public Records (RPIPR)

FROM: Matthew L. Schafer (Adjunct Professor, Fordham Law School[1]), Observer

DATE: January 19, 2024

SUBJECT: First Amendment Implications of RPIPR

On December 6, 2023, the Committee met to discuss, among other things, the First Amendment implications of proceeding with the drafting of the Redaction of Personal Information from Public Records uniform law (the "RPIPR"). After I provided comment on the First Amendment and common law right of access, Committee Chair Vince DeLiberato requested I submit written comments expanding on those comments. This memo responds to that request.

I approach these issues as a scholar and a practitioner. I am an adjunct professor of law at Fordham University Law School where I teach mass media law, a seminar about how the law effects newsgathering and reporting and, by extension, how citizens understand the world around them. I also publish often, in law reviews and the popular press, on First Amendment issues, including the right of access and laws like the RPIPR.[2] And, I speak on these issues at universities, most often at Yale Law School's annual Access and Accountability Conference, which is designed to facilitate collaboration among practitioners, journalists, and law schools to promote governmental accountability and transparency.

I also have significant experience litigating these issues as I have spent a decade representing (both in private practice and in-house) news organizations around the country in access matters. For example, I was previously newsroom counsel at BuzzFeed News, where we used public records every day to report on matters of public concern.[3] There, I also oversaw the largest public records litigation docket among any U.S. news organization and challenged state public records laws on constitutional grounds.

Finally, I approach these issues with a very real sense of their seriousness. Recently, perpetrators have engaged in disturbing and repeated harassment of judicial officials at their homes.[4] These individuals should be identified and held responsible for this unlawful conduct. For our purposes,

---

[1] Affiliation for identification purposes only. Views are those of the author alone.

[2] *See, e.g.*, Matthew L. Schafer, *How Privacy Laws Protect the Powerful, but Keep the Public in the Dark*, THE DAILY BEAST (July 4, 2023); *see also* Matthew L. Schafer, *Does* Houchins v. KQED, Inc. *Matter?*, 70 BUFF. L. REV. 1331 (2022); Jennifer Rodgers, Christopher Pioch, Jessenia Vazcones, & Matthew Schafer, *The Daniel Anderl Judicial Security & Privacy Act*, N.Y. City Bar (Jan. 26, 2022).

[3] Matthew L. Schafer, *How We Used Public Records Laws To Tell You Stories In 2018*, BUZZFEED NEWS (Dec. 27, 2018).

[4] *See, e.g.*, Kevin Breuninger & Dan Mangan, *Trump fraud trial judge home was swatting target, police say*, CNBC (Jan. 11, 2024).

though, I am unaware of evidence the perpetrators used public records in aid of their crimes. And, federal judges who were victims already enjoy the protections of a federal law like the RPIPR, but the perpetrators were still able to locate these judges. Despite this, on a personal level, I can understand the desire to do *something*. Roy Den Hollander, the same individual who murdered Judge Salas' son, had for years targeted me with vexatious litigation, false police reports, and bar complaints after I defended a client he had sued. So I remember the day he attacked Judge Salas' family with a particular sense of clarity and lingering helplessness. For that reason, none of what follows should be read as dismissing the seriousness of the problem.

I hope you find this perspective helpful.

I. The Importance of the Information Subject to Redaction

Before addressing the legal issues attendant to the RPIPR, one question raised at the December 6 meeting was how "private" information subject to RPIPR could be considered newsworthy. This question is important as the newsworthiness of covered information might well weigh on whether the RPIPR can survive a constitutional challenge.

Initially, courts generally defer to news organizations about what is newsworthy. The U.S. Supreme Court long ago explained that the "choice of material to go into a newspaper, and the . . . treatment of public issues and public officials—whether fair or unfair—constitute the exercise of editorial control and judgment."[5] It is the "press, acting responsibly, and not the courts" that "must make the ad hoc decisions as to what are matters of genuine public concern, and while subject to review, editorial judgments as to news content will not be second-guessed so long as they are sustainable."[6] Thus, it is not this Committee's role to make ad hoc decisions as to newsworthiness.

In any event, there can be no doubt that information subject to the RPIPR can be newsworthy, as recent reporting proves. ProPublica reported on land records showing that a conservative donor to political causes bought Supreme Court Justice Clarence Thomas' boyhood home and allowed his mother to live there for free.[7] The New York Times published an investigation into Justice Thomas' purchase of a luxury motor home—via an unconventional loan from a wealthy friend—based on public title records.[8] POLITICO reported on a questionable land deal between Justice Neil Gorsuch and a partner at a law firm that regularly has business before the Court.[9] Because of these reports and others, the Supreme Court adopted for the first time written ethics rules governing the Justices' conduct.[10]

The use of public records extends far beyond the Supreme Court too:

---

[5] *Miami Herald Pub. Co. v. Tornillo*, 418 U.S. 241, 258 (1974).
[6] *Gaeta v. New York News, Inc.*, 465 N.E.2d 802, 805 (N.Y. 1984)
[7] Justin Elliott, Joshua Kaplan & Alex Mierjeski, *Billionaire Harlan Crow Bought Property From Clarence Thomas. The Justice Didn't Disclose the Deal.*, PROPUBLICA (Apr. 13, 2023).
[8] Jo Becker & Julia Tate, *Clarence Thomas's $267,230 R.V. and the Friend Who Financed It*, N.Y. TIMES (Aug. 5, 2023).
[9] Heidi Przybyla, *Law firm head bought Gorsuch-owned property*, POLITICO (Apr. 25, 2023).
[10] *See* Regarding the Code of Conduct, U.S. SUP. CT. (Nov. 13, 2023).

- House Oversight Chairman James Comer was criticized for hypocrisy in rooting out allegedly questionable transactions between President Joe Biden and his son after it was discovered, based on property records, that Comer had engaged in similar transaction.[11]
- Significant questions were raised, based on property records, regarding whether former White House Chief of Staff Mark Meadows engaged in voter fraud.[12]
- The Tennessee Speaker of the House was suspected of not actually permanently living in the district he represents, an alleged violation of the Tennessee Constitution.[13]
- In New Jersey, property records showed that, after retiring, a New Brunswick police officer was rehired as a salaried employee (in addition to his pension) despite having moved far away.[14]
- In Minnesota, a journalist used public records to discover alleged conflicts of interest over the State Senate Majority Leader's effort to water down deer hunting regulations that would have hurt a family business.[15]
- In New York, news outlets reported on then-candidate for New York City Mayor, Eric Adams' questionable declarations about his residency, all based on public records.[16]
- Among the many lies Representative George Santos told, one of the first to come undone was his claim to "a family fortune in real estate"—thanks to public property records.[17]
- In Texas, the Center for Public Integrity discovered that two Fifth Circuit Judges "ruled on cases in which parties in the cases were energy companies that paid the couple royalties for extracting minerals from their property."[18]

As these examples show, the value of public records is not abstract. It is an essential part of accountability. In some cases, public records have been the key to breaking reports of potential wrongdoing. In other cases, once allegations have been made by others, public records have allowed journalists to confirm whether these allegations are true or, as importantly, whether they are untrue. Removing public records from the public domain will make this kind of journalism much more difficult, leaving bona fide allegations undiscovered while preventing journalists from disproving ones that are not.

---

[11] Roger Sollenberger, *James Comer, Like Joe Biden, Also Paid His Brother $200K*, THE DAILY BEAST (Nov. 9, 2023).
[12] *See, e.g.*, Glenn Kessler, *Mark Meadows, his wife, Debra, and their trailer-home voter registration*, THE WASHINGTON POST (Mar. 8, 2022).
[13] Judd Legum, *Where does the Tennessee House Speaker actually live?*, THE TENNESSEE TRIBUNE (Apr. 11, 2023).
[14] S.P. Sullivan, *N.J. journalist asked questions about where a public official lived. Now he's in legal trouble.*, NJ.COM (July 23, 2023).
[15] Sally Jo Sorensen, *More on Miller family deer farm interests*, BLUESTEM PRAIRIE (May 1, 2022).
[16] *See, e.g.*, Sally Goldenberg & Joe Anuta, *Burning the midnight oil: Eric Adams' mysterious whereabouts off the campaign trail*, POLITICO (June 8, 2021); Greg B. Smith & Yoav Gonen, *Eric Adams Admits Owning the Brooklyn Real Estate He Claimed to Have Sold*, THE CITY (June 22, 2022).
[17] Grace Ashford & Michael Gold, *Who Is Rep.-Elect George Santos? His Résumé May Be Largely Fiction*, N.Y. TIMES (Dec. 19, 2022).
[18] Reity O'Brien, Kytja Weir, & Chris Young, *Law-Breaking Judges Took Cases That Could Make Them Even Richer*, THE DAILY BEAST (Apr. 28, 2014).

II. The First Amendment Interests

A difficulty in assessing the constitutionality of the RPIPR is that the Committee process has advanced myriad iterations of such a law: some sealing the subject records from the public entirely; others only redacting certain information; others automatically sealing subject records; and others still suggesting the discretionary sealing of records subject to some factual showing.

Nevertheless, if ultimately adopted, the RPIPR may implicate at least three lines of First Amendment law. ***First*** is whether the RPIPR might be subject to a challenge based on the constitutional right of access. ***Second*** is whether the RPIPR might be subject to a constitutional challenge because of RPIPR's content- or speaker-based distinctions, if any. ***Third*** is whether the RPIPR might implicate one's right to distribute information free from governmental interference.

While each line of case law presents its own issues, they all seek to vindicate a fundamental First Amendment interest: the right to effective self-government. To be able to effectively petition the government, citizens need to be able to assemble to discuss public affairs; and to be able to effectively assemble and discuss their affairs, citizens must be able to share ideas about their government; and to be able to effectively share ideas, citizens must have access to information about the government, its officers, and their conduct in the first place. In short, the right to access information, discuss it, and petition the government are "a part of the working of the national government; . . . a part of the flow of communication which is its lifeblood."[19] This is consistent with the Supreme Court's observation that "'a major purpose of that Amendment was to protect the free discussion of governmental affairs.' By offering such protection, the First Amendment serves to ensure that the individual citizen can effectively participate in and contribute to our republican system of self-government."[20]

The RPIPR also implicates the common law right of access, which vindicates similar interests. Although the focus here is on the First Amendment, it suffices to note that the common law right is relevant to the RPIPR. It dates to our English ancestors,[21] and, for generations, states have recognized that the common law access right extends to broad swaths of public records—including property records. As the Michigan Supreme Court observed in 1889, "I have a right, if I see fit, to examine the title of my neighbor's property, whether or not I have any interest in it, or intend ever to have."[22] Courts have thus held that limits on disclosure in statutory public records laws cannot limit the common law right of access. For example, in *Rivera v. Union County Prosecutor's Office*, the New Jersey Supreme Court found that police disciplinary

---

[19] CHARLES BLACK, STRUCTURE AND RELATIONSHIP IN CONSTITUTIONAL LAW 41–43 (1969).
[20] *Globe Newspaper Co. v. Superior Ct.*, 457 U.S. 596, 604 (1982) (quoting *Mills v. Alabama*, 384 U.S. 214, 218 (1966)).
[21] *Herbert v. Ashburner*, 1 Wils. K. B. 297, 297 (1750) ("These are public books which every body has a right to see . . . .").
[22] *Burton v. Tuite*, 44 N.W. 282, 285 (Mich. 1889) ("I do not think that any common law ever obtained in this free government that would deny to the people thereof the right of free access to and public inspection of public records."); *see also State ex rel. Colescott v. King*, 57 N.E. 535, 537 (Ind. 1900) (noting that the common law right of access was necessary for citizens "to ascertain if the affairs of his country have been honestly and faithfully administered by the public officials charged with that duty").

records were subject to disclosure under the common law access right *even though* they were not subject to disclosure under New Jersey's freedom of information law.[23]

a. The Right of Access to Public Records

Turning back to the First Amendment, the scope of the constitutional access right is unsettled. A leading case is *Houchins v. KQED, Inc*., a 1978 Supreme Court case.[24] That case presented the question of whether, under the First Amendment, the press had a *special* right of access to a jail *beyond* what was provided to the public. Only seven Justices participated. The lead opinion was a three-Justice plurality, and the Court split 3-1-(3). The plurality concluded that "[n]either the First Amendment nor the Fourteenth Amendment mandates a right of access to government information."[25] The concurring opinion agreed with the plurality in part and with the dissenters in part, who would have found that "arbitrarily cutting off the flow of information at its source abridges the freedom of speech and of the press."[26]

Some have read *Houchins* broadly as standing for the proposition that the government can withhold government information from the press and the public altogether. Others have been more discerning. As Chief Justice John Roberts recognized (albeit before his time on the Court): *Houchins* did "not dispose of the more fundamental issue of what must be open to the public generally."[27] In fact, "far from rejecting any first amendment right of public access, certain characteristics of the plurality opinion seem to imply the existence of such a right."[28] The plurality, Roberts wrote, "went to considerable lengths . . . to list the range of alternative means of access to information about prisons available to the public," which "would have been irrelevant if there were indeed no right of access, and the sheriff could have completely sealed off the prison from the public."[29]

The Supreme Court followed *Houchins* a year later with *Gannett Co., Inc. v. DePasquale*, another access case.[30] There, it reserved judgment on the question the *Houchins* plurality purportedly foreclosed, namely, whether there is a First Amendment right of access to government information.[31] This suggested that a majority of the Court agreed with future-Chief Justice Roberts' view that *Houchins* did not finally resolve the question of a First Amendment right of access to government information. Had it, the Court would have had no reason to reserve the question in *Gannett Co., Inc.* Frustrated by the reservation of the First Amendment question in *Gannett Co., Inc.*, then-Justice Rehnquist argued that there was no question to reserve as *Houchins* had already foreclosed it, but he wrote only for himself.[32]

---

[23] 270 A.3d 362, 373 (N.J. 2022) (holding that state public records withholding requirements "does not limit the right of access to government records under the common law").
[24] 438 U.S. 1 (1978).
[25] *Id.* at 15 (plurality opinion).
[26] *Id.* at 38 (Stevens, J., dissenting).
[27] *See* Schafer, *supra* note 2, at 1435 (quoting *Media Right of Access*, 92 HARV. L. REV. 174, 178 (1978)).
[28] *Id.* (quoting *Media Right of Access*, 92 HARV. L. REV. at 184).
[29] *Id.* (quoting *Media Right of Access*, 92 HARV. L. REV. at 184–85).
[30] 443 U.S. 368 (1979).
[31] *Id.* at 392–93.
[32] *Id.* at 404–05 (Rehnquist, J., concurring).

A year after *Gannett Co., Inc.*, in *Richmond Newspapers, Inc. v. Virginia*, seven Justices agreed for the first time that despite the plurality opinion in *Houchins* the First Amendment guarantees some level of access to government information—in that case, access to a criminal trial.[33] And, two years later, in *Globe Newspaper Co. v. Superior Court*, a majority of the Court held that the First Amendment encompassed a right of access to certain government information (again, a criminal judicial proceeding) that "ensure[d] that the individual citizen can effectively participate in and contribute to our republican system of self-government."[34]

Ever since, a dispute has existed as to whether *Richmond Newspapers/Globe Newspaper* controls questions over a right of access to government information or whether the *Houchins* plurality does. If the *Richmond Newspapers/Globe Newspaper* controls, then the access right will be found to attach (1) whenever there is a "tradition of accessibility" and (2) where "public access plays a significant positive role in the functioning of the particular process in question."[35] (This is called the "history-and-logic" or "history-and-experience" test.) If a broad reading of *Houchins* controls (one contrary to Chief Justice Roberts' narrow views), the odds are that no right of access will be found to exist because the plurality said that there is no "First Amendment guarantee of a right of access to all sources of information within government control."[36]

Generally speaking, the Second, Third, Sixth, Eighth, Ninth, and Eleventh Circuits have all found that the *Richmond Newspapers/Globe Newspaper* line of cases control challenges to a denial of public access to government information to the exclusion of *Houchins*.[37] As a result, these circuits have applied the history and logic test to all sorts of government records and proceedings to determine whether a constitutional right of access attaches: voter lists, agency records, police operations on public streets, a town planning meeting, administrative proceedings, horse roundups on federal lands, executions and information relating to them, deportation proceedings, and judicial review boards, among others.

For example, in *Whiteland Woods, L.P. v. Township of West Whiteland*, the Third Circuit invoked the Court's observation in *Globe Newspaper* that "a 'major purpose of [the First] Amendment was to protect the free discussion of governmental affairs.'"[38] Applying that logic, the court concluded that the plaintiff had a "constitutional right of access to the Planning Commission meeting."[39] In so holding, it found that whether such a right existed depended on whether the history and logic test from the *Richmond Newspapers/Globe Newspaper* was

[33] *See generally* 448 U.S. 555 (1980).
[34] 457 U.S. at 604.
[35] *Press-Enterprise Co. v. Superior Ct.*, 478 U.S. 1, 8 (1986) ("*Press-Enterprise II*").
[36] 438 U.S. at 9.
[37] *See, e.g.*, *Wellons v. Comm'r*, 754 F.3d 1260 (11th Cir. 2014); *Leigh v. Salazar*, 677 F.3d 892 (9th Cir. 2012); *N.Y. Civ. Liberties Union v. N.Y.C. Transit Auth.*, 684 F.3d 286 (2d Cir. 2012); *Cal. First Amend. Coal. v. Woodford*, 299 F.3d 868 (9th Cir. 2002); *Detroit Free Press v. Ashcroft*, 303 F.3d 681 (6th Cir. 2002); *Cal-Almond, Inc. v. Dep't of Agric.*, 960 F.2d 105 (9th Cir. 1992).
[38] 193 F.3d 177, 180 (3d Cir. 1999) (quoting *Globe Newspaper Co.*, 457 U.S. at 604).
[39] *Id.* at 180–81.

satisfied.[40] And, it reframed *Houchins* not as setting forth a general rule that no right of access existed but as not presenting a context that satisfied the later-adopted two-part test.[41]

On the other side of the ledger, the First, Fourth, Fifth, Seventh, Tenth, and D.C. Circuits have found that *Houchins* plurality controls over the opinions in *Richmond Newspapers/Globe Newspaper*.[42] These courts have "seriously question[ed] whether *Richmond Newspapers* and its progeny carry positive implications favoring rights of access outside the criminal justice system."[43] Some have gone further to say, despite *Houchins'* status as a plurality opinion, that the "*Supreme Court* has ruled that the First Amendment does not 'guarantee the public a right of access to information generated or controlled by government,'" when, in fact, it never has.[44]

If the access right is found to attach to particular government information, whether a restriction on access to information can survive constitutional scrutiny will depend on four factors: (1) there must be a substantial probability of prejudice to a compelling interest;[45] (2) there must be no alternative to closure that will adequately protect the threatened interest;[46] (3) any restriction on access will effectively protect against the threatened harm;[47] and (4) any restriction on access must be narrowly tailored.[48] Because this test is fact-sensitive, where the access right attaches, access may not properly be restricted (whether as a discretionary or mandatory matter) without findings of fact satisfying each of the four factors.[49] As a result, requiring the automatic sealing of proceedings or records raises serious First Amendment issues. This is especially so where there is no empirical support for the claim that automatic sealing will advance the interests intended to be protected by such sealing.[50]

In sum, while there is a circuit split over when the right of access applies, some courts have found government information like agency records potentially subject to a First Amendment right of access. While one individual at the December 6 meeting questioned why more constitutional access claims have not been made if that is the case, such claims have been raised and courts have applied the history and experience test to determine whether such records are subject to a right of access.[51] This is to say nothing of state constitutional challenges (or those

---

[40] *Id.* at 181.
[41] *Id.* at 182; *see also First Amend. Coal. v. Jud. Inquiry & Rev. Bd.*, 784 F.2d 467 (3d Cir.1986) ("*Richmond Newspapers* is a test broadly applicable to issues of access to government proceedings.").
[42] *See, e.g.*, *Fusaro v. Cogan*, 930 F.3d 241 (4th Cir. 2019); *Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937 (7th Cir. 2015); *Ctr. for Nat'l Security Studies v. Dep't of Justice*, 331 F.3d 918 (D.C. Cir. 2003); *Calder v. IRS*, 890 F.2d 781 (5th Cir. 1989).
[43] *See, e.g.*, *El Dia, Inc. v. Hernandez Colon*, 963 F.2d 488, 495 (1st Cir. 1992).
[44] *Fusaro*, 930 F.3d at 249 (emphasis added).
[45] *Richmond Newspapers, Inc.*, 448 U.S. at 580–81; *Press-Enterprise Co. v. Super. Ct.*, 464 U.S. 501, 510 (1984) ("*Press-Enterprise I*"); *Press-Enterprise II*, 478 U.S. at 13–14.
[46] *Press-Enterprise II*, 478 U.S. at 13–14; *Presley v. Georgia*, 558 U.S. 209, 213–16 (2010) (per curiam).
[47] *Press-Enterprise II*, 478 U.S. at 14.
[48] *Id.* at 13–14.
[49] *Id.*; *Press-Enterprise I*, 464 U.S. at 510.
[50] *Globe Newspaper Co.*, 457 U.S. at 609–10.
[51] *See, e.g.*, *Fusaro*, 930 F.3d at 250 (finding that a state statute limiting inspection of state voter lists "implicate[d] interests that are protected by the First Amendment"); *Speer v. Miller*, 15 F.3d 1007, 1010 (11th Cir. 1994) (finding that a constitutional challenge to a Georgia statute prohibiting the inspection of

based on the common law) to non-disclosure laws.[52] Thus, the RPIPR's viability could vary dramatically by jurisdiction.

b. Discriminatory Access to Public Records

Setting aside whether, generally, a First Amendment right of access to government information exists, courts have also found that the governmental provision of discriminatory access to government information presents its own First Amendment issues. To the extent that the RPIPR draws such lines, this separate line of case law might further undercut the RPIPR's viability.

While not the first case to discuss the issue of discriminatory access to information, the Supreme Court summarized much of its case law on the subject in *Sorrell v. IMS Health Inc.*[53] There, a group of data miners and pharmaceutical manufacturers challenged a Vermont statute restricting "the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual doctors."[54] These records were received by pharmacies when they processed prescriptions. Pharmacies then sold the records to data miners who would lease them to pharmaceutical companies that used them to inform their sales of drugs.

One argument Vermont raised in defending the statute was a twist on the Court's right of access jurisprudence. It argued that the law only regulated "access to information" rather than speech, and, under the Court's prior precedents like *Los Angeles Police Department v. United Reporting Publishing Co.*, presented no constitutional issue because governments can "decide not to give out [government] information at all without violating the First Amendment."[55] While the records were not government records in the traditional sense, Vermont asserted they were generated in compliance with a state law "so could be considered a kind of governmental information."[56]

The Court found "some support" for this argument in *United Reporting* but ultimately rejected it and Vermont's reading of that case. First, it clarified that *United Reporting* was "about the availability of facial challenges" to laws limiting access to information, and (contrary to the June

---

law enforcement records under certain circumstances was likely to succeed); *Dahlstrom*, 777 F.3d at 947 (rejecting claims that state law restricting access to driving records present a cognizable First Amendment injury); *Nation Magazine v. U.S. Dept. of Defense*, 762 F. Supp. 1558, 1572 (S.D.N.Y. 1991) (challenge to executive regulations limiting access to military battlefield); *Buzzfeed, Inc. v. Deputy Com'r*, No. 155278/2018, 2019 WL 2549587 (Sup. Ct., N.Y. Cnty. June 20, 2019) (applying history and logic test under First Amendment but rejecting constitutional challenge to withholding statute); *see also People v. Weinstein*, No. APL-2022-00112 (N.Y.) (pending motion to challenge as unconstitutional statutory provision requiring mandatory sealing of information relating to sexual assault victims); *Soc'y of Pro. Journalists v. Sec'y of Lab.*, 616 F. Supp. 569, 576 (D. Utah 1985) (right of access to administrative proceedings; "Without a first amendment right of access to some governmental information, our system of government by the people will not work.").

[52] *See, e.g.*, *Great Falls Tribune Co. v. Great Falls Pub. Schs.*, 841 P.2d 502 (Mont. 1992) (holding unconstitutional public meetings regulation permitting closed session for certain discussions).

[53] 564 U.S. 552 (2011).

[54] *Id.* at 557.

[55] *Id.* at 556; *see also L.A.P.D. v. United Reporting Publ'g Co.*, 528 U.S. 32 (1999).

[56] *Sorrell*, 564 U.S. at 567–68.

15 Supplemental Response Memo's suggestion) acknowledged that *United Reporting* "did not rule on the merits of any First Amendment claim."[57]

An "even more important reason" for distinguishing *United Reporting*, the Court wrote, was that the "plaintiff in *United Reporting* had neither 'attempt[ed] to qualify' for access to the government's information nor presented an as-applied claim in this Court."[58] Thus, the Court in that case "assumed that the plaintiff had not suffered a personal First Amendment injury."[59] *Sorrell* was different because the respondents claimed the non-disclosure statute burdened "their own speech."[60] This argument, the Court said, found support in the individual opinions in *United Reporting* asserting that selective government disclosures of information "can facilitate or burden the expression of potential recipients and so transgress the First Amendment."[61] The Court went on to strike the Vermont law down in *Sorrell*.

The Fourth Circuit's recent ruling in *Fusaro v. Cogan* shows how this type of claim has evolved. In *Fusaro*, the plaintiff, a Virginia resident, challenged a portion of Maryland's election law that prohibited anyone but registered Maryland voters from accessing a list of registered voters in the state.[62] It also limited the use of the list to the electoral process. The panel in *Fusaro* found that *Houchins* controlled—not *Richmond Newspapers/Globe Newspaper*, which it said provided only a "limited exception" to *Houchins*.[63] Still, the panel found that the law's discriminatory disclosure scheme, which limited disclosure to Maryland residents alone, implicated the First Amendment.[64] *First*, the voter list was "closely tied to political speech, which generally receives the strongest First Amendment protection."[65] Unlike *Houchins* and *United Reporting*, the voter list had a "direct relationship to political speech" and "an explicit connection to 'the electoral process.'"[66] That the list was "sufficiently intertwined with political speech" meant that laws "concerning its distribution are not immune to constitutional scrutiny."[67]

Second, the law was both content-based *and* speaker-based because it limited the use of the list for the "electoral process" and also limited the distribution of the list to Maryland voters.[68] "[S]uch restrictions," the panel said, "are typically subject to heightened scrutiny."[69] The court admitted it knew of no case where such restrictions were found to be onerous enough to "overcome the general principle that there is no First Amendment right to such information," but "neither the Supreme Court in *Houchins* nor any appellate court applying that decision has been

[57] *Id.* at 568.
[58] *Id.* (quoting *United Reporting*, 528 U.S. at 41).
[59] *Id.* at 569.
[60] *Id.*
[61] *Id.*
[62] *Fusaro*, 930 F.3d at 244.
[63] *Id.* at 250.
[64] *Id.*
[65] *Id.*
[66] *Id.* at 251.
[67] *Id.* at 252.
[68] *Id.* at 252–53.
[69] *Id.* at 250.

faced with a situation where the government provided information only to a discrete group for limited purposes, let alone in an overtly political context."[70]

Finally, "Supreme Court precedent indicate[d] that suspect conditions on access to government information may be subject to First Amendment scrutiny."[71] Relying on the concurring and dissenting opinions in *United Reporting*, the panel explained that "eight justices in *United Reporting* 'recognized that restrictions on the disclosure of government-held information can facilitate or burden the expression of potential recipients and so transgress the First Amendment.'"[72]

As a result of these three considerations, the panel held that "a First Amendment claim that challenges suspect conditions on access to government information must be available": "We conclude . . . that the List is a means of political communication, and the combined effect of the content- and speaker-based restrictions contained in [the law] present a sufficient risk of improper government interference with protected speech that Fusaro may challenge [the law] in federal court."[73] Other courts have embraced this reasoning as well.[74]

Consistent with this precedent, the Committee would need to consider the basis on which the RPIPR makes distinctions between various kinds of requesters. While a carve out for journalists may well implicate this case law, a carve out for newsgathering broadly defined may not as it might be less likely to be considered a content- *and* speaker-based restriction. At any rate, even were the Committee to consider a carve out for journalists as a profession (as opposed to a newsgathering carve out) there is a basis to treat journalists differently from members of the public without running afoul of "speaker-based restriction" concerns.

This would not be a special dispensation for the press but rather a recognition that the press acts as a surrogate for the public and any benefit to the press inures to the benefit of the public. Without the press, any individual member of the public would not have the time nor resources to "obtain for himself 'the information needed for the intelligent discharge of his political responsibilities.'"[75] As the Supreme Court explained, the press acts as the "'eyes and ears'" of the public that contributes to the "remedial action in the conduct of public business."[76]

Thus, while members of the Court at times maintained that the press is owed no special access under the First Amendment, the Court has admitted that, in practice, the press *has been accorded special treatment*.[77] In *Richmond Newspapers*, for example, the Court recognized that the press

---

[70] *Id.* at 253.
[71] *Id.* at 250.
[72] *Id.* at 254 (quoting *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 569 (2011)).
[73] *Id.* at 255–56.
[74] *See, e.g.*, *Boardman v. Inslee*, 978 F.3d 1092, 1098 (9th Cir. 2020).
[75] *Gannett Co.*, 443 U.S. at 398 (Powell, J., concurring).
[76] *Houchins*, 438 U.S. at 8 (plurality opinion).
[77] *See, e.g.*, *Houchins*, 438 U.S. at 16 ("the media have no special right of access to the Alameda County Jail different from or greater than that accorded the public generally."). *But see* Genevieve Lakier, *The Non-First Amendment Law of Freedom of Speech*, 134 HARV. L. REV. 229, 2231–32 (2020) ("[S]peakers and listeners can, and sometimes do, receive more protection for their speech, press, and expressive

is often "provided with special seating and priority of entry so that they may report what people in attendance have seen and heard."[78] And in *Houchins*, a plurality of justices agreed that the press "required access" to the government information at issue there "on a more flexible and frequent basis than" the public.[79] This included the right, disallowed to the public, to record audio and video.[80] Lower courts have followed suit.[81]

c. Prohibitions on Access as Restrictions on Speech

In drafting the RPIPR, this Committee must also consider the implications such a law might have on the First Amendment rights of speech and of the press—not only the First Amendment right of access. Although there was a suggestion at the December 6 meeting that such an issue is beyond the Committee's charge, ignoring it would be seriously misguided. Instead, the Committee must consider these issues now and incorporate safeguards against the use of the RPIPR to burden constitutionally protected speech.

The risk that the RPIPR could infringe directly on freedom of speech or of the press is not theoretical—it is already happening with similar laws. In *Kratovil v. City of New Brunswick*, journalist Charlie Kratovil began investigating whether a New Brunswick law enforcement officer who retired with a pension and was rehired on salary months later (in addition to his pension) remained a resident of New Brunswick.[82] When Kratovil asked Director of the New Brunswick Police Department Anthony Caputo, the subject of Kratovil's investigation, about this, Caputo replied, "The public release of a law enforcement officer's place of residence is protected under Daniel's Law," New Jersey's version of the RPIPR.

Kratovil eventually confirmed that Caputo lived hours away in Cape May. He obtained Caputo's voter registration address from a government entity (despite Daniel's Law and in reliance on countervailing authority in New Jersey) that included Caputo's home address. Kratovil took this information to a city council meeting and named the street (but not the house number) where Caputo lived in Cape May. As a result, New Brunswick refused to disclose the unedited video of the city council meeting on the basis that the recording would disclose the address of a police officer. Worse, purportedly because of Daniel's Law, the city allegedly redacted the entirety of the city council discussion about Caputo's residence.

---

association under state constitutional law, state and federal statutory law, and state common law than they do under the First Amendment.").

[78] *Gannett Co.*, 443 U.S. at 398 (Powell, J., concurring).

[79] *Houchins*, 438 U.S. at 18 (Stewart, concurring in the judgment); *see generally id.* at 19 (Stevens, J., dissenting).

[80] *Id.* at 18 (Stewart, concurring in the judgment).

[81] *State v. Lashinsky*, 404 A.2d 1121, 1128 (N.J. 1979) (explaining that a "majority of the voting members" in *Houchins* "recognized the First Amendment's concern that the public be optimally informed could in some instances render unreasonable restraints upon the scope of access to members of the press even where it would not be unreasonable to exclude the general public"); *see also Hanrahan v. Mohr*, 2017 WL 1134772, at *5 (S.D. Ohio Mar. 24, 2017), *aff'd*, 905 F.3d 947 (6th Cir. 2018).

[82] No. A-000216-23T1 (N.J. App. 2023) (pending litigation).

When officials learned that Kratovil was going to publish a news report, Caputo himself sent a cease-and-desist letter citing Daniel's Law and cautioning Kratovil against doing so. That letter is annexed here as **Exhibit A**. New Jersey's Daniel's Law requires that upon notice "a person, business, or association shall not disclose or re-disclose on the Internet or otherwise make available, the home address or unpublished home telephone number of any covered person, as defined in subsection d. of this section."[83] It also provides for civil and criminal penalties for those who disobey. On the civil side, it allows for liquidated damages of $1,000 per violation, punitive damages, and attorney's fees.[84] A "reckless violation" of the law "is a crime of the fourth degree," while a "purposeful" one "is a crime of the third degree."[85]

As a result of being threatened with penalties by the subject of his reporting, Kratovil was forced to obtain legal counsel to vindicate his right to publish his reporting on Caputo's residence. The trial court, however, found against Kratovil. It held that Kratovil was a journalist who had legally obtained the information. It also held that Caputo's residence was a matter of public concern. But it concluded that Caputo's home address was not a matter of public concern and, on that basis, dismissed the complaint. That decision is subject to appeal.

That decision is wrong on the law. State action "to punish the publication of truthful information seldom can satisfy constitutional standards."[86] If "a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order."[87] This is known as the *Daily Mail* principle and is the product of an unbroken line of Supreme Court cases dating back to the 1970s.[88] In 2001, the Court reaffirmed this principle in *Bartnicki v. Vopper.*[89]

Interests the Court has found insufficient to overcome the *Daily Mail* principle include: the privacy interest of the father of a rape victim in his daughter not being named in the press[90]; fair trial rights of a boy charged with murder[91]; protecting the reputation of judges or maintaining the integrity of the courts[92]; protecting the anonymity of juvenile offenders so as to further the likelihood of rehabilitation[93]; and even the physical safety of rape victims and the "goal of encouraging victims of such crimes to report these offenses without fear of exposure."[94]

Members of the Committee have admitted that information sought to be protected by the RPIPR is available either in hardcopy from the government or through third-party data broker websites.

---

[83] N.J. Stat. Ann. § 56:8-166.1(a)(1).
[84] *Id.* § 56:8-166.1(c).
[85] N.J.S.A. 2C:20-31.1(d).
[86] *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97, 102 (1979).
[87] *Id.* at 103.
[88] *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); *Oklahoma Pub. Co. v. District Ct.*, 430 U.S. 308 (1977); *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978); *Daily Mail Publishing Co.*, 443 U.S. 97 (1979); *The Florida Star v. B.J.F.*, 491 U.S. 524 (1989).
[89] 532 U.S. 514 (2001).
[90] *Cox Broadcasting Corp.*, 420 U.S. at 495.
[91] *Oklahoma Pub. Co.*, 430 U.S. at 1046.
[92] *Landmark Communications, Inc.*, 435 U.S. at 841.
[93] *Daily Mail Publishing Co.*, 443 U.S. at 104.
[94] *The Florida Star*, 491 U.S. at 537.

So even if one accepts that physical safety is a compelling interest, this does not end the inquiry. The Court, for example, has recognized that the physical safety of rape victims is a "highly significant interest[.]"[95] But where a law is underinclusive—like the RPIPR would be in light of the public availability of the information from third parties—the law cannot be said to serve its purpose and, therefore, will be found invalid.[96]

Rather than force this question into litigation, however, the Committee should make clear in any draft that the RPIPR's privacy protections may not be used as a sword to prevent the publication of newsworthy information lawfully obtained and that no penalties, civil or criminal, nor injunctive relief against the publication of this information, can be inferred from the RPIPR. The point of the RPIPR is, after all, to protect individuals from having their "private" information disclosed by the government; not to protect covered individuals from critical news reporting.

III. THE PRACTICAL CONSEQUENCES OF THE RPIPR

This memo has focused on First Amendment issues attendant to laws like the RPIPR. But there are other practical issues that this Committee should consider as well while drafting any such law. Initially, the access restrictions contemplated by the RPIPR—restrictions that make reporting more difficult—could not come at a worse time. Journalism, and especially local journalism, is more precariously positioned today than at any time since the nineteenth century. More than half of counties around the country have no or very limited access to local reporting.[97] Local newspapers are dying off at a clip of 2.5 per week, and this past year 130 have closed. Since 2005, of 8,900 newspapers then existing, only 6,000 still exist. And the "country has lost almost two-thirds of its newspaper journalists, or 43,000, during that same time."[98]

While members of the Committee suggested at the December 6 meeting that the RPIPR is only supposed to make it more difficult to obtain subject records, the friction that RPIPR puts into the system might mean that these overburdened newsrooms simply decide to forego attempting to clear RPIPR's hurdles. Because it is efficient and cost effective to engage in digital public records reporting, especially in scaled back newsrooms, removing this resource means time and money—two resources many newsrooms do not have to spare. Not every newsroom can afford to put their reporters on a plane and send them across the country to rummage through public records, like ProPublica did during its investigation into Justice Thomas.

Second, at the December 6 meeting, some members suggested that the RPIPR might be narrowly drafted to prevent intrusion into newsgathering and address attendant concerns from news organizations and open government groups. But no matter how narrowly the Committee drafts the RPIPR, underfunded and understaffed government clerk's offices will react by discontinuing entirely digital or other access to public records rather than sort through mountains of records to remove specific kinds of information about specific individuals covered by RPIPR.

---

[95] *Id.*
[96] *Id.* at 541.
[97] *More than half of U.S. counties have no access or very limited access to local news*, NORTHWESTERN UNIVERSITY, MEDILL (Nov. 16, 2023).
[98] *Id.*

Again, this is not theoretical—it is already happening. These concerns were raised in the Study Committee by more than two-dozen government transparency organizations in a June 17, 2022 letter. Oddly, this letter does not appear to have been included in the March 23, 2023 recommendation letter from the Study Committee. This is a significant omission, because the Study Committee memo inaccurately asserts that open government organizations' concerns over the RPIPR, were "speculative in nature." This is wrong. The June 17 letter provided specific, concrete examples of existing laws that have resulted in harms that the open government organizations identified to the Committee.

As the June 17 letter, which is annexed here as **Exhibit B**, explained, in West Virginia, local officials decided that they were unable to comply with West Virginia's redaction law by way of narrow redactions and, instead, "opted to entirely eliminate public access to any address information in the court records system." And in Florida, a rule that required personal information to be redacted from court records was so burdensome that "many circuits began treating court records as presumptively closed to the public," raising significant legal issues and ultimately leading the Florida Supreme Court to retract the rule.

Other written comments from those opposed to the RPIPR were also omitted from the March 23 recommendation letter. This includes a November 28, 2022 letter from the Georgia First Amendment Foundation, which is annexed here as **Exhibit C**, and an October 14, 2022 letter from the Tennessee Coalition for Open Government, which is annexed here as **Exhibit D**. Among other things, these letters expressed concern over a lack of relevant stakeholder input, research, discussion of the practical implications of the RPRIPR, and empirical evidence linking personally identifiable information in government records to attacks on public officials.

Opponents of the RPIPR also pointed to New Jersey's experience with Daniel's Law, which, while adopted in 2020, has already had to be amended to deal with unintended consequences: the law created "uncertainties and unintended consequences making implementation extremely challenging for local governments."[99] This has real world effects. The Township of Verona took down its public access YouTube Channel "to comply with new state legislation . . . that protects members of the public from having their addresses known."[100] The Mercer County clerk said she would provide access to property records but apparently only to "real estate professionals" who will have to "register with the New Jersey Department of Banking and Insurance."[101]

Also, omitted from the March 23 recommendation letter was a memorandum from Richard Varn dated November 28, 2022, which discussed the practical security implications of the RPIPR and is annexed hereto as **Exhibit E**. As Mr. Varn explained:

> Redacting the very public and easily discovered fact of the addresses of public employees *is security theater*. It's widely known and acknowledged that one can find a person's address by numerous means. Further, the dark web also provides cheap complete profiles of persons gleaned from hacked data, data breaches,

[99] *Daniel's Law and Recent Clean-Up Legislation*, N.J. State League of Municipalities (Jan. 28, 2022).
[100] *Verona Municipal YouTube Channel Taken Down*, TAPINTO VERONA/CEDAR GROVE (Apr. 11, 2023).
[101] Janique Burke, *Mercer County Clerk announces opportunity for real estate professionals despite Daniel's Law*, TRENTON JOURNAL (Apr. 12, 2023).

> malware, apps with loose privacy policies, and data from many, many sources in common circulation. It is also relevant to consider those who are willing to go beyond the stage of thought to actual action to harm, harass, threaten, and stalk a public employee are not in any way likely to be deterred by weak security theater level measures. . . .
>
> During ULC discussions on the redaction topic, it has been stated that putting in barriers to finding a person's address from public records will slow and deter those who wish to harm or harass public employees from doing so. As noted above, those who are determined to do harm or harass are likely substantially more motivated to get the information they need and therefore the redaction barrier is not effective against them. But it is effective in limiting those who want to use that data for informational and beneficial purposes.

No matter how narrowly this Committee drafts the RPIPR, there is a serious risk that the result, if the law is adopted around the country, will be that clerks and other public officials will not invest the substantial resources required to implement the narrow drafting. Instead, they will simply remove troves of records from public access irrespective of whether they contain covered information. And, worse, doing so will do little to advance safety but much in the way of harming the public interest in holding officials accountable by making it more difficult for cash-strapped local journalists to do their jobs.

CONCLUSION

The RPIPR raises a host of First Amendment, journalistic, and good governance issues. These are not academic questions. The information that may be subject to the RPIPR has formed the basis of serious public interest reporting that has called to account everyone from Supreme Court Justices to local police officers. Adopting the RPIPR in whatever form will make this kind of reporting more difficult and sometimes impossible. Worse, the Committee is considering pulling a curtain of secrecy over this information *without any empirical evidence* demonstrating that these kinds of secrecy laws have made public servants safer. That is troubling for a number of reasons, including that observers to the Study Committee repeatedly requested that such an analysis be undertaken.

As I and multiple other observers have conveyed to the Study Committee and now this Committee, we believe that the physical safety of public officials is of the utmost importance. But we also believe the RPIPR is a misguided effort that will not address that serious issue and will instead result in unintended consequences that will shield corruption and deprive the public of important information about their public officials. On this basis, this effort should be abandoned or remanded to the Study Committee to review empirical evidence relating to the efficacy of these kinds of laws. Absent abandonment or remand, the RPIPR must be drafted exceedingly narrow to prevent intrusion on protected constitutional rights and avoid undermining public accountability and oversight.

Exhibit A

NEW BRUNSWICK POLICE DEPARTMENT

25 KIRKPATRICK STREET • POST OFFICE BOX 909
NEW BRUNSWICK, NEW JERSEY 08903
Communications 732.745.5200 / Facsimile 732.565.7544 / Web Page www.cityofnewbrunswick.org

ANTHONY A. CAPUTO
Director of Police
732.745.5178

JT Miller
Deputy Director of Police
732.745.5259

Vincent Sabo
Deputy Chief of Police
732.745.5193

May 4, 2023

VIA REGULAR & CERTIFIED MAIL

Mr. Charles Kratovil
143 Suydam Street
New Brunswick, NJ 08901

RE: NOTICE Pursuant to N.J.S.A. 2C:20-31.1& N.J.S.A. 56:8-166.1

Dear Mr. Kratovil:

On Wednesday, May 3, 2023, you published and/or announced my home address at a public meeting of the New Brunswick City Council. Kindly accept this letter a written notice as required by the above referenced statute.

Pursuant to **N.J.S.A. 2C:20-31.1** and **N.J.S.A. 56:8-166.1,** and as an authorized and otherwise covered person whose home address and unpublished home telephone number are not subject to disclosure, I do hereby request that you cease the disclosure of such information and remove the protected information from the internet or where otherwise made available.

I trust you will be guided accordingly.

Very truly yours,

Anthony A. Caputo

Cc: AP Christopher Kuberiet, MCPO
Mr. TK Shamy, City Attorney
Mr. Steven Altman, Esq.

Exhibit B

National Freedom Of Information Coalition
NFOIC
P.O. Box 405
Williamsburg, VA
23187

GEORGIA FIRST AMENDMENT FOUNDATION
GFAF
7742 Spalding Drive
Suite 209
Norcross, GA 30092

June 17, 2022

Tim Schnabel, Esq., Executive Director
Vince DeLiberato, Esq., Committee Chair
Barbara Ann Bintliff, Esq., Committee Reporter
Uniform Law Commission
111 N. Wabash Avenue, Suite 1010
Chicago, Illinois 60602
Delivered via email: TSchnabel@uniformlaws.org, vdeliberato@palrb.us, bbintliff@law.utexas.edu

RE: Preliminary recommendations from Uniform Law Commission study committee on Redaction of Personal Information from Public Records

Dear Mr. Schnabel, Mr. DeLiberato and Ms. Bintliff:

This letter is on behalf of 26 government transparency organizations concerning the work of the Uniform Law Commission's study committee on Redaction of Personal Information from Public Records. We understand the committee to be considering recommending that model legislation be drafted to provide for per se redaction from public records of information related to public employees, including judicial or law enforcement personnel, and a right for domestic violence victims and certain other groups to request redaction of personal information from public records. Our organizations have reviewed the study committee's latest memorandum and have attended one of the committee's recent meetings.

We write to make the Uniform Law Commission and the study committee aware of a number of concerns that our organizations have with the committee's proposal.

First, the type of legislation being considered by the Uniform Law Commission is highly likely to result in serious unintended reductions in access to public records. Such negative consequences have already occurred following the implementation of similar laws passed across the country as part of the growing trend to limit access to information that could identify public officials and government employees. While that trend may have initially been motivated by a desire to fight back against doxing and increase safety of government employees and their family members, the resulting laws have already created a host of problems and have led to a decrease in government transparency.

For example, the West Virginia legislature passed a Daniel's Law in 2021 intended to shield private information of public employees, including judges and law enforcement. A number of court systems in the state have concluded that they cannot comply with the law through narrow redactions, and instead have opted to entirely eliminate public access to any

address information in the court records system, including the addresses of criminal defendants and the office addresses of public employees.[1]

Florida courts have taken a similar approach to complying with rules designed to protect personal information in public records. In 2010, the Florida Supreme Court adopted amendments to the state rules governing the court system. The amendments required clerks' offices to review court records and redact any personal information therein prior to disclosing the records publicly. The rule was disastrous for public access, creating such delays and administrative headaches that many circuits began treating court records as presumptively closed to the public. Years of complaints from the public, government employees, and the media led the Florida Supreme Court to retract the rule, effective July 2021.[2]

The type of overreactions seen in West Virginia and Florida are not outliers. Indeed, according to a 2021 report from the National Freedom of Information Coalition, "the greatest threats to government transparency today are legal exemptions primarily focused on protecting individual privacy."[3] In our experience, many (if not most) government agencies are either unable or unwilling to carry out a tailored implementation of laws like the legislation that the Uniform Law Commission is considering. Redacting government employees' private information, such as cell phone numbers or home addresses, comes with high administrative burdens that most government agencies, particularly local agencies like police departments or city governments, do not have the resources to absorb. Furthermore, it may not even be possible to achieve such targeted redactions in many government databases.

Our expectation, as reinforced by real-world examples including those in West Virginia and Florida, is that agencies faced with high administrative burdens or with less nimble computer systems will take one of two approaches to sweeping redaction requirements: (1) like the courts in West Virginia or Florida, they will be overinclusive and opt to shield large amounts of data from the public; or (2) they will offload compliance costs to members of the public by charging anyone who requests records for the time it takes a government employee to go through all requested records and personally input appropriate redactions.[4]

---

1 *Court Overreacting to Daniel's Law*, The Dominion Post (May 14, 2022), *available at* https://www.yahoo.com/news/editorial-court-overreacting-daniels-law-111800848.html.

2 Max Marbut, *Filers will be responsible for redacting confidential information in certain cases*, Jax Daily Record (June 22, 2021), https://www.jaxdailyrecord.com/article/court-document-rules-changing-july-1.

3 *States of Denial,* National Freedom of Information Coalition (March 15, 2021), *available at* https://drive.google.com/file/d/1L8yJY1Lrufg-rfqxFBqQfsi54BUhsBRK/view

4 Redaction of public records already results in significant delays and high costs for the production of public records. Often, these delays and costs are prohibitive, leading the requester to abandon their efforts and never obtain the records they need. We expect that laws requiring redaction of private information of government employees, even in records that do not identify those employees by job title, will greatly increase the delays and costs associated with redactions, given the many contexts in which such laws would apply.

Neither outcome will make government employees any safer but will only serve to meaningfully decrease access to information that should be public.

Second, even where government agencies narrowly and appropriately implement legislation requiring redaction of private information of public employees, there is still a real cost to such redactions. Such laws make it difficult to confirm identities of public employees, for example, where a state official has the same name as someone arrested for drunken driving.[5] In other words, the more barriers there are to journalists or members of the public linking a public official's name to personally identifying information, the greater the strain on accountability and oversight of those officials.

We encourage the Uniform Law Commission to consider the legitimate—and valuable—uses of the type of information that would be shielded from public view as a result of the model legislation being studied by the committee. In addition to the high value of such information in fostering oversight and accountability, such information assists the real estate industry and the public in powering title searches and in making insurance and financing determinations, and it enables consumer-focused resources like Zillow, Trulia and Rocket Mortgage, among other beneficial resources.

Third, as an alternative to the type of legislation being studied, the Uniform Law Commission should consider other measures that would not undermine government transparency. Redaction of personal information from public records would provide government officials a false sense of security and prove ineffective as a security measure, because bad actors are more likely to discover an official's whereabouts through already available sources, nefarious or legitimate. In many small communities, redacting personal identifiers would have no practical effect, because people tend to know who works for the local government and where they live.

Laws that directly target imminent and actual threats to government officials are more effective at protecting those officials without imposing the costs that come with shielding information from public access and giving government agencies a tool to seriously curtail existing transparency laws.

In our view, the existing proposal under consideration in the study committee would result in harmful and unnecessary damage to the public's right to conduct oversight of the government. As the study committee continues its work, we encourage both the Uniform Law Commission and the committee to consider the issues raised in this letter and to engage with government transparency advocates, including the signatories to this letter, to provide input on the committee's work.

---

[5] *States of Denial*, *supra* n.2, at 2.

Sincerely,

Todd Fettig
Executive Director
National Freedom of Information Coalition

Sarah Brewerton-Palmer
Legislative Chair
Georgia First Amendment Foundation

Better Government Association of Illinois
Colorado Freedom of Information Coalition
Connecticut Foundation for Open Government
D.C. Open Government Coalition
Espacios Abiertos
Florida Center for Government Accountability
Freedom of Information Foundation of Texas
Idahoans for Openness in Government
Iowa Freedom of Information Council
It's The People's Data
Kentucky Open Government Coalition
Louisiana Press Association
Maine Freedom of Information Coalition
Missouri Sunshine Coalition
Nevada Open Government Coalition
New England First Amendment Coalition
New Mexico Foundation for Open Government
Open Oregon
Pennsylvania Freedom of Information Coalition
Public Affairs Research Council of Louisiana
Tennessee Coalition for Open Government
Virginia Coalition for Open Government
Washington Coalition for Open Government
Wisconsin Freedom of Information Council
Thomas Susman,
NFOIC Vice President
Open The Government steering committee chair

Exhibit C

GEORGIA FIRST AMENDMENT FOUNDATION
your right to know

Nov. 28, 2022

VIA EMAIL
Tim Schnabel, Esq., Executive Director
Vince DeLiberato, Esq., Committee Chair
Barbara Ann Bintliff, Esq., Committee Reporter
Uniform Law Commission
111 N. Wabash Avenue, Suite 1010
Chicago, Illinois 60602
TSchnabel@uniformlaws.org
vdeliberato@palrb.us
bbintliff@law.utexas.edu

RE: Preliminary recommendations from Uniform Law Commission study committee on Redaction of Personal Information from Public Records

Dear Mr. Schnabel:

I write concerning the work of the Uniform Law Commission's study committee on Redaction of Personal Information from Public Records. As the study committee continues its work, the Georgia First Amendment Foundation would like to offer insight into the existing open records law in Georgia and how it could be used as an alternative way of addressing the problems that gave rise to the study committee's work.

Georgia's Open Records Act contains two provisions that allow for (and in some cases, require) the withholding of personal information from public records—for example, by redacting home addresses—while still safeguarding public access to government records.

First, O.C.G.A. § 50-18-72(a)(20)(A) instructs government agencies to redact a host of personal information from public records, including "an individual's social security number, mother's birth name, credit card information, debit card information, bank account information, account number, utility account number, password used to access his or her account, financial data or information, insurance or medical information in all records, unlisted telephone number if so designated in a public record, personal email address or cellular telephone number, day and month of birth, and information regarding public

7742 Spalding Drive, #209 • Norcross, GA 30092
678-395-3618 • info@gfaf.org • www.gfaf.org

"Because public men and women are amenable 'at all times' to the people, they must conduct the public's business out in the open."
— The late Charles L. Weltner Sr., Chief Justice, Georgia Supreme Court, *Davis et al v. City of Macon* (1992)

utility, television, internet, or telephone accounts held by private customers, provided that nonitemized bills showing amounts owed and amounts paid shall be available." The provision then enumerates a list of scenarios where the agency should refrain from redacting such personal information, including: when it appears in court records; when journalists are seeking the records in the course of their work; when government employees are seeking the records for official purposes; when so ordered by a court; when the individual whose personal information is in the record is requesting production; when it concerns a deceased person; when consumer reporting agencies are requesting records; or when it appears in criminal records. O.C.G.A. § 50-18-72(a)(20)(B).

Unlike the proposal being considered by the study committee, Georgia's redaction rule applies to every member of the public—not just preferred categories of public employees. This type of generally applicable provision ensures that everyone receives the same protection for their personal information. In addition, Georgia's exceptions to the redaction rule ensure that journalists can still obtain information that is necessary to do their jobs. As noted in the National Freedom of Information Coalition's June 17, 2022, letter to the ULC, the study committee's proposal is likely to seriously hinder journalists who have a legitimate need for personal information to properly scrutinize the actions of public officials. The structure of O.C.G.A. § 50-18-72(a)(20) strikes a better balance between avoiding unnecessary disclosure of personal information while protecting the legitimate uses for such information.

Second, O.C.G.A. § 50-18-72(a)(21) provides that public disclosure of government records is not required for "[r]ecords concerning public employees that reveal the public employee's home address, home telephone number, personal mobile or wireless telephone number, day and month of birth, social security number, insurance information, medical information, mother's birth name, credit card information, debit card information, bank account information, account number, utility account number, password used to access his or her account, financial data and information other than compensation by a government agency, unlisted telephone number if so designated in a public record, and the identity of the public employee's immediate family members or dependents."

This exception to Georgia's general rule of access to public records provides broad protection to any public employee—not just certain categories of public officials, as contemplated by the study committee's proposal—and includes a comprehensive range of personal information. At the same time, this provision ensures that the public's right to access government records is not unnecessarily eroded by limiting its application only to records that "specifically identify public employees or their jobs, titles, or offices." *Id.* That limitation allows government agencies to more easily identify the records to which this exception applies. As the National Freedom of Information Coalition's letter pointed out, one of the problems with the study committee's proposal is that it would create administrative difficulty for government agencies trying to determine which records include information subject to a mandatory redaction requirement. This in turn will almost certainly lead to either delays in the production of open records or to overbroad enforcement that prevents access to entire categories of documents. Georgia has avoided these problems by cabining O.C.G.A. § 50-18-72(a)(21) to records that identify someone as a public employee and are thus easily identifiable for the government agency responding to an open record request. Notably, public employees who wish to have broader protection for their personal information are still protected by O.C.G.A. § 50-18-72(a)(20), just like the rest of the public.

Overall, the Georgia First Amendment Foundation believes that a uniform law on this topic would be detrimental to the public's right of access to public information across the country. Should the ULC and the study committee conclude that such legislation is necessary, then the Foundation encourages the ULC to consider the structure of Georgia's Open Records Act as a better way to address the concerns

animating this effort, without harming the public's right to know. We have appended a copy of Georgia's Open Records Act to this letter to allow you to review the provisions outlined above in more detail and in the full context of the law.

Please reach out to us if you have any questions about this letter; we would be happy to discuss Georgia's open records laws with you in more detail any time. My contact information is spalmer@caplancobb.com and (404) 596-5609. Or you may contact GFAF President Kathy Brister at kathybrister@yahoo.com and (404) 394-6103.

Regards,

Sarah Brewerton-Palmer
GFAF Legislative Chair

cc: Kathy Brister

Exhibit D

Oct. 14, 2022

Dear Members of the ULC Study Committee on Redaction of Personal Information,

This letter is to express concern about the initial determinations of the ULC Study Committee on Redaction of Personal Information from Public Records.

By way of introduction, I am the executive director of the Tennessee Coalition for Open Government, an organization that has tracked changes to our state's public records and open meetings laws for nearly 20 years. I speak to you as someone who is on the ground, in the field, with experience examining local public records issues and communicating with stakeholders that include government officials as well as journalists and regular citizens.

Perspective from the state level

The issue of residential addresses is not new. Our state, like many others, has laws that in some instances prevent access to residential addresses in public records for privacy purposes. For example, residential addresses of state, county and municipal employees in employment records are not open for inspection under our public records law.

Our state also has a process in which someone with a protective order from a court may have his or her residential information kept confidential upon presentation of the appropriate document to a records custodian.

Aside from the protective order process, none of our statutes allow redaction of residential addresses from *all* public records or from all government databases.

In other words, the Nashville water department would not be required to fulfill a public records request for the home addresses of all of its employees. But that does not exempt the water department manager from having his or her residential address available through property records and voter registration records, for example, just like any other citizen.

What is the committee's intent?

As I understand the committee's decisions so far, it plans to recommend that judges and law enforcement personnel be entitled to "per se redaction" of personally identifiable information (to include residential addresses and dates of birth) from *all* government databases and that this redaction would be "automatic," or, in other words, required to be carried out by the custodian.

I joined this committee as an observer rather late in the game and am struggling to correctly absorb what is meant by this.

At one point, I heard, but have not found affirmed in any memo, that the recommendation would apply only to electronic databases *that are accessible to the public via a government website*. This would be a significant distinction and should be made clear in the memos if that's the intent of the committee.

I also heard at one point that residential addresses in such databases would still be available upon a public records request. Again, this would be a significant distinction to make clear in the memos of the committee.

If the intention is to affect only government-operated online searchable databases, the only ones that I'm aware of in Tennessee are the county property assessor online databases. However, I believe it would be helpful for the committee to identify specific examples of databases that would fall under the ambit of the proposal. You need to know what you're affecting.

Regarding property assessor online databases, a new law was passed in Tennessee this year that allows a residential property owner to file a written request with the county property assessor to "unlist" their name in the ownership field of their primary residence, kind of like asking to unlist your phone number in the old phone books, but here, you're asking to unlist your name associated with an address. The new law does not allow an assessor to redact the owner's name anywhere else but in the online, public-facing database. Importantly, the owner's name in a property record would remain available upon a public records request. In addition, the law is permissive for property assessors. They are not required to fulfill "unlist" requests.

Workability of proposal so far

In the committee's latest memo, the "per se redaction" would be "automatic," but I am unclear whether it would require initiation by the person who is entitled to the redaction by contacting a custodian or whether it would require the records custodian to have a process to gather the names of all who are eligible and who become ineligible after they leave their position. Do they reach out to get lists of all law enforcement personnel (a very large group) and judges? And would this happen daily? Monthly? Annually?

In Tennessee's new law, the person requesting the redaction must initiate it. My understanding based upon a conversation with the executive director of Tennessee's association of property assessors is that anything requiring property assessors to annually gather information from multiple sources would be unmanageable.

Additionally, what *would* be available on a property record online, as envisioned by this committee? Would the name be redacted? That is not the recommendation so far by the committee. Redacting the address is the essence of the property record. In other words, you can't have a property record *without* the address. So would the entire record of that property simply be unavailable in the online database? And if that's the case, wouldn't a search on a city

street then, perversely, allow identification of the street numbers that are homes to judges and law enforcement simply by their omission, creating a precise map of the very homes one hoped to protect?

It's worth diving into the details and talking to people who handle these databases. These are consequential decisions and go to the workability and any imagined effectiveness of a proposed law.

Lack of stakeholder input and research

To that point, I've found nothing in the memos so far that suggests the committee has contacted a wider group of stakeholders — such as property assessor associations or managers of other government online databases, or those companies or professionals who regularly use online searchable databases.

The committee, according to the memo, made clear that security was the purpose, not privacy. Logically, it would be wise for the committee to hear from security experts.

For example, a security expert who has been tasked with reducing risk of home invasion for judges might place a greater priority on residential alarm systems, gated entries, and camera systems at the front door than on removing a property record from a property tax assessor's database.

Even more basic, the memos of the meeting contain no documentation of the stated problem that this legislation is intended to cure. From conversations I've heard, the perceived problem is that judges and law enforcement personnel are enduring violence in their homes at higher rates than other public officials who would not be included in this proposal, and possibly at higher rates than regular citizens who don't deserve such "per se" redaction.

If we're imagining, without any research or documentation, who faces the greatest threats from government online databases containing their address, I'd probably add school board members, young women, journalists and child protective services officers who take children from parents. It's an endless list when you are basing the decisions not on data, but on emotion and who happens to be in your circle of friends or cultural orbit.

Finally, do we really have reason to believe that removing an address from a government online property record would foil someone with criminal intent? In fact, of the home invasions of judges and police officers (if we had such data or research), how many have occurred because the person got the address from a government searchable database online as opposed to, say, following the person home or finding the address somewhere else online? On the latter, the horse has been out of the barn for quite some time. And still would be, even under this proposal, as data companies would continue to be able to purchase unredacted information from the government for resale.

Residential addresses can provide accountability

The National Freedom of Information does an excellent job of describing why access to residential addresses of public officials is important — and how a similar reactive law in New Jersey created a nightmare of costs and confusion — so I won't retread too much here.

But please keep in mind that home addresses have traditionally been considered routine directory information in our country. Even FERPA allows routine directory information, including home addresses of students, to be released.

Additionally, journalists have routinely used home addresses to expose public officials violating local laws, such as election eligibility or voting laws. Should the public be kept from knowing, for example, that former NFL running back Herschel Walker who is running for a U.S. Senate seat in Georgia still resides in Texas? Or that Mark Meadows, former chief of staff for President Donald Trump, registered to vote with a property address of a North Carolina mobile home where he did not live?

And what about tax delinquency lists? If other public and elected officials can be held accountable through access to residential information, why would judges and law enforcement officials, like the locally elected district attorney, get to hide behind a so-called security measure?

Better research is needed

In sum, I urge the committee to consider the wisdom of recommending a model law or uniform legislation on this topic without proper research. This is a complicated issue and a recommendation from the Uniform Law Commission could have a negative effect on multiple stakeholders in exchange for what? A dubious effect on a problem that has not, even yet, been properly documented and examined?

I trust that the procedures of the Uniform Law Commission will deliver on what is promised on its website: “meticulous consideration of every act.” And I urge a rethinking of the next steps toward a proposed law that even the committee’s chair acknowledged on the most recent call would offer a “false sense of security.”

Thank you for your consideration,

Deborah Fisher
Tennessee Coalition for Open Government

Exhibit E

Enhancing Security for Public Employees

Draft 5
Richard Varn
11/28/2022

Introduction

Note: This is a work in progress. It is intended to facilitate discussion about how best to enhance security of public employees.

The purpose of this short paper is to inform the ULC Committee on Redaction of Public Records of possible ways to address growing threats against public employees. The US Federal, State, and Local Governments have responded to threats and incidents in recent years by adopting robust threat analysis/planning/response laws, rules, plans, budgets, training, programs, governance, and operational entities. These efforts fall into two main categories. The first is infrastructure including government buildings as well as public and private assets like transportation assets, power grids, water treatment plants, and dams. The second is digital assets and cybersecurity. While both categories address personnel security to some extent, neither of them focusses on protecting employees and officials nor do they fully reflect the current threats that go beyond the physical workplace and government computer systems. The problem is that most of the effort has gone into protecting the buildings. It was assumed that was the primary way to protect the people who work in them. However, this should now be seen as insufficient given the current environment and threat matrix.

The existing security regimens for physical and cyber security have the right methodologies to address the broader threats to personnel. What is needed is a model approach to making sure threats to personnel are properly included in threat management and risk reduction and that the range of methods and countermeasures is expanded and deployed to address the wider range of current and emerging threats.

To advance the discussion of a model approach, this paper will review how the current methods and best practices for addressing threats work. The paper will identify ways to adapt these methods to better address personnel security. Finally, it will explore the options for improving protection for personnel, their families, and their associates that draws on practices from both the public and private sector.

Brief Threat Management Overview

There are five distinct elements to threat management methods: survey of threats, assessment of threats, determination of countermeasures, decisions on risks to accept and those to address

with available or new resources, and evaluation of maturity, quality, and efficacy of the methods and outcomes.

Survey of Threats

An all-threats approach begins with a wide view of the possible threats. The threats can be individual and combinatory (combining a cyber-attack with a physical one for example) and should be part of an overall risk assessment process for an entity. In other words, do not survey threats in isolation but in the context of the jurisdiction and its overall risks as this allows for better alignment and prioritization of responses later. The threats and threat targets are typically listed within categories. Several of these threat categories and threat targets are beyond the scope of this analysis such as the threat category of natural disasters and the threat target of public utilities. The threat categories of interest here are crime (physical and cyber), civil disturbance, reputational harm, and tortious harm to persons and property. The threat targets of concern are people, buildings/facilities where government employees work and live, and goodwill/public trust.

Assessment and Prioritization of Threats

Risk managers have time-tested methods of enumerating and prioritizing threats. These methods have been honed and committed to rote practice since the terrorist attacks on 9/11 and various other events that have disrupted our lives. The methods can be easily applied in this context to create a complete description of the threats listed above and others considered emergent or relevant. These descriptions identify the frequency, trends, threat vectors, sources, targets, and types of attacks and acts that can be part of the threat. These are then used to create a threat level matrix, like the kind shown below, used to determine which threats to address and what methods and countermeasures are warranted for a given threat.

Threat Level Matrix

	Improbable	Moderately probable	Highly probable	Certain
Unimportant	I	I	I	I
Moderately Serious	I	II	II	II
Serious	II	III	III	IV
Very Serious	III	IV	IV	IV

Levels of Security

I Low
II Medium
III High
IV Very High

Selection of Methods and Countermeasures to Reduce Risk

Once the threats and targets are identified and ranked, available and needed methods and countermeasures for addressing those threats against those targets are inventoried, cost-benefit analyzed, and chosen based on a variety of factors that focus on optimizing risk reduction. The chosen methods and countermeasures will be assigned a cost, a cost avoidance, and a return on investment that weighs the costs against the reductions in risk to find the best ways to use the (always) limited resources available to accomplish the goal of making public service work safer.

Alignment of Resources with Desired Level of Risk Reduction

After the methods and countermeasures are identified, the risk tolerance level of the leadership that determines the allocation of resources is determined, the level of resources needed to reach that level of acceptable risk is calculated, and the available resources are compared to what is needed. If resources are available and adequate, they are allocated. If they are insufficient, the decision is made to either accept more risk or find more resources.

Implementation of Risk Reduction Methods and Countermeasures
Once the resources are allocated, the entities and persons responsible for implementation are charged with that duty. The process of selecting the staff, vendors, or other parties that will implement the methods and countermeasures is undertaken. Then the projects are launched and managed to completion and placed into routine operation.

Evaluation of Risk Reduction Efficacy
After implementation, the risk reduction levels are measured, and the methods and countermeasures are evaluated for their respective contributions to risk reduction. The cost of the methods and countermeasures are set against their effectiveness to see which ones provide the most protection for the money, time, and effort and accomplished the desired goals. The ongoing challenge of risk management is that when done well, nothing happens. Therefore, the avoidance of bad outcomes must be acknowledged and valued.

Monitor Active, Emerging, and Unaddressed Threats
A surveillance and survey process needs to be undertaken periodically to inform the threat management and risk reduction process. By monitoring what is happening vis a vis threats to public employees by querying both the people affected and various data sources, a jurisdiction can make sure their risk management plan can remain evergreen.

Periodic Revision and Re-evaluation of Threat Reduction Strategy
Using the efficacy and threat monitoring data, the threat management plan and strategy should undergo periodic review and updating. This should include level setting the risk tolerance of the leadership and evaluating availability of resources to ensure ongoing alignment.

Existing Resources and Laws

The process laid out above is practiced in most all state and local jurisdictions and there are trained staff that would be able to apply their knowledge to the problem of public employee protection and threat and risk reduction. The Federal Government, some of these state and local jurisdictions, and private companies have done just that. The Federal Government has several laws and programs aimed at keeping public officials and employees safe. For example, the Election Threats Task Force surveyed and investigated threats against election workers and has begun prosecuting some of these cases. Here is a summary of their findings:

- *"The task force has reviewed over 1,000 contacts reported as hostile or harassing by the election community.*
- *Approximately 11% of those contacts met the threshold for a federal criminal investigation. The remaining reported contacts did not provide a predication for a federal criminal investigation. While many of the contacts were often hostile, harassing, and abusive towards election officials, they did not include a threat of unlawful violence.*
- *In investigations where the source of a reported contact was identified, in 50% of the matters the source contacted the victim on multiple occasions. These investigations*

accordingly encompassed multiple contacts. The number of individual investigations is less than 5% of the total number of reported contacts.

- *The task force has charged four federal cases and joined another case that was charged prior to the establishment of the task force. There have also been multiple state prosecutions to date. The task force anticipates additional prosecutions in the near future.*
- *Election officials in states with close elections and postelection contests were more likely to receive threats. 58% of the total of potentially criminal threats were in states that underwent 2020 post-election lawsuits, recounts, and audits, such as Arizona, Georgia, Colorado, Michigan, Pennsylvania, Nevada, and Wisconsin."*

The Congressional Research Service lists the following Federal laws that are relevant to election threats as well as threats in general:

- *18 U.S.C. § 115, which prohibits threats "to assault, kidnap or murder" federal officials, employees, or their family members with the "intent to impede, intimidate, or interfere with" the performance of official duties, or in retaliation for official duties;*
- *18 U.S.C. § 610, which prohibits intimidating or threatening federal employees to engage in or to not engage in "any political activity";*
- *18 U.S.C. § 876, which prohibits knowingly sending by mail "any communication ... addressed to any other person and containing any threat to kidnap any person or any threat to injure" and includes additional penalties for mailing threats to federal officials;*
- *18 U.S.C. § 1503, which prohibits "corruptly or by threats or force, or by any threatening letter or communication, influences, obstructs, or impedes or endeavors to influence, obstruct, or impede, the due administration of justice";*
- *18 U.S.C. § 1505, which prohibits the obstruction of justice, including by threats, for any proceeding before a U.S. agency or a congressional investigation;*
- *18 U.S.C. § 1512, which prohibits threatening or intimidating a witness in an official proceeding to withhold testimony, tamper with evidence, or prevent someone from reporting a federal offense to law enforcement;*
- *52 U.S.C. § 20511, which provides criminal penalties for any person, including an election official from, among other things, "knowingly and willfully intimidat[ing], threat[ening], or coerc[ing] or attempt[ing] to intimidate, threaten, or coerce any person for ... urging or aiding any person" in voting or registering to vote in a federal election; and*
- *52 U.S.C. § 10307, which prohibits persons acting under the color of law or otherwise from intimidating, threatening, or coercing any person "for urging or aiding any person to vote or attempt to vote" or for enforcing the right to vote.*

A reasonable line of inquiry regarding this list of statutes is to see where states need, but do not have, comparable laws if federal jurisdiction cannot be established. Since the list above is not an exhaustive one of all the relevant laws that can be considered and applied to this problem, a thoughtful inventory and analysis of existing law is needed, which can be used to determine what advice to states could be generated regarding gaps in state laws. There is also active

discussion of numerous bills at the federal level, and one recently passed bill of note summarized here by CNN:

> *"The House voted 396-27…to pass a bill extending security protections to Supreme Court justices' immediate family members.*
>
> *The bill – the Supreme Court Police Parity Act of 2022 – will now be sent to President Joe Biden to be signed into law. It was introduced by Republican Sen. John Cornyn of Texas and passed the Senate in May…the final measure…does allow the Marshal of the Supreme Court to provide security to "any officer" of the bench if the Marshal deems it necessary.*
>
> *Supreme Court justices are currently covered by federal security protection under US Code. The bill would extend those protections to immediate family members of the justices as well if the Marshal of the Supreme Court "determines such protection is necessary," according to the text of the legislation."*

Congress has also acted on this topic for its own members and staff by allocating and allowing the use of funds for office and home security for members and their families. This activity shows that beyond laws, there are numerous protection programs that can serve as models or inform us as to what needs to be improved to make public employees safer. This includes the programs of the Marshall Service, the Supreme Court Police, the US Congress, the Federal Protective Service of the Department of Homeland Security, the Capitol Police, FBI, Justice Department, State Department, and many others. Private companies also have robust programs ranging from executive protection plans to safety programs for all employees. Grants have been given and used by several jurisdictions to improve security in the run up to the last election. Gleaning best practices from such programs, grants, and practices is also a task worth consideration to inform state and local government as to how best to improve their security for public employees.

Laws and programs that improve security of public employees that are informed by a robust security planning and risk mitigation process is what is needed to rise to the level of this problem in our society. We need to know what the viable threats are, how to address them, know what works, and allocate resources to meet our level of risk tolerance. Next, we can consider what kinds of countermeasures and methods could be considered as part of a study process and potential model law.

Countermeasures and Methods to Be Considered as Part of a Model Law and Policy Process

A best practice in risk reduction is what is called "security in depth." Security-in-depth, also known as layered protection, is a concept that means placing a series of progressively more difficult obstacles in the path of an aggressor. These obstacles are often referred to as lines of

defense. What this means is that one should use a variety of risk reduction methods and countermeasures to avoid single points of failure and to make the security response itself more robust and resilient.

One thing to avoid in pursuing security in depth is "security theater." Wikipedia defines this as "the practice of taking security measures that are considered to provide the feeling of improved security while doing little or nothing to achieve it." The article goes on to say that "by definition, security theater provides no security benefits (using monetary costs or not), or the benefits are so minimal it is not worth the cost." And further notes that "critics such as the American Civil Liberties Union have argued that the benefits of security theater are temporary and illusory since after such security measures inevitably fail, not only is the feeling of insecurity increased, but there is also loss of belief in the competence of those responsible for security." Redacting the very public and easily discovered fact of the addresses of public employees is security theater. It's widely known and acknowledged that one can find a person's address by numerous means. Further, the dark web also provides cheap complete profiles of persons gleaned from hacked data, data breaches, malware, apps with loose privacy policies, and data from many, many sources in common circulation. It is also relevant to consider those who are willing to go beyond the stage of thought to actual action to harm, harass, threaten, and stalk a public employee are not in any way likely to be deterred by weak security theater level measures.

The following is a list of possible methods and countermeasures that have been deployed in public and private sector security plans that have proven to be effective. These could be applied alone and in various combinations and at various levels of effort depending on the threat and what works best against it. Using combinations of these would create lines of defense that would be deployed in alignment with the process described above for threat management.

- Identity, Reputation, and Credit Management, Monitoring, and Repair Services
    - This can be considered as a new and necessary employee benefit for all or for selected employees deemed at higher risk
- Electronic Surveillance, Monitoring, and Threat Detection
    - This includes video surveillance, social media monitoring, gunshot sensors, chemical sensors, AI programs, computer network monitoring, and device security
- Security Personnel
    - This includes those routinely assigned to locations as well those who can be deployed to where the threat may be realized and when the threat level for a person or group of persons goes up
- Physical Barriers
- Cybersecurity Training and Services
- Personal Safe Rooms and Panic Buttons
- Self-Defense Training

- Self-Protection Devices and Weapons
- Safety Procedures and Protections
    - For example, safe words, pattern variance, having an electronic way to monitor home entrances and not answering the door directly when a stranger is present, and so on
- Civil Legal Processes and Support
    - Public employees may need assistance to use the laws available to protect themselves and pursue those to have harmed them or seek to harm them
- Protective Orders
- Law Enforcement and Prosecutorial Personnel and Policy Priorities
- New Criminal and Civil Laws, Rules, and Policies (as discussed above)

During ULC discussions on the redaction topic, it has been stated that putting in barriers to finding a person's address from public records will slow and deter those who wish to harm or harass public employees from doing so. As noted above, those who are determined to do harm or harass are likely substantially more motivated to get the information they need and therefore the redaction barrier is not effective against them. But it is effective in limiting those who want to use that data for informational and beneficial purposes. We lack any solid evidence that informational obscurity on addresses will deter the determined who have the capacity for violence and harmful behavior. We know that public employees are facing a more hostile and violent subset of the public that is willing and able to harm them. We must take this threat seriously and match the threats with processes, programs, and laws that will reduce and prevent risks, deter bad actors, and apprehend and punish those who break the law while targeting public employees. A longer and more complete study of ways to enhance public employee safety that goes beyond a single weak solution to a security in depth approach is what the times demand and what public employees deserve.