the journal of CIVIC INFO

The Journal of Civic Information

Volume 1 | Number 1 September 2019

Journal homepage: https://journals.flvc.org/civic/ ISSN (online): 2641-970X

The Journal of Civic Information is an interdisciplinary peer-reviewed open-access online journal published by the Brechner Center for Freedom of Information through the Public Knowledge Project and is supported by the University of Florida College of Journalism and Communications.

Contact:
David Cuillier, Ph.D.
cuillier@email.arizona.edu

DOI: https://doi.org/10.32473/joci.v1i1

JCI Editorial Board

the journal of CIVIC INFO

The Journal of Civic Information

Volume 1 | Number 1 September 2019

Journal homepage: https://journals.flvc.org/civic/ ISSN (online): 2641-970X

An Introduction

Frank LoMonte, J.D., Publisher, *University of Florida*

David Cuillier, Ph.D., Editor, *University of Arizona*

Welcome to the inaugural edition of *The Journal of Civic Information*, a forum for sharing ideas about meeting the public's need for civically actionable information.

This journal, hosted by the Brechner Center for Freedom of Information at the University of Florida's College of Journalism and Communications, launches at a time when access to reliable information in the United States seems especially precarious. U.S. newsroom employment is at the lowest recorded levels in modern history, and the contraction in the industry – more than 20 percent of newspapers have closed since 2004 – is unrelenting. If people consume news at all, it is increasingly from dubiously reliable and ideologically polarized sources.

Because there are fewer "learned intermediaries" being paid to gather and distribute information to the public, we must make information easier to collect, understand, and use. That theme runs throughout the articles you will read in this debut issue of the journal, and those to come in each successive quarterly edition.

At a time of diminished public confidence in established institutions, both public and private, it is essential for trust to be earned through transparency – or, as tenth-grade Geometry teachers have admonished for generations, "Show your work."

In coming up with the journal's title, the word doing most of the lifting ended up being "Civic." A publication needs an identity, and some guardrails. We intend to focus on the kinds of information that people need to participate in self-governance, broadly defined.

This journal resides somewhere between the immediacy of a blog and the comprehensiveness and rigor of a traditional law journal or peer-reviewed scholarly publication. Its publishing schedule and review process are designed to react nimbly to unfolding developments in technology, law, and public policy. All submissions will undergo double-blind peer review by some of the nation's top scholars and information experts.

We intentionally created this new publication as an open-access online journal, because it would be ironic to hide this much-needed research behind a paywall or subscription. We also saw a need for a single publication dedicated to civic information research, currently found among various disciplinary publications.

Indeed, it is our hope that this journal will bring together research from across disciplines and methodologies, including law, public administration, journalism, information science, sociology, and any others concerned with the access, dissemination, use, and effects of civic information. This is reflected in the journal by providing a legal analysis section in Bluebook citation style and a social science section in American Psychological Association style. We invite experts from across those disciplines – anyone whose work, as a scholar or practitioner, touches on the technological, legal, and policy issues that arise in managing information for the public's benefit – to contribute articles or suggest topics.

We are fortunate to launch the journal with four excellent articles – two legal analyses, a survey, and a content analysis – that shed light on access to civic information:

- Communication law scholars Daxton "Chip" Stewart and Amy Kristin Sanders, in the "Secrecy, Inc." article, provide insightful legal analysis and recommendations for challenging increased civic secrecy through privatization of government services.
- Katie Blevins and Kearston L. Wesner, also First Amendment scholars, examine access to government officials' communications on social media, including analysis of the most recent court ruling regarding Donald J. Trump's Twitter account.
- Journalism scholar Alexa Capeloto reports results of a survey exploring the perspectives of government record custodians on the pros and cons of online public records request portals, an emerging transparency tool in the United States.
- Finally, journalism scholar Jodie Gil provides a national look at how state public record laws include or exempt home addresses to protect personal privacy, which informs policy debates in state legislatures.

All of these articles were initially presented at the inaugural freedom of information research competition hosted by the National Freedom of Information Coalition national summit in Dallas, Texas, in April 2019. Other papers presented at the competition will be published in forthcoming issues of this journal.

In addition to the collaborative partnership with NFOIC, we are grateful for Diane McFarlin, dean of the University of Florida's College of Journalism and Communications, for hosting and supporting this journal. The animating principle behind the journal, and all of the work being done at the Brechner Center for Freedom of Information, is to create "practical scholarship" that helps people solve pressing real-world problems.

As Dean Sarah Bartlett of the CUNY Graduate School of Journalism has said, in challenging the field of journalism education to become more agile and less tradition-bound, "if we allow our reverence for abstract academic ideals to paralyze us or make us overly fearful of change, we will become irrelevant." We hope you will find this journal to be occasionally irreverent and always relevant.

DOI: https://doi.org/10.32473/joci.v1i1.115656

** Please send correspondence about this article to Frank LoMonte, Brechner Center for Freedom of Information, School of Communication & Journalism, University of Florida, flomonte@ufl.edu, or David Cuillier, University of Arizona, cuillier@email.arizona.edu.*

the journal of CIVIC INFO

The Journal of Civic Information

Volume 1 | Number 1 September 2019

Journal homepage: https://journals.flvc.org/civic/ ISSN (online): 2641-970X

Secrecy, Inc.: How Governments Use Trade Secrets, Purported Competitive Harm and Third-Party Interventions to Privatize Public Records

Daxton "Chip" Stewart & Amy Kristin Sanders *

Article Information

Received: Jan. 21, 2019

Accepted: Feb. 13, 2019

Published: Sept. 4, 2019

Keywords

Freedom of information
Public records
Government transparency
Privatization

Abstract

As governments engage in public-private partnerships, they have devised ways to shield the public's business from the traditional level scrutiny offered by citizens and journalists, watchdogs of the public trust. The authors propose rethinking public oversight of private vendors doing government business. First, the authors explore the historical and legal background of open records laws. This core purpose is undermined by overly broad interpretations of trade secrets and competitive harm exceptions, a trend exacerbated by the U.S. Supreme Court in a 2019 ruling. The authors demonstrate why public-private collusion to sabotage transparency demands a reinvigorated approach to the quasi-government body doctrine, which has been sharply limited for decades. The authors conclude with recommendations on reversing the trend.

* Daxton "Chip" Stewart, Texas Christian University; Amy Kristin Sanders, University of Texas at Austin. Please send correspondence about this article to Daxton "Chip" Stewart at d.stewart@tcu.edu. An earlier version of this work earned first-place paper at the National Freedom of Information Coalition summit FOI Research Competition, April 12, 2019, in Dallas, Texas.

To cite this article in Bluebook: Daxton "Chip" Stewart & Amy Kristin Sanders, *Secrecy, Inc.: How Governments Use Trade Secrets, Purported Competitive Harm and Third-Party Interventions to Privatize Public Records,* 1(1) J. CIVIC INFO 1 (2019).
To cite this article in APA: Stewart, D. C., & Sanders, A. K. (2019). Secrecy, Inc.: How governments use trade secrets, purported competitive harm and third-party interventions to privatize public records. *Journal of Civic Information, 1*(1), 1-29.

DOI: https://doi.org/10.32473/joci.v1i1.115657

Introduction

As cities and regions were climbing over one another with bids to become the location of Amazon's new headquarters in 2018, some local governments began offering a new perk: the cover of darkness. The two winning bidders, New York and Northern Virginia,[1] both offered billions of dollars of investment and tax incentives to draw the Internet retail behemoth to their respective areas. And they also both offered aid in dodging open records requests made under their states' freedom of information laws.

Virginia promised to give Amazon at least two days' notice of any public records request regarding the company, to cooperate with Amazon in responding to records requests, and to "limit disclosure, refuse to disclose, and redact and/or omit portions of materials to the maximum extent permitted by applicable law."[2] Although New York Mayor Bill de Blasio's spokesperson initially denied the city offered a similar deal to Amazon, that statement turned out to be false.[3] The city's Economic Development Corporation offered to "give Amazon prior written notice sufficient to allow Amazon to seek a protective order or other remedy" upon the city receiving an open records request regarding the company.[4]

These concessions represent a growing challenge to open records laws. As governments engage in public-private partnerships or otherwise outsource government work to private companies, they have devised ways to shield the public's business from the traditional level scrutiny afforded to citizens and journalists, watchdogs of the public trust.

The trend toward secrecy is emerging in other areas as well, as courts carve out special exceptions to open records laws that favor private business interests. In 2015, the Texas Supreme Court fashioned an enormous loophole in the state's Public Information Act, essentially exempting government contracts with private vendors from public disclosure.[5] The high court allowed aerospace giant Boeing to intervene into a citizen's request for a copy of the company's 20-year lease agreement with the Port Authority of San Antonio to use and redevelop city property.[6] Further, the court ruled that the lease, which included the amount of government expenditures, could be exempted from disclosure because releasing it "would give advantage" to Boeing's competitors.[7] This approach allowed Texas government bodies to prevent disclosure of information a company claims would be "competitively sensitive," analogizing the records to property or personal privacy interests. And it led to absurd outcomes in other situations. For

[1] After "fierce backlash from lawmakers" about the nearly $3 billion in incentives and giveaways to Amazon, the company canceled its plans to build a headquarters in New York. J. David Goodman, *Amazon Scraps New York Campus*, N.Y. TIMES, Feb. 14, 2019, at A1.

[2] Robert McCartney, *Amazon HQ2 to benefit from more than $2.4 billion in incentives from Virginia, New York and Tennessee*, WASH. POST, Nov. 13, 2018, https://www.washingtonpost.com/local/virginia-news/amazon-hq2-to-receive-more-than-28-billion-in-incentives-from-virginia-new-york-and-tennessee/2018/11/13/f3f73cf4-e757-11e8-a939-9469f1166f9d_story.html?utm_term=.689f11d22c04.

[3] Cale Guthrie Weissman, *New York will give Amazon an early warning about HQ2 records requests after all*, FAST COMPANY, Dec. 11, 2018, https://www.fastcompany.com/90279607/report-new-york-will-give-amazon-a-heads-up-to-any-foia-requests.

[4] Sally Goldenberg & Dana Rubinstein, *Top city official gave Amazon a role in public records release*, POLITICO, Dec. 11, 2018, https://www.politico.com/states/new-york/city-hall/story/2018/12/11/top-city-official-gave-amazon-a-role-in-public-records-release-737885.

[5] On June 14, Texas Gov. Greg Abbott signed into law Senate Bill 943, designed to remedy the loopholes created by the Texas Supreme Court in *Boeing Co. v. Paxton.*

[6] Boeing Co. v. Paxton, 466 S.W.3d 831 (Tex. 2015).

[7] *Id*. at 834.

example, the city of McAllen was able to claim the exception to avoid disclosing how much money it lost after hosting a holiday parade that featured singer Enrique Iglesias.[8] The attorney general, citing *Boeing*, upheld the McAllen's decision not to release the information in a letter ruling, saying that the city had established that release of the cost of hiring Iglesias to perform "would give advantage to a competitor or bidder," presumably another city spending tax dollars to hire performers.[9] The ludicrous policy result of this, of course, is that cities wind up bidding against one another, paying even more for services than they would if they engaged in basic transparency typically required by open records laws. It took nearly four years for the Texas legislature to remedy the loophole created by the Texas Supreme Court, but not before nearly 4,000 requests for government contracts with private vendors had been denied by the attorney general on *Boeing* grounds.[10]

Similar issues have arisen at the federal level as well. In June 2019, the U.S. Supreme Court in *Food Marketing Institute v. Argus Leader Media*, overturned a pro-transparency ruling out of the U.S. Court of Appeals for the Eighth Circuit that narrowly read the "trade secrets" exemption to the Freedom of Information Act, striking down 45 years of lower court precedent that had interpreted "confidentiality" under Exemption 4 to include a showing of substantial competitive harm, rather than mere assertion of harm.[11] The ruling came after the Department of Agriculture had chosen not to appeal a decision that required release of how much money grocery stores were receiving from the government under the Supplemental Nutrition Assistance Program (SNAP), a third-party industry group, the Food Marketing Institute, intervened to take up the appeal, in an attempt to make it easier to protect corporate privacy interests.[12]

These moves, along with gutting of the quasi-government entity doctrine that typically would mandate transparency of government deals to conduct public business through private vendors,[13] are emblematic of a parade of darkness that appears to be advancing largely unabated. Courts broadly interpret "trade secrets" and other exemptions favoring private vendors on government contracts. Private businesses are enabled to intervene in court as a third party in an open-records matter typically handled by an administrative agency or attorney general, dragging issues into litigation to frustrate and delay citizens seeking to provide oversight. Government entities conspire to subvert transparency laws as an inducement to lure private businesses such as Amazon with bundles of cash and tax incentives. The practice in the recent Amazon headquarters bidding has the look of a new "Ashcroft memo"[14] for public-private partnerships, dangerously

---

[8] Jason Cobler, *Bill takes aim at open records loophole made infamous by Enrique Iglesias show*, SAN ANTONIO EXPRESS-NEWS, Feb. 22, 2019, https://www.expressnews.com/news/politics/texas_legislature/article/Bill-would-close-open-records-loophole-made-13637808.php.

[9] TEX. ATT'Y GEN. ORD-5179 (2016).

[10] *See* Jeremy Blackman, *No right to know? Texas public records get harder and harder to acquire*, HOUSTON CHRONICLE, Mar. 14, 2019, https://www.houstonchronicle.com/news/investigations/article/Texas-public-records-get-harder-and-harder-to-13683497.php.

[11] Food Mktg. Inst. v. Argus Leader Media, ____ U.S. _____ (2019); *see also* Food Mktg. Inst. v. Argus Leader Media, 202 L. Ed. 2d 641 (2019).

[12] Argus Leader v. Dep't of Agric., 889 F.3d 914 (8th Cir. 2018).

[13] *See* Greater Houston Partnership v. Paxton, 468 S.W.3d 51 (Texas 2015) (in which the Texas Supreme Court went beyond the plain language of the word "support" to find that the government paying a chamber-of-commerce-like entity to do public business did not make the entity subject to the Public Information Act because "support" means more than financial support, instead requiring fuller "sustenance" from the government).

[14] The "Ashcroft memo" is an infamous part of recent FOIA history. Shortly after the terrorist attacks of Sept. 11, 2001, U.S. Attorney General John Ashcroft essentially told federal agencies that denial of any FOIA requests would be defended by his office unless they "lacked a sound legal basis." It overturned the "strong presumption in favor of information disclosure" by previous Attorney General Janet Reno and ushered in an era of unprecedented obstinance

creating incentives that favor secrecy over government transparency. Government bodies are essentially telling private vendors, "We'll help you spend tax dollars without any pesky oversight. Do whatever you want. We've got your back." The public-private collusion to undermine open records laws, if left unchecked, opens the door to unparalleled waste, fraud, and corruption.

In this article, we propose rethinking public oversight of private vendors doing government business. First, we explore the historical and legal background of open records laws to demonstrate the core purposes behind their enactment, and how that purpose has transparency of government contracts at its center. Next, we look at how overly broad interpretations of trade secrets and competitive harm exceptions undermine this core purpose, especially when paired with procedural advantages that allow private businesses to intervene in open-records disputes as a third party. Finally, we demonstrate why public-private collusion to sabotage transparency demands a reinvigorated approach to the quasi-government body doctrine, which has been sharply limited for decades. At a time when government corruption and exporting public business to private vendors is on the march, it is time for open-records advocates to reclaim transparent democracy and draw the swords that a century of freedom of information law have provided.

Background

The watchdog function is at the heart of the guarantee of a free press. As legal historian Tim Gleason noted, scrutiny by a free press was "a means of combating what 18th-century men in America viewed as an inevitable condition – the abuse of government power" which was "the core of the dominant theory of freedom of the press at the time of the adoption of the First Amendment to the Constitution of the United States and state constitutional free-press clauses."[15] Constitutional scholar Thomas Emerson, writing on the heels of Watergate, argued that the right to know had grounds to be observed as an "emerging constitutional right," rooted in the First Amendment. "The public, as sovereign, must have all information available in order to instruct its servants, the government," Emerson wrote. "As a general proposition, if democracy is to work, there can be no holding back of information; otherwise ultimate decision-making by the people, to whom that function is committed, becomes impossible."[16]

If there is one principle at the heart of open records laws, it is most succinctly stated by Harold L. Cross, the attorney and scholar who addressed the failings of government transparency in the burgeoning administrative state during the middle of the last century, in his 1953 treatise *The People's Right to Know*: "Public business is the public's business. The people have the right to know. Freedom of information is their just heritage. Without that the citizens of a democracy

by federal agencies handling FOIA requests. *See* Jane E. Kirtley, *Transparency and Accountability in a Time of Terror: The Bush Administration's Assault on Freedom of Information*, 11 COMM. L. & POL'Y 479, 491 (2006); Keith Anderson, *Is There Still a "Sound Legal Basis?": The Freedom of Information Act in the Post-9/11 World*, 64 OHIO ST. L. J. 1605 (2003). President Obama revoked the memo on his first day in office in 2009, ordering federal agencies to once again approach FOIA with a clear presumption that "(i)n the face of doubt, openness prevails." OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OPEN GOVERNMENT DIRECTIVE (Dec. 8, 2009).

[15] TIMOTHY W. GLEASON, THE WATCHDOG CONCEPT: THE PRESS AND THE COURTS IN NINETEENTH CENTURY AMERICA 24 (1990).

[16] Thomas Emerson, *Legal Foundations of the Right to Know*, 1976 WASH. U. L. Q. 1, 14 (1976). While Emerson acknowledged that the "right to gather information from private sources" was not encompassed by this, he focused exclusively on "private people" and not businesses; additionally, he did not address businesses doing public work funded by government sources. *Id*. at 19.

have but changed their kings."[17] Cross' work was hugely influential in the push to enact the federal Freedom of Information Act and remains a foundational work in our understanding of the origins of transparency and the law in the United States.[18]

Although *The People's Right to Know* was a comprehensive report on state and federal approaches to open records and meetings at the time, it did not specifically address transparency of public business done in conjunction with private companies. The closest Cross came to this topic was mentioning advances in secrecy "covering financial dealings between government and citizens" such as collection of income taxes or penalties paid to government, as well as distribution of government benefits through "public assistance programs"[19] such as SNAP. But the latter part of the 20th century saw the proliferation of government favoring privatization in areas of public programs, such as local economic development efforts, operation of prisons and hospitals, parks and land management, and even public education. Privatization is done "in the expectation of realizing greater operational efficiency and cost savings," as Mitchell Pearlman, the longtime attorney and executive director of the Connecticut Freedom of Information Commission, said.[20] But this has also come with an expectation built into the law that because private companies are not subject to transparency laws, they may be able to avoid similar public oversight.

This notion, of course, frustrates not only the purpose of open-records laws, but also the foundations of informed democracy in the United States. And state and federal courts and legislatures have largely failed to reconcile the public-private tensions regarding records access, putting into place "complicated, indeterminate rules to resolve the fundamental conflict between laws intended to cover government agencies and the increasing reliance by those agencies on private firms for research and for the operation of traditional government functions," as Mark Fenster noted.[21] It's an issue that has bedeviled transparency advocates and scholars in areas such as university foundations,[22] private prisons,[23] and economic development agencies.[24] And even when traditional open government arguments carry the day when access matters are raised in court, Aimee Edmondson and Charles Davis noted, the process quickly devolves into a cycle in which private entities on contract to do public business seek protection from legislators instead to protect them from scrutiny, part of a "recent push by lawmakers and developers to bring unprecedented secrecy to efforts to lure businesses to their communities."[25]

Although corporations may be people for the purpose of making campaign contributions,[26] they are not extended the same rights of privacy as individual citizens, at least under the language

---

[17] HAROLD L. CROSS, THE PEOPLE'S RIGHT TO KNOW XIII (1953).

[18] *See* David Cuillier, *The People's Right to Know: Comparing Harold L. Cross' Pre-FOIA World to Post-FOIA Today*, 21 COMM. L. & POL'Y 433 (2016).

[19] Cross, *supra* note 17 at 9.

[20] MITCHELL W. PEARLMAN, PIERCING THE VEIL OF SECRECY: LESSONS IN THE FIGHT FOR FREEDOM OF INFORMATION 75 (2010).

[21] Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 918 (2006).

[22] *See* Scott Reinardy & Charles N. Davis, *A Real Home Field Advantage: Access to University Foundation Records*, 34 J. L. & EDUC. 389 (2005); Alexa Capeloto, *A Case for Placing Public University Foundations Under the Existing Oversight Regime of Freedom of Information Laws*, 20 COMM. L. & POL'Y 311 (2015) (arguing in favor of recognizing university foundations as public agencies subject to open records laws).

[23] *See* Mike Tartaglia, *Private Prisons, Private Records*, 94 B.U. L. REV. 1689 (2014) (arguing that private prisons should not be able to avoid public oversight because of an "essentially meaningless distinction concerning their legal status" as a private entity).

[24] *See* Aimee Edmondson & Charles N. Davis, *"Prisoners" of Private Industry: Economic Development and State Sunshine Laws*, 16 COMM. L. & POL'Y 317 (2011)

[25] *Id*. at 320.

[26] *See* Citizens United v. Federal Election Comm'n, 558 U.S. 310 (2010).

of the Freedom of Information Act. In 2011, the Supreme Court declined telecommunication company AT&T's request to be afforded the same personal privacy as an individual person. AT&T intervened as a third party in a FOIA request by a competitor for records involving an FCC enforcement action against AT&T, arguing that it was a "'private corporate citizen' with personal privacy rights" that should be shielded from disclosure under Exemption 7(C).[27] Chief Justice Roberts, writing for a unanimous majority, looked at the plain meaning and dictionary definitions of the word "personal" and found "little support for the notion that it denotes corporations."[28] Indeed, ruling against A&T, Roberts concluded that the company should "not take it personally."[29] Yet companies, and the governments that try to entice them into contract agreements, seem to be arguing that their relationship is on par with personal privacy concerns that are well within the policy allowing exemptions to open records laws. The notion is absurd, and it is unsupported by the history of FOIA and its interpretation by federal courts during the past five decades.

Despite recent dicta from courts asserting that FOIA is equally about balancing citizen access to records and government interest in secrecy,[30] the actual purpose of the law could not be clearer. When Congress was drafting FOIA in 1966, it was in response to the failures of provisions of the Administrative Procedure Act to allow access to government records in a timely and effective manner. The purpose of FOIA, the House of Representatives asserted in a report on the bill, was "to establish a general philosophy of full agency disclosure."[31] After agencies and federal courts frustrated these purposes through broad construction of exemptions favoring government secrecy, turning FOIA into a "freedom from information law" according to some critics, Congress responded with revisions in 1974, 1976, 1996, 2007, and 2016, each one favoring broader transparency and narrower interpretation of exemptions.[32] In 1985, the Supreme Court recognized this purpose, noting that FOIA "established a broad mandate for disclosure of governmental records," with exemptions "narrowly tailored" to serve "the fundamental goal of disclosure."[33] In 2005, the House Committee on Government Reform drafted a guide for citizens to use FOIA to access records, commenting, "Above all, the statute requires Federal agencies to provide the fullest possible disclosure of information to the public…The history of the act reflects that it is a disclosure law."[34]

Indeed, the notion of corporate privacy and a purpose-agnostic FOIA flies in the face of Supreme Court interpretation of the law. In 1989, even in one of the most notoriously anti-transparency decisions in the court's history, a unanimous court identified the "central purpose" underlying the Freedom of Information Act as shedding light on government operations.

---

[27] FCC v. AT&T Inc., 562 U.S. 397, 401 (2011).
[28] *Id*. at 405.
[29] *Id*. at 410.
[30] The Court dismissed what it called a "policy argument about the benefits of broad disclosure" in efforts by Argus Leader that would favor narrow construction of exemptions, instead suggesting that Congress sought a "'workable balance' between disclosure and other governmental interests." Food Marketing Inst. v. Argus Leader Media, 139 S. Ct. 2356, 2366 (2019).
[31] H.R. REP. NO. 89-913, at 38 (1965).
[32] *See* Martin Halstuk & Bill Chamberlin, *The Freedom of Information Act 1966-2006: A Retrospective on the Rise of Privacy Protection Over the Public Interest in Knowing What the Government's Up To*, 11 COMM. L. & POL'Y 511, 533 (2006); Daxton R. "Chip" Stewart & Charles N. Davis, *Bringing Back Full Disclosure: A Call for Dismantling FOIA*, 21 COMM. L. & POL'Y 515, 519-21 (2016).
[33] CIA v. Sims, 471 U.S. 159, 182 (1985).
[34] "A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records," H.R. REP. NO. 109-226, at 2 (2005).

The decision in which this determination was made has long been reviled by open records advocates, not to mention fans of statutory interpretation. In *Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court unanimously ruled that the FBI did not have to release the criminal "rap sheet" of convicted felon Charles Medico to journalists seeking it under FOIA because it would invade his personal privacy.[35] In doing so, the court asserted that the "central purpose" of FOIA was "to ensure that the *Government's* activities be opened to the sharp eye of public scrutiny," rather than merely allowing public access to all documents held by the government about private citizens.[36] The "central purpose" standard is nowhere to be found in the language of FOIA, as Justice Ruth Bader Ginsburg later noted, and "changed the FOIA calculus of" a previous series of "prodisclosure decisions."[37] The standard essentially created a new burden for requesters that "seemingly contravenes the legislative intent of the FOIA by narrowly defining a disclosable record as only official information that reflects an agency's performance and conduct," said Martin Halstuk and Charles Davis as they examined the havoc the new standard had caused FOIA requesters in the decade after it was decided.[38]

The outcome of the case and its long-term effect may have been outright harmful to transparency efforts so far, serving as a shield for government agencies to defend against citizens and journalists seeking access to records. But the "central purpose" doctrine, and the logic underlying it, should be wielded by freedom of information advocates as well – as an argument endorsed by the highest court in the land undergirding open records laws. For three decades now, a unanimous ruling has identified records that "contribute significantly to public understanding *of the operations or activities of the government*" are the "core purpose" of FOIA.[39] This is not a terrible basis, altogether, for reclaiming the point of accounting for public funds doing public work that have been designated to private businesses. Nothing is more illustrative of the "operations or activities of government" than records detailing how the government spends taxpayers' money. Whether these records are in the possession of the government or the agencies it authorizes to do government business, they clearly shed light on government operations. This is why freedom of information laws exist. Although each state law has a statement of purpose or legislative history that may be slightly distinct, they all rest on this same bedrock principle that transparent government is good government, that the policy of the state is to favor openness and for courts to construe provisions liberally to favor disclosure, and that governments are the servants of citizens rather than their masters.

The new twist, of public-private collusion to subvert open records law compliance as part of contracts awarding public money to private entities for public purposes, is a shocking escalation. It is what Pearlman called a "cloaking device" for government spending, a brazen effort to dodge public oversight in a way that would cover up "issues of self-dealing, excessive compensation at the public's expense—and even corruption in the awarding of these arrangements."[40]

Corporate privacy is not a real thing. The "central purpose" of freedom of information laws – as advocated by the government while trying to avoid releasing private information – is disclosing records that allow oversight of government spending. Even when that spending is funneled through a private organization, it is no less the business of the public. To ensure that this

[35] Dep't of Justice v. Reporters Committee for Freedom of the Press (hereinafter, "RCFP"), 489 U.S. 749 (1989).
[36] *Id*. at 797
[37] Dep't of Defense v. Federal Labor Relations Auth., 510 U.S. 487, 507 (1994) (Ginsburg, J. concurring).
[38] Martin E. Halstuk & Charles N. Davis, *The Public Interest Be Damned: Lower Court Treatment of the Reporters Committee 'Central Purpose' Reformulation*, 54 ADMIN. L. REV. 983, 991 (2002).
[39] *RCFP*, 489 U.S. at 775 (emphasis in original).
[40] Pearlman, *supra* note 20 at 75, 79.

purpose is fulfilled, transparency advocates must look to limit the expansion of business privacy exemptions in the name of potential competitive harm and revelation of trade secrets that are becoming more commonplace. The *Boeing v. Paxton* decision and *Food Marketing Institute v. Argus Leader Media*, a pair of cases driven by third-party interveners seeking to assert business privacy interests, are illustrative of this downward spiral toward secrecy.

Open records laws and non-governmental entities

Since it took effect in 1967, the federal Freedom of Information Act has been grounded in the presumption of openness, and many state open records laws modeled after it followed suit. Even the current About Page on FOIA.gov details this purported commitment to disclosure: "The FOIA provides that when processing requests, agencies should withhold information only if they reasonably foresee that disclosure would harm an interest protected by an exemption, or if disclosure is prohibited by law. Agencies should also consider whether partial disclosure of information is possible whenever they determine that full disclosure is not possible and they should take reasonable steps to segregate and release nonexempt information."[41] But, as we have briefly outlined above, that fundamental commitment to transparency has been eroding. It's nearly impossible to identify a singular watershed moment when the scales began to tilt more heavily toward secrecy, but key court cases around the country have charted the course away from transparency, interpreting federal and state open records laws in ways that provide the public with less potential for oversight as the government continues to engage the private sector in more of its daily activities. To be sure, the convergence of the government's increasing privatization efforts and the courts' broadening of open records exemptions is troubling.

Statutory open records provisions regularly define the term "public record" in a way that limits disclosure of records not created directly by a government agency, and very few state open records law specify that all documents produced by a government contractor, or for the government, are subject to disclosure. In general, state open records laws fall into one of several categories with regard to their position on whether the records of nongovernmental bodies should be public. At one end of the spectrum, a number of state laws do not even mention nongovernmental bodies. Others condition availability of records on whether the entity receives government funding, with some specifying how much funding the entity must receive. A few states have a "functional equivalence" test that suggests entities acting in ways comparable to a public agency are subject to disclosure.

Finally, the broadest approach, taken by Alaska, encompasses even records of private contractors created for public agencies. After amending its open records law in the 1990s, Alaska defines public records to include "books, paper, files, accounts, writing, including drafts and memorializations of conversations, and other items … that are developed or received by a public agency, or by a private contractor for a public agency, and that are preserved for their informational value or as evidence of the organization or operation of the public agency."[42] To date, no relevant court interpretations of the private contractor language have been issued, but the plain language meaning suggests an atypically broad interpretation of the term "public records" that places significant importance on the public's right to information about government business.

[41] U.S. Dep't of Justice, *What is FOIA?* https://www.foia.gov/about.html.
[42] ALASKA STAT. § 40.25.220 (2018).

A promising decision out of the Louisiana Supreme Court took a similarly broad approach, ruling that the Louisiana Society for the Prevention of Cruelty to Animals, a private 501(c)(3), was subject to the state's open records law.[43] In that case, the LSPCA had entered into a contract with the City of New Orleans to provide animal control for the municipality. The New Orleans Bulldog Society, a nonprofit animal rescue, had filed a public records request with the City of New Orleans, seeking release of the LSPCA's standard operating procedures related to adoption eligibility determinations for stray dogs.[44] In typical fashion, the city referred the animal rescue to the LSPCA, saying it did not have the documents that New Orleans Bulldog was seeking. In response to Bulldog's request, the LSPCA asserted it was not a "public body" under the Louisiana Public Records Act.[45] However, the Louisiana Supreme Court, in its 2017 decision, found the LSPCA to be an "instrumentality" of the city and required that it comply with the open records law.[46] "Through the discharge of its responsibilities … with the City of New Orleans, as well as the receipt of public money as remuneration for such services, we find the LSPCA is functioning as an instrumentality of a municipal corporation, and is therefore subject to the Louisiana Public Records Act. … The LSPCA is requires to disclose all documents specifically related to the discharge of its duties and responsibilities … with the City of New Orleans."[47] The statutory approach taken in Alaska and the judicial interpretation by the Louisiana high court represent the high-water mark of the public's right to access information about private companies engaged in government business.

A few states have a functional equivalence test to determine whether records should be released. Rhode Island specifically codifies this approach noting that the use of the terms "agency" or "public body" in the public records law includes "any other public or private agency, person, partnership, corporation, or business entity acting on behalf of and/or in place of any public agency.[48] Often this functional approach may not be clearly articulated in the statute itself, but it exists as a product of case law. The Oregon Supreme Court decision in *Marks v. McKenzie HS Fact-Finding Team* represents a fairly typical common law approach.[49] There, the court established a six-part test aimed at evaluating whether the entity is functionally equivalent to a government entity.[50] When a private entity is considered functionally equivalent to government, then any records related to that undertaking are subject to disclosure. Georgia[51], Maine[52], New Mexico[53], Vermont, and Tennessee take a similar approach in their open records laws.[54]

---

[43] New Orleans Bulldog Society v. Louisiana Society for the Prevention of Cruelty to Animals, 222 So. 3d 679 (La. 2017).
[44] *Id.* at 681.
[45] *Id.* at 682.
[46] *Id.* at 681.
[47] *Id.* at 687.
[48] R.I. GEN. LAWS § 38-2-2(1).
[49] *Marks v. McKenzie High School Fact Finding Team*, 319 Or 451, 878 P.2d 417 (Ore. 1994).
[50] *Id.* Essentially, the factors include: (1) Whether the government created the entity? (2) Is the entity's function typically performed by the government (3) Does the entity have decision-making authority or is it advisory to the government? (4) How much financial and nonfinancial support does the entity receive from the government? (5) How much control does the government maintain over the entity's operations? and (6) Are the entity's officers or staff public employees? *Id.*
[51] GA. CODE ANN. § 50-18-70(b)(2).
[52] *Turcotte v. Humane Society of Waterville*, 103 A.3d 1023 (Me. 2014).
[53] *State ex rel Toomey v. City of Truth or Consequences*, 287 P.3d 364 (N.M. 2012).
[54] *See generally* REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, OPEN GOVERNMENT GUIDE, https://www.rcfp.org/open-government-sections/4-nongovernmental-bodies/.

More typically, though, state open records laws contain language similar to the Arkansas Freedom of Information Act, which covers records related to the performance of work carried out by "any other agency … that is wholly or partially supported by public funds or expending public funds."[55] As a result, the state's FOIA applies to some, but not all, private nongovernmental entities that engage in work for the government.[56] As the Arkansas Supreme Court established in *City of Fayettville v. Edmark*, the deciding factor is whether the private entity has undertaken "public business."[57] But that broad term has been severely limited by the state's courts. The free use of public property alone will not trigger the FOIA provisions; instead an entity must directly receive public funds.[58] The court also exempted from the state FOIA private entities that sell equipment and supplies to the government because the government cannot be expected to produce all the materials it uses or provide all the services it requires.[59] Although these carve-outs may seem to gut the law's effect, open government scholars John J. Watkins and Richard Peltz-Steele note that some limitation makes sense "or anyone who received government largesse, including welfare recipients and private hospitals that receive Medicare and Medicaid payments" would be subject to disclosure.[60]

Not surprisingly, many of the state statutes requiring support by or expenditure of public funds operate similarly, but they provide little guidance as to how much financial support is required. Michigan law, for example, defines a public body as one that "is primarily funded by or through state or local authority."[61] Similarly, although Montana's Public Records Act doesn't specifically address whether these kinds of records would be open,[62] Section 9 of the Montana Constitution provides citizens with the "right to examine documents … of all public bodies or agencies of state government and its subdivisions." Under the state's open meetings provision, Montana defines "public body" to include "organizations or agencies supported in whole or in part by public funds or expending public funds…"[63] Other states with similar funding-related approaches include Kansas, Louisiana, Maryland, North Dakota, Oklahoma, South Carolina, Texas, Virginia, and West Virginia.[64] As a result, litigation over whether an organization falls under the open records laws regularly ensues in states that don't provide clear guidance as to how much funding is required to consider a private entity as a public body.[65]

The Kentucky Open Records Act, however, provides a very specific definition of public agency that includes specific funding thresholds. "Any body which, within any fiscal year, derives at least twenty-five percent (25%) of its funds expended by it in the Commonwealth of Kentucky from state or local authority funds. However, any funds derived from a state or local authority in

---

[55] ARK. CODE ANN. § 25-19-103(7)(A) (2017). *See also Denver Post v. Stapleton Dev. Corp.*, 19 P.3d 36 (Colo. App. 2000); 29 DEL. C. § 10002(c); IND. CODE § 5-11-1-16(e); KAN. STAT. ANN. § 45-217(f)(1).

[56] *See generally* Ark. A.G. Opin. No. 2001-069, *available at* http://www.arkansasag.gov/assets/opinions/2001-069.pdf.

[57] *See generally* City of Fayetteville v. Edmark, 801 S.W.2d 275 (1990).

[58] *Sebastian County Chapter of American Red Cross v. Weatherford*, 846 S.W.2d 641 (1993)

[59] *See generally* Ark. A.G. Opin. No. 2003-064, *available at* https://www.arkansasag.gov/assets/opinions/2003-064.pdf.

[60] JOHN J. WATKINS & RICHARD PELTZ, THE ARKANSAS FREEDOM OF INFORMATION ACT, at 50-51 (4th ed. 2004).

[61] MICH. COMP. LAWS ANN. § 15.232(h)(iv).

[62] *See generally* MONT. CODE ANN. §§ 2-6-1002(10), 2-6-1002(13).

[63] MONT. CODE ANN. § 2-3-203(1).

[64] *See generally* REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, OPEN GOVERNMENT GUIDE, https://www.rcfp.org/open-government-sections/4-nongovernmental-bodies/.

[65] *See, e.g., Great Falls Tribune Co. Inc. v. Day*, 959 P.2d 508 (Mont. 1998); *Kubick v. Child and Family Serv. of Michigan, Inc.,* 429 N.W. 2d 881 (Mich. App. 1988).

compensation for goods or services that are provided by a contract obtained through a public competitive procurement process shall not be included in the determination of whether a body is a public agency under this subsection."[66] As a result, those agencies are required to disclose any records pertaining to the "functions, activities, programs or operations funded by state or local authority."[67] Although the 25% benchmark certainly provides a bright-line test for how much funding is required, it also means that whether a private entity is considered a public body for open-records law purposes can vary from year to year, despite the entity engaging in the same function.

Perhaps the worst-case scenario exists in states where the open records law does not even mention nongovernmental bodies. South Dakota's law contains a definition of public record that only mentions government entities. "[P]ublic records include all records and documents … of or belonging to this state, any county, municipality, political subdivision, or tax-supported district in this state, or any agency, branch, department, board, bureau, commission council, subunit, or committee of any of the foregoing."[68] Ohio represents a similarly troubling approach.[69] Idaho, New Hampshire, and New Jersey are among the states that do not clearly articulate how to address nongovernmental entities in their open records laws.[70] Such an oversight in the language, in the era of increasing public-private partnership, leaves open the possibility of arguing the open records law intends no public accountability for these activities.

Exemptions for trade secrets and competitive harm

Even if a state clearly articulates that records of nongovernmental entities are covered by its open records law, public access can still be thwarted in a number of ways. Perhaps the most common approach to limiting transparency can be found when legislatures broadly draft, or courts liberally construe, exemptions to state open records laws. Often this occurs when a private entity claims disclosure of information would result in a disclosure of trade secrets or cause competitive harm for the entity. The previously mentioned Texas Supreme Court decision in *Boeing* typifies these judicially created carve-outs, highlighting an instance – discussed in greater detail below – where judicial overreach bastardized the plain-language meaning of the state's open records statute in a manner that has resulted in significant harm to the public's right to access information.

The case stems from a real estate deal involving the aerospace giant's attempt to lease property for its military maintenance operations. Originally, Boeing had leased property in Oklahoma from American Airlines for this aspect of its business, but it was in need of a new facility when the lease expired. Around the same time, the Department of Defense was scheduled to close Kelly Air Force Base in San Antonio, a location that would be well-suited to Boeing's needs. In 1998, the aerospace company signed a 20-year lease for the parcel of land. This undertaking, Boeing asserted, included nearly a dozen employees and consultants who worked for nearly two years developing a long-term strategy that would allow the company to negotiate a lease deal with would result in the successful execution of military aircraft maintenance contracts over the course of the two-decade lease period.

---

[66] KY. REV. STAT. § 61.870(1)(h).
[67] KY. REV. STAT. § 61.870(2).
[68] S.D. CODIFIED LAWS § 1-27-1.1.
[69] OHIO REV. CODE § 149.011.
[70] *See generally* REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, OPEN GOVERNMENT GUIDE, https://www.rcfp.org/open-government-sections/4-nongovernmental-bodies/.

After the lease had been executed, a former Boeing employee requested the company's lease agreement and other documents under the Texas Public Information Act. The Port, who oversaw the redevelopment of Kelly Air Force Base, notified Boeing of the request, which allowed the company to intervene as a third party. Boeing provided redacted documents and filed an objection with the state Attorney General's office, noting that release of the information would advantage its competitors. "[A] competitor could take the detailed information in Boeing's lease and determine Boeing's physical plant costs at Kelly, allowing the competitor to underbid Boeing on government contracts by enticing another landlord to offer a lower lease rental." However, the Attorney General ruled against Boeing, concluding that none of the information withheld would be considered exempt from disclosure under the state's open records law.

Using a provision in the Texas Public Information Act that allows third parties to raise concerns about a request for information prior to the information's disclosure, Boeing went to court, asserting the release of bid information would cause competitive harm. At the initiation of the case, Boeing was a key tenant in the base's redevelopment project. In ruling against Boeing, the state trial court concluded that the information was not exempt under the public information law's trade secrets provision. It also concluded Boeing could not assert the competitive disadvantage claim because it lacked standing. Boeing, appealed, but the appeals court affirmed the lower court decision. Citing the appellate court's interpretation of Section 552.104(a) of the Texas Public Information Act,[71] Boeing appealed to the Texas Supreme Court.

In a decision that open government advocate Joe Larsen called "one of the worst rulings to ever come out of the Texas Supreme Court," the justices ruled 7-1 in favor of Boeing and "blew a hole in the Texas Public Information Act."[72] Four years have transpired since the Texas high court ruled that information submitted to the state government by private businesses may be withheld from disclosure under the state's public information law if it were deemed to cause competitive harm, and similar attempts to thwart transparency are on the rise around the country. In many instances, attorneys in a vast number of states are specifically pointing to the *Boeing* precedent to justify intervention by private companies as third parties, illogical readings of state open records statutes or abandonment of the quasi-government doctrine, which we discuss in detail below.

Defining trade secrets and competitive harm – a task not undertaken

Broad use of the trade secrets exemptions – found in the federal and nearly all state open records laws – to protect companies contracting with the government contravenes the original intent of the law. In the beginning, FOIA Exemption 4 was largely designed to protect regulated industries from being harmed as a result of the information they were required to submit to the government. In essence, it was designed to encourage business to disclose information as part of the regulatory process.[73] Fundamentally, these laws and their exemptions were never intended to protect the government when it was "acting as a customer and not as a regulator, because secrecy is not abetting the government's regulatory power."[74] But through lazy legislative drafting and

[71] "Information is excepted from the requirements of Section 552.021 if it is information that, if released, would give advantage to a competitor or bidder." TEXAS GOV'T CODE ANN. § 552.104(a).

[72] DALLAS MORNING NEWS, *Editorial: Texas court ruling lets government keep contracts secret, inviting corruption to fester*, Aug. 9, 2016, https://www.dallasnews.com/opinion/editorials/2016/08/09/editorial-texas-court-ruling-triggered-unacceptable-loss-public-accountability.

[73] *See generally* Soucie v. David, 448 F.2d 1067, 1078 (D.C. Cir. 1971).

[74] *See generally* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City,* 20 YALE J. L. & TECH. 103, 158 (2018) (summarizing the intent behind trade secrets exemptions in open records laws).

creative judicial interpretation, the trade secrets exemption in many state open records laws has lost its meaning and become subject to abuse. On the federal level, a current circuit split has left the jurisprudence in a disarray. Often, open records laws do not contain specific definitions for either "trade secrets" or "competitive harm." In the best-case scenarios, this means governments must look to other parts of the law – either statutes or case decisions – for the meaning of these terms. In the worst-case scenarios, it leaves agencies free to make ad-hoc decisions about the meaning. Although some state attorneys general and courts have begun to limit this abuse and articulate clearer standards in some areas, it continues to be a serious issue.

The Delaware Freedom of Information Act contains a pretty typically drafted exemption for trade secrets that is modeled after the federal law's Exemption 4. "Trade secrets and commercial or financial information obtained from a person which is of a privileged or confidential nature"[75] are not deemed to be public. However, a series of recent Attorney General Opinions in the state has narrowed the scope of the broadly worded exemption in way that supports access to information. First, the state does not recognize third-party assertions of trade secret status as binding.[76] Additionally, trade secret information will not be exempted from disclosure if there is no apparent likelihood of competitive harm.[77] In addition, these opinions clearly articulate a standard for both trade secrets and competitive harm, drawing on other sources of law. But, Delaware's approach certainly is not representative of the situation in most states with broadly worded trade secrets exemptions that keep much information from being disclosed.

Idaho's Public Records Act provides for more than 40 exemptions, many of which relate to proprietary business information, trade secrets, and economic development, among other areas of corporate interest.[78] As an example of its largess, the Idaho Public Records Act exemption titled "Trade Secrets, Production Records, Appraisals, Bids, Proprietary Information" is more than 2,200 words long and provides extremely broad definitions for what records can be withheld.[79] Of

---

[75] 29 DEL. CODE ANN. § 10002(l)(2).

[76] *See* Del. Op. Att'y Gen. No. 13-IB07 (Nov. 21, 2013), https://opinions.attorneygeneral.delaware.gov/2013/11/21/13-ib07-112113-foia-informal-opinion-letter-to-mr-chase-re-foia-complaint-concerning-delaware-department-of-corrections/.

[77] *See* Del. Op. Att'y Gen. No. 14-IB04 (July 18, 2014), https://opinions.attorneygeneral.delaware.gov/2013/11/21/13-ib07-112113-foia-informal-opinion-letter-to-mr-chase-re-foia-complaint-concerning-delaware-department-of-corrections/; https://opinions.attorneygeneral.delaware.gov/2014/07/18/14-ib04-071814-foia-opinion-letter-to-mr-myers-re-foia-complaint-concerning-the-department-of-technology-and-information/.

[78] *See* IDAHO CODE § 74-101 *et seq*.

[79] IDAHO CODE § 74-107. "The following records are exempt from disclosure:
(1) Trade secrets including those contained in response to public agency or independent public body corporate and politic requests for proposal, requests for clarification, requests for information and similar requests. "Trade secrets" as used in this section means information, including a formula, pattern, compilation, program, computer program, device, method, technique, process, or unpublished or in-progress research that:
(a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use; and
(b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
(2) Production records, housing production, rental and financing records, sale or purchase records, catch records, mortgage portfolio loan documents, or similar business records of a private concern or enterprise required by law to be submitted to or inspected by a public agency or submitted to or otherwise obtained by an independent public body corporate and politic. Nothing in this subsection shall limit the use which can be made of such information for regulatory purposes or its admissibility in any enforcement proceeding.
(3) Records relating to the appraisal of real property, timber or mineral rights prior to its acquisition, sale or lease by a public agency or independent public body corporate and politic.

particular note, legislative efforts are under way in Idaho to require the government to disclose the algorithms used in pretrial risk assessments to determine whether a criminal defendant should receive bail. House Bill No. 118, which was passed by the Idaho House in early March specifically prohibits reliance on the trade secrets exemption or other protections as a means of withholding disclosure.[80] "All documents, data, records and information used to build or validate the risk assessment and ongoing documents, data, records, information, and policies surrounding the usage of the risk assessment shall be open to public inspection, auditing and testing."[81] Although any effort to ensure records are open to the public is a welcome one, mandating access to individual types of information – here related to the privately created algorithms used in criminal justice – fails to address the serious problem of exemption creep.

Not all state open records laws contain a specific exemption for trade secrets. Arizona, for example, does not list trade secrets among the possible types of records that may be withheld.[82] It does, however, set out procedures for those who seek records for a commercial purpose as well as penalties for those who misuse records for a commercial purpose.[83] Punishing the misuse of information by competitors seems far favorable to preventing the disclosure of information in the name of preventing speculative harm. Other statutes, though they may not make specific mention

(4) Any estimate prepared by a public agency or independent public body corporate and politic that details the cost of a public project until such time as disclosed or bids are opened, or upon award of the contract for construction of the public project.
(5) Examination, operating or condition reports and all documents relating thereto, prepared by or supplied to any public agency or independent public body corporate and politic responsible for the regulation or supervision of financial institutions including, but not limited to, banks, savings and loan associations, regulated lenders, business and industrial development corporations, credit unions, and insurance companies, or for the regulation or supervision of the issuance of securities.
(6) Records gathered by a local agency or the Idaho department of commerce, as described in chapter 47, title 67, Idaho Code, for the specific purpose of assisting a person to locate, maintain, invest in, or expand business operations in the state of Idaho.
(7) Shipping and marketing records of commodity commissions used to evaluate marketing and advertising strategies and the names and addresses of growers and shippers maintained by commodity commissions.
(8) Financial statements and business information and reports submitted by a legal entity to a port district organized under title 70, Idaho Code, in connection with a business agreement, or with a development proposal or with a financing application for any industrial, manufacturing, or other business activity within a port district.
(9) Names and addresses of seed companies, seed crop growers, seed crop consignees, locations of seed crop fields, variety name and acreage by variety. Upon the request of the owner of the proprietary variety, this information shall be released to the owner. Provided however, that if a seed crop has been identified as diseased or has been otherwise identified by the Idaho department of agriculture, other state departments of agriculture, or the United States department of agriculture to represent a threat to that particular seed or commercial crop industry or to individual growers, information as to test results, location, acreage involved and disease symptoms of that particular seed crop, for that growing season, shall be available for public inspection and copying. This exemption shall not supersede the provisions of section 22-436, Idaho Code, nor shall this exemption apply to information regarding specific property locations subject to an open burning of crop residue pursuant to section 39-114, Idaho Code, names of persons responsible for the open burn, acreage and crop type to be burned, and time frames for burning.
(10) Information obtained from books, records and accounts required in chapter 47, title 22, Idaho Code, to be maintained by the Idaho oilseed commission and pertaining to the individual production records of oilseed growers. [Sections 11-29 have been redacted for length considerations]." *Id.*

[80] H.B. 118, 65th Sess. (Idaho 2019) https://legislature.idaho.gov/wp-content/uploads/sessioninfo/2019/legislation/H0118A2.pdf. "No builder or user of a pretrial risk assessment tool may assert a trade secret or other protections in order to quash discovery in a criminal or civil case." *Id.*

[81] *Id.*

[82] *See generally* ARIZ. REV. STAT. ANN. § 39-121.

[83] ARIZ. REV. STAT. ANN. § 39-121.03.

of trade secrets, outline scathes of information that could be argued would result in competitive harm, if disclosed. The Arkansas Freedom of Information Act does not include trade secrets in a list of exemptions, but instead the law exempts myriad records related to economic development.[84] "(A) Files that if disclosed would give advantage to competitors or bidders and (B)(i) Records maintained by the Arkansas Economic Development Commission related to any business entity's planning, site location, expansion, operations, or product development and marketing, unless approval for the release of those records is granted by the business entity."[85] In essence, the Arkansas legislature has specifically codified the troubling practice of allowing third parties to intervene in open records requests into its open records law. Although, as one scholar points, out "Arkansas courts have not interpreted its version of the § 552.104 exception in a way that grants third parties standing to raise the exception,"[86] that doesn't mean they won't in the future. Currently "Arkansas has held that the burden is on government agencies to show that the information requested qualifies for the exception to disclosure, and that state agencies may raise the exception on behalf of third parties."[87]

Some state statutes contain sweeping exemptions allowing the withholding of information in the name of the public interest, a nebulous construct that begs to be misused. The California Public Records Act lists, among its provisions, Section 6255(a), which states "The agency shall justify withholding any record by demonstrating that the record in question is exempt under the express provisions of this chapter *or that on the facts of the particular case the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record*" [emphasis added]. Under the California law, the determination of whether the "catch-all" exemption applies is conducted on a case-by-case basis, with the burden on the government to justify non-disclosure.[88] Case law in California has suggested this burden is a heavy one for the government to bear, but the "catch-all" nature of this exemption remains troubling. A California appellate court, for example, ruled that a university foundation could not use the exemption to withhold the names of athletic licensees and license agreements. "We … can conceive of many examples where the licensee's identity could be of significant interest to the public. … If so, the public has an interest in knowing the licensee's identity to determine whether that licensee is receiving special consideration in contract negotiations."[89] However, broad exemptions that use vague language open the door for those who favor secrecy to demand information be withheld from disclosure.

But the real challenge in nearly all instances where records requests have been denied on the basis of trade secrets or competitive harm is the lack of clarity about what the words actually mean – or should mean – under state open records laws. Even at the federal level, a circuit split gave rise to the Supreme Court's grant of certiorari in *Argus Leader*. The actual practice of allowing exemptions based on trade secrets or competitive harm suggests a possible need to allow third parties to intervene in records requests, though government entities seem to have no trouble asserting these rights for private companies. In one recent example, the City of New York denied a request for information about Palantir's predictive policing algorithm under New York's FOIL,

[84] *See generally* ARK. CODE ANN. § 25-19-105 *et seq*.
[85] ARK. CODE ANN. § 25-19-105(9).
[86] Alexandra Schmitz, Comment, *Don't Mess with the Texas Public Information Act: The Threat to Government Transparency Posed by Boeing v. Paxton and How to Fix It*, 50 TEX. TECH. L. REV. 249, 272 (2018).
[87] *Id.*
[88] *See generally* CBS v. Block, 725 P.2d 470 (Cal. 1986).
[89] California State Univ., Fresno Ass'n. v. Superior Court, 90 Cal. App. 4th 810, 834 (2001).

citing the trade secrets exemption.[90] The New York trial court agreed with the Brennan Center, ruling that the New York City Police Department had produced no evidence to support its claim that turning over vendor documents would reveal trade secrets. The documents sought by the Brennan Center included email correspondence with Palantir, historical output of the system through mid-2017, notes on the development of the current algorithm and summary results of NYPD's various trials of Palantir products.[91]

In Illinois, a Chicago suburb denied a reporter's request under the state open records law[92] for the budget associated with a construction project undertaken by a private contractor, claiming it was a trade secret.[93] In the case, the city asserted both that the developer submitted the information under the implied promise of confidentiality and that release of the information would result in competitive harm because other developers could use the information that had been submitted. Citing a 2017 decision[94] out of the Illinois Court of Appeals, The Illinois Attorney General's Office ruled the trade secrets exemption required both that the information was provided under a claim of confidentiality *and* that there was evidence of substantial competitive harm. Specifically, in the Attorney General's Opinion noted that the legislature revised the exemption in 2010, and the addition of the requirement "indicates its intention to limit the scope" of the exemption.[95] Citing differing standards out of the First/D.C.[96] and Fifth[97] Circuits, the ruling noted that the city failed to present evidence of substantial competitive harm under either approach.

Despite these recent wins in New York and Illinois, the use of the trade secrets exemption has flourished in a number of states in part because of lax definitions that provide little guidance. A March 2019 opinion piece in the *Tennessean* details how governments have capitalized on the trade secrets exemptions, signing non-disclosure agreements with private companies to keep their business dealings confidential.[98] Pointing to major dealings with Google and Volkswagen in the state, Tennessee Coalition for Open Government Executive Director Deborah Fisher detailed a

---

[90] *See* Brennan Center for Justice v. New York City Police Dept., No. 160541/2016 (N.Y. Sup. Ct. Dec. 27, 2017), https://www.brennancenter.org/sites/default/files/opinion12222017.pdf.

[91] Rachel Levinson-Waldman & Erica Posey, *Court: Public Deserves to Know How NYPD Uses Predictive Policing Software,* Brennan Center (Jan. 26, 2018), https://www.brennancenter.org/blog/court-rejects-nypd-attempts-shield-predictive-policing-disclosure.

[92] *See* 5 ILL. COMP. STAT. § 140/7(1)(g). The exemption protects "[t]rade secrets and commercial or financial information obtained from a person or business where the trade secrets or commercial or financial information are furnished under a claim that they are proprietary, privileged or confidential, and that the disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested." *Id.*

[93] Ill. A.G. Op. 18-004, http://illinoisattorneygeneral.gov/opinions/2018/index.html.

[94] Chicago v. Janssen Pharm., Inc. 78 N.E.3d 446 (Ill. App. 1st. 2017).

[95] Ill. A.G. Op. 18-004, http://illinoisattorneygeneral.gov/opinions/2018/index.html.

[96] *See* New Hampshire Right to Life v. United States Dep't. of Health & Human Serv., 778 F.3d 43, 50 (1st Cir. 2015) (quoting Public Citizen Health Research Group v. Food & Drug Administration, 704 F.2d 1280, 1291 (D.C. Cir. 1983)). "Parties opposing disclosure need not demonstrate actual competitive harm; instead, they need only show actual competition and a likelihood of substantial competitive injury in order to 'bring [that] commercial information within the realm of confidentiality.'" *Id.*

[97] *See* Calhoun v. Lyng, 864 F.2d 36, 36 (5th Cir. 1988). "To show substantial competitive harm, the agency must show by specific factual or evidentiary material that: (1) the person or entity from which information was obtained actually faces competition and (2) substantial harm to a competitive position would likely result from the disclosure of information in the agency's records." *Id.*

[98] Deborah Fisher, *Tennessee Must Stop Treating Government Business as a Trade Secret,* TENNESSEAN, Mar. 10, 2019, https://www.tennessean.com/story/opinion/2019/03/10/tennessee-sunshine-law-trade-secret-open-records/3109008002/.

routine process used to keep the public in the dark.[99] The first step is for the government and private business to enter a nondisclosure agreement, saying that information in any contract with the government should be considered a trade secret under the state open records law.[100] Step two requires they agree not to disclose information to the public even in the meeting where they vote to approve the contract.[101] Typically, the government will even clear news releases with the company before issuing them.[102] And, the final nail in the transparency coffin involves the government notifying the company about public records requests to allow time for the company to intervene in court.[103] At least in Tennessee, some legislators have banded together in an attempt to stop these secretive contracts between the government and private industry. A new piece of legislation[104] in the Tennessee General Assembly, House Bill 370/Senate Bill 1292, aims to curtail the use of the trade secrets exemption to cloak payments from the government to private entity.

Although the legislation in Idaho and Tennessee suggest that some parties are concerned with the erosion of transparency at the state level, the greatest test of how the trade secrets exemption – and the definition of competitive harm – was decided by the U.S. Supreme Court in June 2019 in *Food Marketing Institute v. Argus Leader Media*.[105] At issue were two key issues related to FOIA Exemption 4, which covers trade secrets. It exempts from disclosure "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential."[106]

The Court granted certiorari in *Argus Leader* to clarify whether Exemption 4's use of confidential bore its plain meaning and to determine the proper standard to determine competitive harm. The case arose after a South Dakota newspaper filed a FOIA request with the Food & Drug Administration in 2011 seeking names and sales figures for stores in the U.S. that participate in the federal food stamp program, known as SNAP. Initially, the FDA released some information, but argued other information was confidential business information under Exemption 4. The newspaper appealed the agency decision, and it eventually filed a federal lawsuit. The district court granted the USDA's motion for summary judgment, causing the newspaper to appeal to the Eighth Circuit, who reversed the grant of summary judgment. At trial in the U.S. District Court for the District of South Dakota, the *Argus Leader* prevailed. Applying the *National Parks* test[107] from the D.C. Circuit, which had been adopted by the Eighth Circuit,[108] Judge Karen Schreier ruling the USDA could not prove that releasing sales data would cause substantial competitive harm. "Because the USDA received a small percentage of responses from SNAP retailers, there is little evidence that supports the inference that the majority of SNAP retailers are not concerned about any competitive harm that might stem from the disclosure of individual store data."[109]

---

[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] H.B. 370/S.B. 1292 (Tenn. 2019), http://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=HB0370.
[105] Food Marketing Inst. v. Argus Leader Media, 139 S. Ct. 2356, 2362 (2019).
[106] 5 U.S.C. § 552(b)(4) (2006).
[107] *See* Nat'l Parks & Conservation Ass'n. v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974). "Information is confidential if disclosure of the information is likely to have either of the following effects: (1) to impair the Government's ability to obtain necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained." *Id.*
[108] *See* Contract Freighters, Inc. v. Sec'y of U.S. Dep't. of Transp., 260 F. 3d 858, 861 (8th Cir. 2001).
[109] Argus Leader Media v. U.S. Dep't. of Agric., 224 F.Supp.3d 827 (D. S.D. 2016).

In an unusual (and troubling) twist of facts, the USDA decided not to appeal, but an industry group known as the Food Marketing Institute intervened to prevent the information from being disclosed. A three-judge panel of the Eighth Circuit eventually affirmed[110] the trial court decision, and FMI's petition for *en banc* review was denied. FMI petitioned the U.S. Supreme Court for a writ of certiorari.[111]

In a 6-3 decision, Justice Gorsuch wrote for the Court that FMI did have proper standing under Article III in the case, noting that "it has suffered an actual or imminent injury that is 'fairly traceable' to the judgment below and that could be 'redress[ed] by a favorable ruling.'"[112] Although the Court failed to adopt the standard articulated by FMI, who asserted that confidential should be interpreted to mean "private and not publicly disclosed,"[113] it was not willing to accept the *Argus Leader*'s assertion that "confidential" was a business term of art that requires an evaluation of competitive harm.[114] Instead, the Court carved its own path, with Justice Gorsuch looking at the term's "ordinary, contemporary, common meaning"[115] in 1966 at the time of FOIA's enactment.[116] Relying on his handy copy of Webster's Seventh New Collegiate Dictionary from 1963 as well as a 1961 version of Webster's Third New International Dictionary and the Revised 4th Edition of Black's Law Dictionary, Justice Gorsuch deduced that information that owners share freely cannot be considered confidential.[117] Noting that retailers do not publicly disclose store-level SNAP data, he concluded the information had not been shared freely. Noting that under the SNAP program, the government promises to keep information provided by retailers private, Justice Gorsuch then avoids addressing whether information provided without such a promise would be considered confidential. As a result, the Court ruled that any information customarily and actually treated as private by its owner and provided to the government under an assurance of privacy constitutes confidential information under Exemption 4 of FOIA.

The outcome of the *Argus Leader* case is sure to have substantial impact on open records law across the country. The Court's adoption of the more lenient standards urged by FMI – a plain language approach to confidentiality or the "reasonable possibility" of competitive harm – deals a serious blow to the public's right to access important government information. Whether third parties have the right to intervene to prevent disclosure of information held by the government represents a significant issue in cases involving trade secrets exemption, and a ruling that FMI had no standing would have dramatically limited the ability of private companies to prevent the public from having access to government information. Moving forward, the *Argus Leader* decision likely sets the stage for greater intervention by third parties and stands to prevent significant disclosure of information to the public. In addition, it also opens the door for organizations to balk at providing the government with certain information without a promise of confidentiality.

---

[110] Argus Leader Media v. Food Marketing Inst., 889 F.3d 914 (8th Cir. 2018).
[111] Petition for a Writ of Certiorari, Food Marketing Inst. v. Argus Leader Media, No. 18-48, 2018 WL 5016257 (Oct. 11, 2018).
[112] Food Marketing Inst. v. Argus Leader Media, 139 S. Ct. 2356, 2362 (2019), *quoting* Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149-150 (2010).
[113] *See* Brief for the Petitioner, Argus Leader v. Food Marketing Inst., No. 18-481, 2019 WL 929007 (Feb. 15, 2019).
[114] *See* Brief for the Respondent, Argus Leader v. Food Marketing Inst., No. 18-481, 2019 WL 1310225 (Mar. 18, 2019).
[115] Perrin v. United States, 444 U.S. 37, 42 (1979).
[116] Food Marketing Institute v. Argus Leader Media, 139 S. Ct. 2356, 2362 (2019).
[117] *Id.* at 2363.

The narrowing of the quasi-government doctrine

When government and private entities work together to undertake government businesses, open records and meetings laws occasionally extend to the private entity on the theory that it is acting as a quasi-governmental agency. Although the degree of transparency required of such quasi-governmental agencies varies greatly from state to state, in general, the principle is that at a bare minimum, the quasi-government designation attaches to private entities that are both (1) funded by the government and (2) exist to serve a government function. Examples include operating public facilities such as stadiums and parks, public school bus services, and private prisons and other security services.[118]

In some jurisdictions, such as the federal government, the government must also establish and control the agency. The D.C. Circuit held in 1998, for example, that the Smithsonian museums were not quasi-government agencies subject to FOIA because the federal government had neither created them by statute or other executive-branch action nor controlled them, even though the government funded the Smithsonian, which also had government employees serving on its board.[119]

Some jurisdictions have broader definitions that require private entities to be subject to open records laws. Texas, for example, includes in its definition of "government body" an "agency that spends or is supported in whole or in part by public funds."[120] But even that plain language has been whittled away, rendered almost meaninglessness by courts favoring business privacy over public transparency interests. In 1988, the U.S. Court of Appeals for the Fifth Circuit, reviewing Texas law in *Kneeland v. National Collegiate Athletic Association*, ruled that the Southwest Conference and the NCAA, despite receiving funding from public universities in Texas, were not subject to open records requests under state law because the contract involved a "*quid pro quo*" exchange of money for services that did not involve any additional level of government oversight or control.[121] And shortly after its widely criticized 2015 ruling in *Boeing v. Paxton*, the Texas Supreme Court delivered another blow to transparency by further restricting the application of the Public Information Act in *Greater Houston Partnership v. Paxton*.[122] The court ruled that Greater Houston Partnership (GHP) – a private, nonprofit corporation that essentially serves as a "chamber of commerce" – was not subject to the requirements of the Public Information Act, even though it received funds from the City of Houston and served in an "agency-type relationship" with the city. The state supreme court rejected the plain meaning of the phrase "supported in whole or in part by public funds," which the attorney general and lower courts had relied upon for decades to make similar entities "government bodies" for the purpose of the act. Instead, the court held that "supported" *actually* meant "*sustained* by public funds,"[123] finding the GHP was a *quid pro quo* arrangement with the government, and not one in which the government "maintains" an agency with financial support. Three justices dissented, noting that the majority opinion "discards over forty years of legal interpretations and announces a brand new interpretation that, at best, reflects the Court's concerns instead of the Legislature's language," and finding that the majority's

[118] *See* Rani Gupta, *Privatization v. The Public's Right to Know*, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS 1-5 (Summer 2007).
[119] Dong v. Smithsonian Inst., 125 F.3d 877, 878 (D.C. 1997), *cert. denied*, 524 U.S. 922 (1998).
[120] TEX. GOV'T CODE § 552.003(1)(A)(xii) (Vernon 2018).
[121] Kneeland v. National Collegiate Athletic Ass'n, 850 F.2d 224, 230 (5th Cir. 1988).
[122] Greater Houston Partnership v. Paxton, 468 S.W.3d 51 (Tex. 2015).
[123] *Id*. at 60-61 (emphasis added).

construction was "irreconcilable" with the express language of the statute.[124] Basically, although Texas law says support can be "in whole or in part," the majority opinion wrote out the words "in part" to limit the Public Information Act's application only to bodies that could not exist or survive without government funds, a limitation found neither in the text of the law nor its legislative intent, which expressly calls for liberal construction of the provisions of the law to serve the purpose of the broadest transparency possible.[125]

The "quid pro quo" nature of a relationship with the government – that is, an arms-length bargain for goods or services – is at the heart of many quasi-government determinations, including the aforementioned Fifth Circuit ruling in *Kneeland* between the NCAA and Southwest Conference and the state universities that were members of those groups. The case is often cited in decisions about whether quasi-government bodies are subject to public records laws, both in Texas and out. For example, relying on the logic of *Kneeland*, a Texas court of appeals found that Rural Hill Emergency Medical Services, a not-for-profit organization providing ambulance and other medical transportation services, was not a "government body" even though it received public funding; rather, it was a *quid pro quo* payment for services that was not "so closely associated with the governmental body" in its management or operation to render it subject to the Public Information Act.[126]

But several other state supreme courts have applied the *Kneeland* standard to hold that private entities on contract with governments were quasi-governmental and thus subject to state records laws. These include:

- The Indianapolis Convention and Visitors Association, as a "private not-for-profit corporation that receives revenue from both public and private sources," which the Indiana Supreme Court held was subject to the state's Public Records Law, in part because the amount of money it received was neither negotiated nor designated as fees, but rather dictated by contract as a portion of city hotel-motel taxes.[127]
- The Carolina Research and Development Foundation, a body funded entirely by public funds to benefit the University of South Carolina, led the South Carolina Supreme Court to reach the "unavoidable conclusion that the Foundation is a 'public body'…mandated by the clear language of the FOIA."[128]
- The Greater North Dakota Association, a non-profit pro-business lobbying organization that included "ten state governments which have purchased thirty memberships,"[129] and which the state's attorney general had found to be public body in part because of the public funds it received to publish a magazine. The North Dakota Supreme Court ruled it to be arguably at least enough of a public body to overcome a summary judgment motion, thus supporting the legislature's preference of transparency to read the statute broadly to give "expansive meaning" to its definitions.[130]
- Cherokee Children & Family Services, a not-for-profit corporation providing social services on contract with the Tennessee Department of Human Services, which the

[124] *Id*. at 68.
[125] The majority dismissed this language by saying that "the TPIA's liberal-construction clause" was not a problem here because "even liberal construction must remain grounded in the statute's language and cannot overwhelm contextual indicators limiting public intrusion into the private affairs of non-governmental entities." *Id*. at 62.
[126] CareFlite v. Rural Hill Emergency Med. Serv., Inc., 418 S.W.3d 132, 139 (Tex. App. 2012).
[127] Indianapolis Convention & Visitors Ass'n, Inc. v. Indianapolis Newspapers, 577 N.E.2d 208, 209 (Ind. 1991).
[128] Weston v. Carolina Research & Dev. Found., 303 S.C. 398, 403 (S.C. 1991).
[129] Adams County Record v. Greater North Dakota Ass'n, 529 N.W.2d 830, 832 (N.D. 1995).
[130] *Id*. at 838.

> Tennessee Supreme Court held operated as the "functional equivalent of a government agency," as it received most of its funding from the government and had some level of government control; thus, as part of the state's policy favoring liberal construction of the Public Records Act, was thus subject to requests made under the law.[131]

In *Greater Houston Partnership*, the Texas Supreme Court found that GHP, which was under contract to "provide consulting, event planning, and marketing services to the city of Houston," and was ruled by both the attorney general and the lower court to be a body subject to the Public Information Act in spite of a contract provision that the body was not subject to the Act, was nevertheless part of a "*quid pro quo* arrangement" with the city.[132] Curiously, the majority referenced each of the aforementioned four cases out of Indiana, South Carolina, North Dakota, and Tennessee to support its decision, citing dicta about *quid pro quo* agreements while neglecting to mentioning the actual outcome of those cases to support the dubious proposition that "our sister courts have unanimously construed the phrase ('supported in whole or in part by public funds') to exclude, as a general matter, private entities receiving public funds pursuant to quid pro quo agreements without regard to whether such an agreement is the entity's only funding source."[133] In fact, the only case it cited that reached an outcome denying access to records was from the Ohio Supreme Court, which found that Oriana House, a private non-profit company operating "community-based correctional facilities," was not a public agency subject to the state's Public Records Act. Even though it was largely funded by government and served a historic government function, the entity was not managed on a day-to-day basis by government, nor was it created specifically to avoid the Public Records Act, at least to the point that it could satisfy the "clear and convincing evidence" standard required to establish a private entity as a public office under Ohio law.[134] This evidentiary burden is significantly higher than the broad policy of liberal construction to favor openness stated in the Texas statute.

The lengths to which the Texas Supreme Court was willing to bend both plain language and precedent are indicative of the trend in which quasi-government arguments are being crafted. When a valid quasi-government argument is to be made, a court limits the construction to favor business privacy. When a court rules in favor of transparency, the legislature swoops in to exempt the business from future scrutiny. And now, government agencies have ditched the pretense and engaged in direct collusion with private companies – such as Amazon and Boeing – to shield them from open records laws by notifying them in advance of open records requests. This allows private companies to intervene as third parties in litigation, making such requests an expensive and time-consuming proposition for citizens and journalists.

Conclusion

Privatization has allowed government bodies to surrender public oversight of the entities they pour money into for the purpose of doing government work. By negotiation, by litigation, and by legislation, the government our tax dollars pay to support has come down firmly on the side of business privacy at the expense of transparency. This flies in the face of more than two centuries of democratic philosophy, rooted in the very real and practical concerns of our nation's founders that an unwatched government will necessarily be a corrupt government, and a recognition that, as

[131] Memphis Publ'g Co. v. Cherokee Children & Family Serv., 87 S.W.3d 67, 78-79 (Tenn. 2002).
[132] 468 S.W.3d at 54.
[133] *Id*. at 63.
[134] State ex rel. Oriana House, Inc. v. Montgomery, 854 N.E.2d 193 (Ohio 2006).

Louis Brandeis famously remarked, "Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."[135] Transparency and government accountability are "essential ingredients of 'free consent,' the *sine qua non* of a true democracy."[136]

We are living in a time when unprecedented numbers of public-private partnerships are finding ways to avoid transparency, with the blessing of government groups who seem eager to let businesses hide their activities after receiving public funding, tax waivers, and other government-granted handouts. At the highest level of United States government, we are also witnessing unavoidable entanglements between the Executive Branch and the personal businesses of the president, drawing numerous lawsuits and ethics complaints. The president's businesses received payments from foreign governments; he awarded government contracts and federal jobs to club members from his golf courses; and he operated a hotel in Washington, D.C., on property leased from the federal government that has become a hotspot for conservative lobbyists and donors.[137] An analysis by *USA Today* found that it was largely impossible to tell whether Donald Trump had kept his promises to keep his role as president separate from his entanglements in his private businesses, as "information about his businesses is so secretive … the only way to know whether Trump kept his promise is to take his word for it."[138]

Open records laws exist to make government acts transparent, and classic freedom of information doctrine holds that, although private businesses are not required to be open to public scrutiny, those receiving government funds to do government business should be subject to some level of public oversight. As Pearlman put it, "It's simply unacceptable in a democratic society to permit government to avoid popular oversight and accountability merely by entering into a contract with a private entity."[139] Yet myriad examples demonstrate the ways public bodies have collaborated with private businesses to keep both of their operations in the dark.

How can freedom of information advocates and oversight-minded citizens curb the tide? We offer three potential routes. In short, they are (1) radically rethinking the quasi-government doctrine through legislative amendments to shed light on what has become an increasingly prevalent tactic of government handouts to private businesses with few strings attached; (2) in litigation, emphasizing the broad democratic policies favoring openness that the U.S. Supreme Court has announced in its decisions interpreting the federal Freedom of Information Act, even despite its recent ruling in *FMI v. Argus Leader*; and (3) pushing for legislative limits on the ability of third parties to intervene in the open records request process, particularly when matters are within public officials' discretion rather than laws barring release of certain information.

Reclaiming and expanding the quasi-government doctrine

Countering the trend favoring business privacy over public transparency requires radical rethinking of the quasi-government doctrine, which has become quite narrow and seemingly extends only to situations in which the government establishes, pays for, and directs the private entity doing work on its behalf. But what if the quasi-government doctrine were extended to serve

[135] Louis D. Brandeis, *What Publicity Can Do*, HARPER'S WKLY., Dec. 20, 1913.
[136] Pearlman, *supra* note 20 at 31.
[137] Steve Reilly, Christal Hayes & Bart Jansen, *Did Trump keep his 19 promises to insulate himself from his business? Only he knows*, USA TODAY, March 18, 2019, https://www.usatoday.com/in-depth/news/politics/2019/03/18/president-donald-trumps-promises-didnt-end-business-entanglements/3030377002/.
[138] *Id*.
[139] Pearlman, *supra* note 20 at 78.

the aforementioned "central purpose" of open records laws – that is, to ensure transparency of government operations and decision-making so the public could serve as an effective watchdog for abuse, fraud, waste, and corruption?

Think about it as an "Overton Window" situation. The "Overton Window of Political Possibilities," outlined by political scientist Joe Overton in the 1990s, is the idea is that within a full, wide-ranging spectrum of political ideas on a topic, "only a portion of this policy spectrum is within the realm of the politically possible at any time."[140] For example, on matters of health care in the United States, at one time it may have been less politically palatable – and thus impossible – for single-payer, socialized medicine to be a legitimate consideration at one end of the spectrum; likewise, abandoning long-standing services like Medicare and Medicaid and turning to full privatization is also very likely outside the range of political possibility. But the window can shift with waves of events and public opinion, perhaps broadening the range of political possibilities.[141] The scope of proper discussion about freedom of information laws has been centered on the notion that it is only official acts of government – rather than the conduct of government business – that should be subject to open records laws, with very limited exceptions covering a narrow interpretation of private bodies receiving public funding and other quasi-government agencies. The increase of public-private partnerships and government funding of private operations, though, renders that approach to quasi-government records outdated and ineffectual. The window of debate must now shift, aided by freedom of information advocates and transparency-concerned citizens watching government action increasingly take place behind closed doors. It's a trend that even bothered the most conservative voices on the Texas Supreme Court. Don Willett, a conservative darling and strict constructionist appointed to the Fifth Circuit in 2017 and shortlisted for a U.S. Supreme Court nomination, joined the dissenters in *Greater Houston Partnership*, finding the majority's tortured explanations outside of the bounds of statutory interpretation that he could support.[142] Transparency must be an issue whose appeal transcends partisanship.

Consider multimillion-dollar tax giveaways to private businesses, done ostensibly to serve the public interest through job creation and economic stimulation. The private businesses get all the benefit of government funding without any of the concomitant responsibilities of serving the public interest. One recent example would be the building of the Foxconn LCD screen factory in Wisconsin. Under a deal negotiated by local government bodies and the governor's office, Foxconn would receive nearly $4 billion in public subsidies, with the promise of creating 13,000 jobs and investing $10 billion in the local economy. Local governments are investing hundreds of millions of dollars in land purchases, infrastructure improvements, and "incentive payments" to the private business to lure it to the region.[143] Although some limits exist on how much the government will pay in exchange for what return of jobs and local investment, the extent to which the records generated in these transactions would be open to public inspection to determine

---

[140] Nathan J. Russell, *An Introduction to the Overton Window of Political Possibilities*, MACKINAC CENTER FOR PUBLIC POL'Y (Jan. 4, 2006), https://www.mackinac.org/7504.

[141] *See* Chris Weigant, *Bernie Moves the Overton Window on Single-Payer*, HUFFINGTONPOST, Sept. 13, 2017, https://www.huffingtonpost.com/entry/bernie-moves-the-overton-window-on-single-payer_us_59b9d3dfe4b06b71800c36a3.

[142] Rachel Cohrs, *Texas judge Don Willett is back under consideration to be Trump's next Supreme Court pick*, DALLAS MORNING NEWS, June 27, 2018, https://www.dallasnews.com/news/politics/2018/06/27/texas-judge-don-willett-back-consideration-betrumps-next-supreme-court-pick.

[143] Rick Romell & Molly Beck, *After discussions with Trump, Foxconn says it will build factory in Racine County*, MILWAUKEE J. SENTINEL, Feb. 1, 2019. https://www.jsonline.com/story/money/business/2019/02/01/foxconn-now-says-indeed-build-lcd-factory-wisconsin/2744111002/.

whether the deal actually benefits the public as promised is unclear. Under the Wisconsin Open Records Law, emails of government officials with Foxconn would likely be open for inspection, but Foxconn leaders discussing tax payments and receipt of public dollars and conduct of business in conjunction with those incentives with one another would not be subject to the same scrutiny. The "central purpose" of open records laws – providing oversight of public expenditures used for public purposes – would be frustrated.

In their examination of economic development companies, Edmondson and Davis concluded that from a legislative perspective, sunshine laws "should be rewritten to spell out that quasi-public development entities always must be subject to the law. Such entities might be defined as any entity that utilizes public resources, including tax dollars or office space in public buildings, among other things."[144] This would be a good starting place for freedom of information advocates, particularly in this moment, when large swaths of the public are skeptical about government in general, and tax giveaways to large companies in particular. The main reason the Amazon HQ2 deal in New York fell apart was that it was so unpopular with citizens and activists that it became bad politics for legislators at the local, state, and federal level.[145] The more the public learned about the deal, the worse it sounded, to the point that the pushback was more than Amazon was willing to accept. The "Overton Window" may have opened enough to rethink the definition of when a public entity qualifies as a "government body" or "quasi-government agency" by expanding to include any private business receiving public funds. At the very least, the amount of public funds expended should be made transparent; no legitimate reason justifies the government being able to hide how much it spent to secure the services of an entertainer at a holiday parade. Indeed, an example from Oklahoma demonstrates how interesting (and detailed) these contracts can be. In 2015, *OU Daily*, the student newspaper at the University of Oklahoma, reported the university paid guitar legend Jack White $80,000 to perform a concert, but the contract also revealed the dining preferences of the band, including specifications on how they prefer their guacamole: "We want it chunky."[146]

From multibillion-dollar government handouts to massive private companies to eccentric details in a performer's contract, the public's business is the public's business. When a tax dollar is spent, citizens are entitled to know how and why. As courts have chipped away at this transparency, carving out new exceptions and expanding others in the name of protecting trade secrets and competitive advantages, freedom of information advocates must continue advocating for legislative changes that address business privacy creep.

Don't let SCOTUS get you down

The U.S. Supreme Court rarely hears Freedom of Information Act cases. But when it does, the decisions have the potential to carry significant weight as a statement on democratic principles by the highest court in the country despite only addressing the application and interpretation of federal open records law. Advocates of the right to know should not neglect these important opinions, even when debating policy matters at the state level. Likewise, advocates should not let the Court's adverse ruling in *Food Marketing Institute v. Argus Leader* get them down, as it can

[144] Edmondson & Davis, *supra* note 24 at 340-41.

[145] *See* Seth Fiegerman, *Amazon cancels plans to build New York headquarters*, CNN, Feb. 15, 2019, https://www.cnn.com/2019/02/14/tech/amazon-hq2-nyc/index.html.

[146] Paighten Harkins, *"We want it chunky" and other gems from Jack White's contract with OU*, OU DAILY, Jan. 29, 2015, http://www.oudaily.com/blogs/we-want-it-chunky-and-other-gems-from-jack-white/article_e6b4f946-a804-11e4-a216-4bdde136d4fa.html.

largely be seen as more about the Court's conservative wing opining on statutory construction principles than directly undermining the purpose of FOIA.

As argued above, although the Court's 1989 ruling in *Department of Justice v. Reporters Committee for Freedom of the Press* is decidedly not pro-transparency, the language the Court used to articulate the "central purpose" of FOIA should be used to identify the kinds of records that fall squarely within the ambit of open records laws. How the government spends tax dollars is unquestionably illustrative of the "operations or activities of the government;"[147] indeed, it is hard to imagine any record held by government to be more reflective of how our elected and appointed officials conduct the public's business.

Before *FMI v. Argus Leader*, the Roberts Court's FOIA decisions had been more favorable toward transparency under FOIA. In 2011, the Court decided two cases in favor of disclosure and against asserted privacy interests. In *FCC v. AT&T*, the Court unanimously ruled against AT&T as a third-party intervener, when it asserted a corporate privacy right in its letters from the federal regulatory agency as an expansion of "personal privacy" in the language of Exemption 7(C).[148] Although Chief Justice Roberts did not get into the fundamental purposes underlying FOIA – as a constructionist, he is less moved by legislative intent, and more likely to turn to statutory language and a dictionary in his decisions[149] – he certainly, in his writing, illustrated how exemptions detailed by Congress in FOIA should be read, favoring "ordinary meaning" and consistency within the context of the statute. The majority declined, for example, to invoke other areas of privacy law such as the Fourth Amendment or double jeopardy to expand the reach of the personal privacy provision, noting, "this case does not call upon us to pass on the scope of a corporation's 'privacy' interest as a matter of constitutional or common law."[150]

Shortly after *FCC v. AT&T*, the Court again ruled in favor of transparency and narrow construction of exemptions, but this time with more discussion of FOIA's purpose. *Milner v. Department of the Navy* concerned a citizen's request for "data and maps used to help store explosives at a naval base" that was denied by the Navy on grounds that the requested materials were "personnel matters" under Exemption 2.[151] Justice Kagan, writing for the Court and joined by Chief Justice Roberts, said the 12 words in Exemption 2, "related solely to the internal personnel rules and practices of an agency," could not be read in a way that plausibly included data and maps about explosives, turning to the dictionary for examples of what "personnel" meant in plain language.[152] But she went on to invoke FOIA's preference for broad disclosure of government records, coupled with narrow interpretations of exemptions in furtherance of that purpose:

> We would ill-serve Congress's purpose by construing Exemption 2 to reauthorize the expansive withholding that Congress wanted to halt. Our reading instead gives the exemption the "narrower reach" Congress intended, through the simple device of confining the provision's meaning to its words.[153]

---

[147] 489 U.S. at 775

[148] 562 U.S. at 400.

[149] *See* James J. Brudney & Lawrence Baum, *Oasis or Mirage: The Supreme Court's Thirst for Dictionaries in the Rehnquist and Roberts Eras*, 55 WM. & MARY L. REV. 483, 522 (2013) (noting that Roberts used a dictionary in 35.7 percent of his decisions regarding statutory interpretation between 2005 and 2010, tying Justice Thomas for the highest rate of justices on the court for that entire time period).

[150] 562 U.S. at 407.

[151] Milner v. Dep't of the Navy, 562 U.S. 562, 564-65 (2011).

[152] *Id*. at 569.

[153] *Id*. at 571-72.

These are important points for freedom of information advocates. Narrow construction of exemptions serves the purpose of open records laws by setting transparency and openness as the default positions for government records. When a government agency fears the consequences of transparency, it may, as Justice Kagan pointed out, "seek relief from Congress," rather than requiring the courts to rewrite legislative acts to address those concerns.[154] This approach cuts both ways, as Justice Gorsuch detailed in *FMI v. Argus Leader*, undoing 45 years of lower court precedent and Congressional acceptance of that interpretation through inaction in reading that "confidential" in Exemption 4 meant only what the dictionary said in 1966, and not what courts had interpreted it to mean in the half a century since. But the decision itself was not a broadside at FOIA or an endorsement of corporate privacy; rather, it was an exercise in statutory construction that the right wing of the Court has embraced to undo court discretion in interpreting the meaning and purpose of federal laws. It was purpose agnostic; according to Gorsuch, FOIA has no purpose other than what the dictionary says.

In the face of this, if legislative purpose and practical functioning of laws is meaningless without specific words to support them, freedom of information advocates should push for a statement of purpose in FOIA that mirrors similar statements in state laws, which courts have often relied upon to favor transparency. The statement of purpose in the Texas Public Information Act, for example, specifically notes the "American constitutional form of representative government that adheres to the principle that government is servant and not the master of the people" as a driving factor in the law, establishing that "The people insist on remaining informed so that they may retain control over the instruments they have created," and thus the Public Information Act "shall be liberally construed to implement this policy" of transparency.[155] As noted above, the history of FOIA is replete with similar examples favoring transparency, both legislatively and in the courts. And though there is no explicit presumption in FOIA favoring openness, Congress has recognized that one has seemingly emerged; the Committee on Government Reform in 2005 commented that FOIA "establishes a presumption that records in the possession of agencies and departments of the executive branch of the U.S. government are accessible to the people."[156]

And when, in the absence of strong pro-transparency language explicitly in FOIA, the Supreme Court hands down purpose-agnostic decisions that favor secrecy, right-to-know advocates should push for quick revisions to the law to fix the problem the Supreme Court creates. Within days after the ruling in *FMI v. Argus Leader,* Congressional leaders began to express disapproval of the decision. Senate Judiciary Chairman Chuck Grassley said he would work on legislation to correct the ruling, with which he disagreed. "In a self-governed society, the people ought to know what their government is up to," Grassley said in a statement on the Senate Floor three days after the Supreme Court ruling. "Transparency laws like the Freedom of Information Act help provide access to information in the face of an opaque and obstinate government."[157] Grassley also commented in his inimitable Twitter style:

[154] "All we hold today is that Congress has not enacted the FOIA exemption the Government desires." *Id*. at 581.
[155] Texas Gov't Code § 552.108.
[156] H.R. 109-226, *supra* note 34 at 2.
[157] Chuck Grassley, *Grassley on the Importance of the Freedom of Information Act*, June 27, 2019. https://www.grassley.senate.gov/news/news-releases/grassley-importance-freedom-information-act.

> Americans deserve 2kno what their govt is up to Freedom of Information Act designed to promote transparency when govt lacks openness but recent SCOTUS ruling+EPA &Interior regs undermine FOIA I will write legislation 2fix TRANSPARENCY BRINGS ACCOUNTABILITY[158]

Where right-to-know advocates should be concerned, and where they should push back the hardest, is against anti-transparency dicta that has emerged in recent years. In *McBurney v. Young*, a 2013 case that held that Virginia could deny records requests made by people who were not citizens or residents of the state without offending the U.S. Constitution's Privileges and Immunities Clause.[159] Justice Alito did not entirely reject the important transparency goals of state public records laws, recognizing that Virginia's FOIA "essentially represents a mechanism by which those who ultimately hold sovereign power (*i.e.*, the citizens of the Commonwealth) may obtain an accounting from the public officials to whom they delegate the exercise of that power."[160] And although Justice Alito was quite dismissive of any constitutional grounds for transparency, his dicta overreached in pointing out the relative newness of freedom of information laws and concluding they lacked importance because "there is no contention that the Nation's unity foundered in their absence."[161] The "workable balance" language favored by Justice Gorsuch in *FMI v. Argus Leader* likewise undermined decades of expressions of legislative purpose and court interpretation of words meant to make FOIA functional. It will be up to Congress, pushed by advocates for transparency, to make the law so explicit it cannot be undone by strict adherence to the dictionary and turned into more misinformed dicta regarding the importance of transparency to the American style of government.

Limit third-party intervention

Perhaps the most troubling trend in recent years is the readiness with which governments are willing to allow, and encourage, private entities to intervene in court to assert reasons to keep records closed, as well as the willingness of government and quasi-government bodies to collaborate in this behavior, as evidenced by the New York and Virginia promising secrecy to draw Amazon headquarters to their regions. It is particularly troubling when private businesses engage in this tactic to deny or delay access to records that are well within a government body's discretion to disclose under freedom of information laws, even if an exemption may apply.

Exemptions or exceptions in public records laws are often discretionary rather than mandatory. If an exemption applies, the government is not completely barred from disclosing the record; rather, it may choose not to provide the record to the requester. For example, the exemptions to the federal Freedom of Information Act do not create an affirmative right to privacy for all matters encompassed in them. Instead, FOIA's language says that the law "does not apply to matters" in the exemptions.[162] Permissive language – that exemptions "may" (not "shall" or "must") be invoked to avoid disclosure – rather than mandatory language is present throughout the

[158] Chuck Grassley (@ChuckGrassley), Twitter (June 26, 2019, 12:17 p.m.), https://twitter.com/ChuckGrassley/status/1143961565080760320.
[159] McBurney v. Young, 569 U.S. 221 (2013).
[160] *Id*. at 228.
[161] *Id*. at 234.
[162] 5 U.S.C. § 552(b) (2018).

law enforcement records exemption.[163] So when AT&T intervened to prevent the FCC from disclosing regulatory letters under FOIA, it did so not by asserting an affirmative right to have the records protected in the name of corporate privacy, but rather in an effort to compel a court to determine that Exemption 7(C) prohibited disclosure by the FCC. When the Supreme Court ultimately denied AT&T's request, it had been *seven years* since the initial FOIA request was made.[164]

Likewise, in *Boeing v. Paxton*, Boeing intervened as a third party regarding application of a discretionary exception to the Texas Public Information Act. The law says that information that "would give advantage to a competitor or bidder" is "excepted from requirements" of the Act – not that it is affirmatively deemed private and confidential.[165] A Texas government body has the discretion to release this information, even if it finds that the statutory exception applies. The Boeing employee seeking the records filed his records request in 2005; [166] Boeing was allowed to intervene, against the objection of the attorney general, litigating the case up to the state's highest court, which issued a decision *ten years* later saying that, indeed, the Port Authority of San Antonio was not mandated by law to release the documents. *Food Marketing Institute v. Argus Leader*, began with a request by the newspaper in 2011; the Department of Agriculture chose not to appeal a bench trial ruling in favor of disclosure in 2016, but the third-party trade group intervened to continue litigating to preserve its claims of business privacy after losses at the district court and the Eighth Circuit.[167] It took eight years from the time the request was made for the Supreme Court to reverse decades of FOIA jurisprudence and ultimately deny access to the records.

Argus Leader raised the argument that Food Marketing Institute, as a trade industry group, should not have standing to intervene in what is ultimately a discretionary decision by a federal agency. However, the USDA "represented unequivocally that, consistent with longstanding policy and past assurances of confidentiality to retailers, it 'will not disclose' the contested data unless compelled to do so" by a court. The Supreme Court essentially found this surrender of statutory discretion to agency policy to be equivalent to a statutory mandate, dismissing the standing argument and allowing FMI to intervene.[168]

The ability of private companies to intervene in discretionary matters bestows upon them an enormous procedural advantage to run out the clock on requesters, employing attorneys at costs that private citizens or freedom of information advocates simply cannot match. As a U.S. House of Representatives committee considering FOIA revisions in 2016 found, the greatest barrier to access is "Delay, Delay, Delay," [169] a situation that is exacerbated when third-party litigation and appeals enter the process. When an affirmative right to privacy is invoked – such as under the federal Privacy Act[170] or Family Educational Rights and Privacy Act[171] – that would mandate agencies to protect individual privacy, it makes more sense to allow third parties to intervene to

[163] *See* 5 U.S.C. § 552(c)(1)(B) ("the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section").
[164] *See* In the Matter of FCC Communications Inc.; On Request for Confidential Treatment, 45 Comm. Reg. (P&F) 1335 (2008).
[165] TEXAS GOV'T CODE § 552.104(a).
[166] Boeing Co. v. Abbott, 412 S.W.3d 1, 6 (Tex. App. 2012).
[167] Argus Leader Media v. Dep't of Agric., 889 F.3d 914, 916 (8th Cir. 2018).
[168] Food Marketing Inst. v. Argus Leader Media, 139 S. Ct. 2356, 2362 (2019).
[169] U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, FOIA IS BROKEN: A REPORT 34 (2016).
[170] Privacy Act of 1974, Pub. L. No. 93-579 (1974).
[171] Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380 (1974).

assert those rights. Otherwise, their intervention into discretionary matters has a deleterious effect on the freedom of information process, creating stronger incentives for secrecy and disincentives for transparency, counter to the fundamental purpose at the heart of open records laws.

A troubling trend toward secrecy when private entities receive public funds to serve government functions has emerged. But the trend does not guarantee a final destination. Using the strategies detailed above, freedom of information advocates can combat encroachments on the transparency that our democracy demands, resist judicial and legislative efforts to narrow the scope of public transparency, and reclaim the important role of citizen oversight of government business.

The Journal of Civic Information

Volume 1 | Number 1 September 2019

Journal homepage: https://journals.flvc.org/civic/ ISSN (online): 2641-970X

Access to Government Officials in the Age of Social Media

Katie Blevins & Kearston L. Wesner *

Article Information

Received: Jan. 21, 2019

Accepted: Feb. 13, 2019

Published: Sept. 4, 2019

Keywords

Freedom of information
Right to know
Public records
Government transparency
Social media
Public forum

Abstract

As social media platforms have become more pervasive, there has been a concomitant increase in the number of government officials using their personal social media accounts to perform official government duties. Most notably, President Donald Trump continues to use his personal Twitter account, established in 2009, prior to his presidency, to conduct a variety of official tasks. While the First Amendment's Free Speech Clause traditionally protects an individual's right to engage in self-expression, the Supreme Court has not unequivocally recognized an affirmative right to know as an extension of the First Amendment. Recent court decisions suggest this may change. This study addresses the contours of public access to government officials on social media. Specifically, it considers the circumstances in which government officials are likely to be held to a standard of accountability and the case for treating public officials' social media accounts as public forums, including how factors relating to account ownership and content impact that analysis.

* Katie Blevins, University of Idaho; Kearston L. Wesner, Quinnipiac University. Please send correspondence about this article to Katie Blevins at katieblevins@uidaho.edu. An earlier version of this work was presented at the National Freedom of Information Coalition summit FOI Research Competition, April 12, 2019, in Dallas, Texas.

To cite this article in Bluebook: Katie Blevins & Kearston L. Wesner, *Access to Government Officials in the Age of Social Media,* 1(1) J. CIVIC INFO 30 (2019).
To cite this article in APA: Blevins, K., & Wesner, K. L. (2019). Access to government officials in the age of social media. *Journal of Civic Information, 1*(1), 30-58.

DOI: https://doi.org/10.32473/joci.v1i1.115658

Introduction

As social media platforms have become more pervasive, with unprecedented levels of engagement, there has been a concomitant increase in the number of government officials using personal social media accounts to perform official government duties. Most notably, President Donald Trump continues to use his personal Twitter account, which he established in 2009 prior to his presidency, for a variety of official tasks, from making policy announcements to interacting with constituents and world leaders.[1] Trump's Twitter account has even been characterized as "one of the White House's main vehicles for conducting official business."[2] Sean Spicer, then-White House Press Secretary, acknowledged in 2017 that Trump's tweets are "considered official statements by the President of the United States."[3] This position is consistent with the Presidential Records Act of 1978, which defines "Presidential records" to include materials that the President creates "in the course of conducting activities which relate to or have an effect upon the carrying out of the constitutional, statutory or other official or ceremonial duties of the President."[4]

Social media platforms have become ubiquitous among those with access to the internet.[5] In 2005, just 5% of American adults used a social media platform.[6] As of 2018, Facebook, the most prominent social media platform, was used by 68% percent of American adults, 75% of whom access the platform daily.[7] In all, in 2018 Facebook had 1.49 billion daily users, and 2.27 billion monthly users.[8] Twitter is used by nearly one-quarter of all adults; notably, 45% of the 18-to-24 demographic uses Twitter. Other social media platforms reflect similar staggering growth, especially among that 18-to-24 demographic. Snapchat and Instagram are particularly popular; the former is used by 78% of that population, and the latter is used by 71%.[9] Even the non-traditional social media platform YouTube is used by 73% of adults and 94% of the 18-to-24 population.

Unsurprisingly, political figures have embraced social media to reach their constituents. These officials have also found themselves in a legal quagmire connected to their use of social media to deliver official messages. When these officials block constituents or deny them access to social media posts concerning official duties, what, if any, First Amendment claims are raised? Traditionally the First Amendment's free speech clause protects an individual's right to speak and engage in self-expression. However, the Supreme Court has not unequivocally recognized an affirmative right to know as an extension of the First Amendment. This might be changing.

In May 2018, the United States District Court for the Southern District of New York confronted this question in the context of President Trump's practice of liberally blocking users

---

[1] Donald Trump (@realDonaldTrump), TWITTER, https://twitter.com/realDonaldTrump.
[2] Knight First Amendment Inst. v. Trump, 928 F.3d 226 (2d Cir. 2019).
[3] Aric Jenkins, *Sean Spicer Says President Trump Considers His Tweets 'Official' White House Statements*, TIME (June 6, 2017), http://time.com/4808270/sean-spicer-donald-trump-twitter-statements/.
[4] 44 U.S.C. § 2202. *See Knight First Amendment Inst*., 928 F.3d at 232 (discussing the application of the Presidential Records Act to President Trump's tweets).
[5] Even in the United States, access to internet is not universal. In 2000, only 50% of Americans had access to the internet. As of 2018, 89% of American adults use the internet. Pew Research Center, *Internet/Broadband Fact Sheet*, 2018, PEW RESEARCH CENTER (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/internet-broadband/.
[6] Aaron Smith & Monica Anderson, *Social Media Use In 2018*, PEW RESEARCH CENTER (Mar. 1, 2018), http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/.
[7] *Id.* Facebook is also notable for a variety of other reasons: it is the largest global social media platform, and its users reflect a wide variety of demographics.
[8] FACEBOOK NEWSROOM, https://newsroom.fb.com/company-info/.
[9] Smith & Anderson, *supra* note 6.

who spoke out or disagreed with him on Twitter.[10] In holding that this practice violated the First Amendment, the court decried Trump's practice of "viewpoint-based exclusion."[11] On appeal, the United States Court of Appeals for the Second Circuit agreed that public officials who use social media accounts to conduct official business cannot block people who have expressed disagreement.[12] That court, however, declined to rule on the more general constitutional question of whether elected officials can exclude individuals from private social media platforms.[13]

Similar issues have arisen elsewhere. For example, in June 2018, a Missouri resident sued a state representative for violating his First Amendment rights by blocking him on Twitter.[14] And in January 2019, a federal court in Virginia held that an elected official violated the First Amendment by blocking a constituent on Facebook,[15] and a federal court in Wisconsin granted summary judgment, holding that three Wisconsin state representatives unconstitutionally blocked a liberal advocacy group on Twitter.[16] These issues will, in all likelihood, continue to spread, given the widespread use of social media by elected officials to reach constituents, as well as a general shift in officials' Twitter "habits" that parallel Trump's approach.[17]

The question this study addresses is this: What are the boundaries of public access to government officials on social media? Traditionally, statutes like FOIA, the Government in the Sunshine Act, and the Presidential Records Act have governed the public's access to official government information. However, the variable of social media use has changed the traditional calculus and raised important questions about the intersection of technology, transparency, and the First Amendment.

This study uses traditional legal research methodology. First, it reviews Supreme Court jurisprudence regarding an affirmative right to know, in order to establish the foundation for the study. Second, it examines the courts' statutory interpretation to clarify the boundaries of public access. And third, it assesses court decisions regarding access to officials' social media accounts as a springboard to explore the relevant legal issues. Throughout the study, the following questions are answered: Under what circumstances are government officials likely to be held to a standard of accountability? What case can be made for a public forum argument? Does this determination depend on whether the social media account is "personal" or "official"? Does the content posted

---

[10] *Memorandum and Order*, Knight First Amendment Inst. at Columbia Univ. v. Trump, 1:17-cv-05205-NRB (S.D.N.Y. May 23, 2018), https://knightcolumbia.org/sites/default/files/content/Cases/Twitter/2018.05.23%20Order%20on%20motions%20for%20summary%20judgment.pdf.

[11] *Id.*

[12] *Knight First Amendment Inst.*, 928 F.3d at 230. According to the court, "[T]he First Amendment does not permit a public official who utilizes a social media account for all manner of official purposes to exclude persons from an otherwise-open dialogue because they expressed views with which the official disagrees."

[13] *Id.*

[14] *Complaint*, Campbell v. Reisch, 2:18-CV-04129-BCW (W.D. Mo. June 27, 2018), https://www.columbiatribune.com/assets/MO30424628.PDF.

[15] Davison v. Randall, 912 F.3d 666 (4th Cir. 2019). *See* James M. LoPiano, *Public Fora Purpose: Analyzing Viewpoint Discrimination on the President's Twitter Account*, 28 FORDHAM INTELL. PROP., MEDIA AND ENT. L.J. 511, 516 n. 23 (2018) (discussing various lawsuits brought by constituents against government officials who had blocked them on Facebook or Twitter).

[16] *Opinion and Order*, One Wisconsin Now v. Kremer, 3:17-cv-00820-wmc, at *28-29 (W.D. Wis. Jan. 18, 2019), https://drive.google.com/file/d/1OtytYQFFgRZFXqUoVZtfvHnI_lw1SZMn/view.

[17] Ann Marimow, *Trump's Twitter Habits Are Affecting How Local Politicians Behave Online*, WASHINGTON POST, Mar. 5, 2019, https://www.washingtonpost.com/local/legal-issues/trumps-twitter-habits-are-affecting-how-local-politicians-behave-online/2019/03/25/bd8bd94c-4be1-11e9-93d0-64dbcf38ba41_story.html?utm_term=.5a88dabc190a.

to the account suggest that the account was intended as a public forum? And how does the legal question of access to a public official's social media account fit into our current First Amendment jurisprudence, specifically regarding transparency and a "right to know"?

Clarifying these issues is critical for a variety of audiences: government agencies ensuring that officials' social media use complies with applicable law; FOI advocates fighting for government transparency; and access practitioners seeking to engage with elected officials and exercise their voices. Absent clarification, access to the accounts of public officials is, at best, under threat.

The Supreme Court and the right to know

The right to know, defined as the public's right to access government-controlled information in the form of records, can be found in common law, statutes, and early administrative law at both the state and federal levels. But this right has a complicated and muddled history.

It was articulated as far back as 1787, before the U.S. Constitution was ratified, when Constitutional framer James Wilson argued that Congress was obligated to publish its proceedings. He said, "[The] people have a right to know what their Agents are doing or have done, and it should not be in the option of the Legislature to conceal their proceedings."[18] Despite Wilson's passionate defense of the right to know, no clear scholarly consensus suggested that the Founders intended citizens to have access to government information.[19] Although the Founders may have discussed concepts related to a right to know, these ideas were presented as a political ideal, not a concrete right.[20] FOI pioneer and advocate Harold L. Cross, who contributed much of the rationale undergirding modern federal freedom of information law, argued, however, that the history of free speech and press "bars any notion that the men of 1791 intended to provide for freedom to disseminate such information but to deny freedom to acquire it."[21]

The modern right to know initially appeared in early 20th century Supreme Court opinions.[22] Beginning in the 1930s, the Supreme Court struggled with whether, and then how, to

---

[18] *Journal of the Federal Convention August 11th 1787*, FREEREPUBLIC.COM, http://www.freerepublic.com/focus/f-bloggers/2762059/posts. This quote comes directly from the *Journal of the Federal Convention* from August 11, 1787. This is an historical version of the origination of a right to know that Brian Richardson, respected journalistic ethicist at Washington and Lee University, recognized in one of his publications. Brian Richardson, *The Public's Right to Know: A Dangerous Notion*, 19(1) J. MASS MEDIA ETHICS 46, 46 (2004). Eventually, the Constitution adopted Wilson's argument, saying, "Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy; and the Yeas and Nays of the Members of either House on any question shall, at the Desire of one fifth of those Present, be entered on the Journal." U.S. CONST. art. 1 § 5.

[19] *See* Martin Halstuk, *Policy of Secrecy--Pattern of Deception: What Federalist Leaders Thought About a Public Right to Know*, 1794-98, 7 COMM. L. & POL'Y 51 (2002).

[20] Despite this generally accepted academic view, some instances suggest that the Founders intended to provide for a certain level of governmental transparency. James Wilson's stance that the Legislature should publish their proceedings so that "people have a right to know what their Agents are doing or have done" seems to demonstrate an early preoccupation with a right to know. *Journal of the Federal Convention August 11th 1787*, FREEREPUBLIC.COM, http://www.freerepublic.com/focus/f-bloggers/2762059/posts.

[21] HAROLD L. CROSS, THE PEOPLE'S RIGHT TO KNOW: LEGAL ACCESS TO PUBLIC RECORDINGS AND PROCEEDINGS 131-132 (Columbia Univ. Press 1953).

[22] *Grosjean v. American Press Co.* (1936), the first case to state a First Amendment link to information, invalidated a Louisiana law that taxed newspapers with a circulation of more than 20,000 copies weekly. The newspaper publishers successfully argued that this law violated their First Amendment free speech rights. In a unanimous opinion, Justice Sutherland wrote a compelling history of taxation on the press in pre-colonial England. He explained that these taxes

recognize a constitutional right to know. Five Supreme Court justices endorsed a limited but constitutionally enforceable right to know during their various tenures.[23] However, extending any constitutional right is fraught with problems for the judiciary because critics fear that this activity reflects unbridled judicial activism. Yet some constitutional rights exist only because justices elected to extend the shadow of certain constitutional protections. This gray area, or shadow, of the Constitution is known as the penumbra.

Legally, the penumbra comprises the implicit rights granted by a constitution. The concept originated in Justice Stephen J. Field's majority decision in the 1871 case *Montgomery v. Bevans*.[24] Penumbral rights have been articulated in different ways. In 1873, Supreme Court Justice Oliver Wendell Holmes disparagingly referred to the penumbra as a "gray area where logic and principles falter."[25] And in a variety of opinions during his lengthy tenure as a U.S. Court of Appeals judge for the Second Circuit, Judge Learned Hand used the idea of a penumbra when referring to ideas that he deemed poorly defined and/or unclear.[26]

While it is true that penumbral rights have been treated with suspicion and hostility, the fact is that certain deeply valued rights only exist by virtue of the penumbra. In 1965, the Supreme Court created a penumbral right to privacy when it invalidated a Connecticut law that banned contraceptives.[27] In the majority opinion, Justice Douglas noted that the "First Amendment has a penumbra where privacy is protected from governmental intrusion. In like context, we have protected forms of "association" that are not political in the customary sense, but pertain to the social, legal, and economic benefit of the members."[28] More than 50 years have passed since that decision, during which the right to privacy has become entrenched in our jurisprudence.

The Supreme Court's First Amendment decisions implicate a constitutionally protected right to know. These cases contain reasoning in majority opinions, dicta, and even dissenting opinions demonstrating that Supreme Court justices have repeatedly considered or assumed that a right to know exists within the penumbra of the First Amendment. This nearly 100-year record clarifies the judiciary's current position regarding government officials' use of social media accounts.

As a threshold matter, relevant Court decisions also speak in terms of a constitutional right to receive information, which was firmly established by the 1960s. For example, in *Stanley v.*

---

were designed to limit the circulation of ideas contrary to the monarchy. The opinion noted that the Framers rejected these limitations and created the First Amendment. Grosjean v. Am. Press Co., 297 U.S. 233, 250-51 (1936).

[23] Justice Douglas was the most significant advocate for a right to know, though Justices Brennan, Powell, Marshall, and Stevens were equally inclined at times. DAVID O'BRIEN, THE PUBLIC'S RIGHT TO KNOW: THE SUPREME COURT AND THE FIRST AMENDMENT 60 (Praeger 1981). Justice Brennan, for example, said, "It is a mistake to suppose that the First Amendment protects only self-expression, only the rights to speak out. I believe that the First Amendment in addition fosters the values of democratic self-government." *Id*. at 143. None of these justices currently occupy the bench of the Supreme Court. Concerning this endorsement, the five justices who supported a right-to–know incurred criticism from the majority of their peers. Justice Stewart, for example, argued that extending a right to know to the constitutional penumbra would constitute an unacceptable level of judicial activism. *Id*. at 62.

[24] Montgomery v. Bevans, 17 F. Cas. 628 (9th C.C.D. Cal.) (1871). This is the case that historically has been referred to as first referencing the idea of a penumbra legally. The case concerned Mexican land grants under the Van Ness ordinance, not a topic that on its surface ties to modern discussions of a penumbra. *Id*.

[25] Oliver Wendell Holmes, *The Theory of Torts,* 7 AM. L. REV. 652, 654 (1873). Citing the penumbra is not a common legal idea. Four judges are responsible for the majority of decisions referencing a penumbra: Oliver Wendell Holmes Jr., Learned Hand, Benjamin N. Cardozo, and William O. Douglas. *See* Burr Henley, *'Penumbra': The Roots of a Legal Metaphor*, 15(1) HASTINGS CONST. L.Q. 81 (1987).

[26] Henley, *supra*, at 87-89.

[27] Griswold v. Connecticut, 381 U.S. 479, 479 (1965).

[28] *Id.* at 483.

Georgia, a search of someone's home turned up obscene materials that were illegal under Georgia law.[29] Even though these materials clearly violated applicable law, the Court refused to criminalize the mere possession of private obscene material. In its holding, the Court protected the individual's First Amendment right to free expression, saying, "[I]t is now well established that the Constitution protects the right to receive information and ideas."[30]

The cases analyzed in this section are divided into two areas: access to publicly available information, and access to government information.

Access to publicly available information

Cases regarding the access to publicly available information help resolve the question of whether the public can successfully assert a right to know and demand access to a government official's social media account. President Trump's Twitter feed, for example, is publicly available. It is only when Trump blocks users that they lose the ability to access his accounts.[31] When they are blocked, the users lose the ability "to view the President's tweets, to directly reply to those tweets, or to use the @realDonaldTrump webpage to view the comment threads associated with the President's tweets."[32] These cases involve analogous instances in which the public was denied access to information that was otherwise publicly available. The majority of cases fall within this category.

These cases reveal two important points regarding a presumed right to access government officials' social media accounts. First, the Supreme Court has repeatedly held that an individual's right to know is heightened when the desired information is necessary to further the goals of participatory democracy. And second, the government is prohibited from contracting the knowledge available to citizens or creating an undue burden on citizens who seek that information.

The right to know furthers the goals of participatory democracy

The right to know is perhaps most pronounced when the information at issue involves participation in the political process. Indeed, the Court has explicitly and unequivocally stated the importance of citizens' right to know in a democratically elected state. In *Marsh v. State of Alabama*, the Court stated that "citizens … must make decisions which affect the welfare of the community and nation. To act as good citizens, they must be informed. In order to enable them to be properly informed their information must be uncensored."[33]

As such, the Court has afforded ample protection for an individual's right to *receive* information.[34] Perhaps the clearest and most directly relevant example involved the Supreme Court

[29] Stanley v. Georgia, 394 U.S. 557, 557 (1969). Specifically, law enforcement officials entered Stanley's home with a warrant and searched it in connection with illegal bookmaking activities. In the course of the search, officers found films that they viewed and deemed as obscene, confiscating them and arresting Stanley. *Id*.

[30] *Id.* at 564 (1969).

[31] In August 2018, President Trump was forced to unblock over forty users who had been blocked from his public Twitter account after a U.S. district judge ruled in May that blocking users violated their First Amendment rights. David Shepardson, *Trump Unblocks More Twitter Users After U.S. Court Ruling*, REUTERS (Aug. 29, 2018), https://www.reuters.com/article/us-usa-trump-twitter/trump-unblocks-more-twitter-users-after-u-s-court-ruling-idUSKCN1LE08Q.

[32] *Knight First Amendment Inst.*, 928 F.3d at 232.

[33] Marsh v. Alabama, 326 U.S. 501, 508 (1946).

[34] *See* text accompanying notes 29-30, *supra*.

upholding the right of individuals to receive political information. In *Lamont v. Postmaster General*, the Court analyzed a section of the Postal Service and Federal Employees Salary Act of 1962, which required the Postmaster General to deliver communist mailings only upon the recipient's affirmative request.[35] The Court determined that the postmaster's actions both in withholding information *and* requiring individuals to request the mailings were unconstitutional.[36] The Court rationalized that people should be able to receive information in the mail without first having to clear these hurdles.

The Court also considered the right to receive information as a political speech issue in *First National Bank of Boston v. Bellotti*.[37] In *Bellotti*, the Court examined the issue of whether corporations had a First Amendment right to make monetary contributions to help influence the political process.[38] The appellants in this case, a national association of banks and corporations, wanted to spend money to publicize their political view on a referendum to enact a new tax.[39] They were constrained by an existing Massachusetts statute that made it a crime for organizations to make political contributions or expenditures intended to sway voters.[40] In a 5-4 ruling, the Court held that corporations have the right to make contributions to the political process.[41] According to Justice Powell in the majority, this case is less about the rights of the corporation *per se* than the public's right to the information pertaining to the political contributions.[42]

This basic principle was again articulated in *Board of Education v. Pico*, a suit brought by schoolchildren who protested the school board's removal of "anti-American, anti-Christian, anti-Semitic, and just plain filthy" texts from district's junior high and high school libraries.[43] In a plurality decision, Justice Brennan wrote that students had a First Amendment right to access available information in the library so they could become more informed citizens.[44] As the *Pico* Court explained:

> [J]ust as access to ideas makes it possible for citizens generally to exercise their rights of free speech and press in a meaningful manner, such access prepares students for active and effective participation in the pluralistic, often contentious society in which they will soon be members.[45]

While the students obviously could not demand the school board purchase certain books, they had a right to obtain existing information, even in venues, like public schools, that have traditionally limited First Amendment rights.

In a comparatively significant context, two Supreme Court cases involving the distribution of religious information held that the First Amendment protects both the right to distribute *and to receive* literature. These cases, which involved the prosecution of Jehovah's Witnesses for illegally distributing religious tracts, recognized that the receipt of information is critical to perpetuating

[35] Lamont v. Postmaster Gen., 381 U.S. 301, 301 (1965).
[36] *Id.*
[37] First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765 (1978).
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.* at 776-77.
[43] Bd. of Educ. v. Pico, 457 U.S. 853, 853 (1982). This was done contrary to the recommendations made to the school board by a committee of parents and school staff. *Id*.
[44] *Id.* at 854.
[45] *Id.* at 868.

democratic ideals. In *Martin v. City of Struthers*, the Court conceded that although distributing literature door-to-door may be "a nuisance," it nevertheless enables "citizens to engage in the dissemination and discussion of ideas, per democratic tenets."[46] According to the Court, "Information enriches public discourse and is a fundamental component of deliberative democracy."[47] Echoing the Court's rationale in *Martin*, the Court in *Marsh v. Alabama* emphasized the privileged role of information in a representative democracy.[48]

The cases thus far involve political information fairly directly, but the Court has read this interest broadly. It has asserted that some information, though not specifically political in nature, can still be vital to participatory democracy. Society as a whole is concerned with preserving democratic principles in ways that fall outside traditional political debate or discourse.[49] The Supreme Court evaluated these issues in two cases concerning access to reproductive information that is commercial in nature.[50]

First, in *Bigelow v. New York*, the Court invalidated a Virginia statute that made it a misdemeanor to circulate advocacy that helped individuals procure an abortion. The Court said that citizens were entitled to receive this information – an advertisement that included "information and counseling" for New York abortion services – because it was "factual material of clear 'public interest.'" [51]

And second, in *Virginia State Pharmacy Board v. Virginia Citizens Consumer Council*, the Court found unconstitutional a statute barring pharmacists from advertising prescription drug prices.[52] Consumers who challenged the statute argued that it prevented them from comparing prices of prescription medications.[53] The Court recognized that this impacted consumers, especially "the poor, the sick, and particularly the aged," who had a vested interest in obtaining this life-or-death information.[54] This interest was of the highest concern: "As to the particular consumer's interest in the free flow of commercial information, that interest may be as keen, if not keener by far, than his interest in the day's most urgent political debate."[55] Therefore, the consumers had a right to know, which stemmed from traditional free speech principles. According to the Court, "Freedom of speech presupposes a willing speaker. But where a speaker exists, as is the case here, the protection afforded is to the communication, *to its source and to its recipients*

---

[46] Martin v. City of Struthers, 319 U.S. 141, 143 (1943).
[47] *Id.*
[48] Marsh v. Alabama, 326 U.S. 501, 508 (1946).
[49] Virginia State Pharmacy Bd. v. Virginia Citizens Consumer Council, 425 U.S. 748, 763 (1976).
[50] This articulation is particularly interesting because commercial speech traditionally receives reduced First Amendment protection, yet the Court deemed these issues so critical that it was compelled to rule in favor of protection. Originally, commercial speech was not protected under the First Amendment. *See* Valentine v. Chrestensen, 316 U.S. 52 (1942). The Supreme Court eventually developed a test which provided for limited protection for commercial speech, known as the *Central Hudson* test. This test asks four questions to determine whether the restriction on speech passes constitutional muster:

1) Is the speech concerning a lawful activity and not misleading?
2) Is the asserted government interest substantial?
3) Does the regulation directly address the government interest?
4) Is the regulation more extensive than necessary to meet that interest?

The government bears the burden of proof in this test. *See* Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557 (1980).
[51] Bigelow v. Commonwealth of Virginia, 421 U.S. 809, 812 & 822 (1975).
[52] Virginia State Pharmacy Bd., 425 U.S. at 748 (1976).
[53] *Id.*
[54] *Id.*
[55] *Id.* at 763.

both."[56] Access here functioned as a mechanism to thwart paternalism and ignorance.[57] This decision was driven by an analysis of democratic principles and societal interests.[58]

The *Bigelow* and *Virginia State Pharmacy Board* cases may appear to be outliers because they involve sensitive medical information. However, the Court has decided other pure commercial speech cases similarly. The Court protected commercial speech interests in real estate "For Sale" and "Sold" signs, asserting that the "societal interest in 'the free flow of commercial information' […] is in no way lessened by the fact that the subject of the commercial information here is realty rather than abortions or drugs."[59] It also prioritized the public's interest in receiving advertisements from attorneys over the State Bar of Arizona's interest in propounding professional values by restricting those same commercial advertisements.[60]

The principles intrinsic to these cases would support protecting an individual's access to public officials' social media posts. Being able to view and respond to policy announcements and statements associated with the officials' duties is critical to participatory government. Without access, fruitful dialogue is stymied.

The government cannot contract available knowledge or impose an undue burden on obtaining information

The government cannot act capriciously by curbing knowledge to which the public already has access.

This issue has arisen with some frequency in cases involving access to reproductive health information, from sex education to contraceptive counseling for couples and information for sexual assault victims. The cases have uniformly upheld the individual's right to obtain critical health information. In *Griswold v. Connecticut*, for example, the Court invalidated a statute that criminalized dispensing contraceptives or *information about contraception*.[61] The executive director of the Planned Parenthood League of Connecticut and its medical director, a licensed physician, were convicted as accessories under this statute, partly for providing contraceptive devices to couples, and partly for giving "information, instruction, and medical advice" to stop conception.[62] The Court specifically articulated the individuals' right to know, saying that the "right of freedom of speech and press includes not only the right to utter or to print, but the right

[56] *Id.* at 756.
[57] *Id.* at 770 (decrying the board's "highly paternalistic approach" that functions to "keep[ ] the public in ignorance."
[58] Extending Justice Blackmun's argument, society may also benefit from protecting consumer information. Using the informed democracy approach, Blackmun noted that "[a]dvertising, however tasteless and excessive it sometimes may seem, is nonetheless dissemination of information as to who is producing and selling what product, for what reason, and at what price. So long as we preserve a predominantly free enterprise economy, the allocation of our resources in large measure will be made through numerous private economic decisions. It is a matter of public interest that those decisions, in the aggregate, be intelligent and well informed. To this end, the free flow of commercial information is indispensable." *Id.* at 765.
[59] Linmark Assocs., Inc. v. Township of Willingboro, 431 U.S. 85, 92 (1977)
[60] Bates v. State Bar of Ariz., 433 U.S. 350, 364-65 (1977). Justice Blackmun quoted from Arizona Justice Holohan's dissenting opinion in the lower court, which said, "Obviously the information of what lawyers charge is important for private economic decisions by those in need of legal services. Such information is also helpful, perhaps indispensable, to the formation of an intelligent opinion by the public on how well the legal system is working and whether it should be regulated or even altered. . . The rule at issue prevents access to such information by the public." *Id*. at 358.
[61] Griswold v. Connecticut, 381 U.S. 479, 479 (1965) (emphasis added).
[62] *Id.* at 480.

to distribute, the right to receive, the right to read."[63] As a result, "[T]he State may not, consistent with the spirit of the First Amendment, contract the spectrum of available knowledge."[64] Even Justice Stewart acknowledged in his dissent that had the directors of Planned Parenthood merely advised people on the use of contraceptives, they would have had a strong First Amendment free-speech claim.[65]

This same rationale guided the Court in *Pico*.[66] The students in *Pico* protested the widespread censorship of materials in the library, but access to those materials was critical. Once the information was generally made available to the students, the school board could not limit that information without substantial justification, and certainly not with an eye to "prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion."[67] While the students obviously could not demand that the school board purchase certain books, they had a right to obtain existing information, even in venues like public schools, which traditionally have limited First Amendment rights.

Similarly, the government cannot impose an undue burden on citizens exercising their right to know certain information. This is why the Court rejected the postmaster's claims in *Lamont*. It declined to allow the postmaster to impose any type of duty on recipients to affirmatively request communist literature.[68]

In the context of social media accounts, otherwise public accounts that contain political content, such as President Trump's account, should be made available for users to access. These accountholders should be prohibited from engaging in viewpoint discrimination to block users. Purported "solutions" that impose barriers on blocked individuals to regain access are insufficient. Demanding that blocked individuals engage in additional actions to access content would contravene existing right-to-know and undue-burden cases. The only effective solution is to provide legally robust protections that protect users *from* being blocked to begin with.

Access to compelled government information

This study has thus far focused on accessing information that was or could be publicly available, such as political and religious information, reproductive health information, and commercial information. The issues presented are far different when that information is not generally available to the public. A narrower and more contentious line of cases purport to establish what rights, if any, individuals have to *compel* the release of government information. If a public official has a private social media account, is there a First Amendment justification for making that account public?

---

[63] *Id.* at 482.
[64] *Id.*
[65] *Id.*
[66] *See* Bd. of Educ. v. Pico, 457 U.S. 853 (1982), discussed *supra* in text accompanying notes 43-45.
[67] *Id.* at 871-872.
[68] Lamont v. Postmaster Gen., 381 U.S. 301, 301 (1965). Historically, the Courts are hesitant to impose any barriers to gathering information. Although the context was wildly different, the Court demonstrated the same commitment to the free flow of information when it invalidated the "segregate and block" portions of the Cable Television Consumer Protection and Competition Act of 1992. Denver Area Educ. Telecomms. Consortium, Inc. v. FCC, 518 U.S. 727 (1996). These provisions required cable providers to block "patently offensive" programming, which could be restored only after the consumer sent in a written request. *Id.* at 754. The Court said these provisions were "overly restrictive, sacrificing important First Amendment interests for too speculative a gain." *Id.* (internal citations and quotations omitted).

Typically, the Court has declined to force the government to reveal information. Because the Constitution lacks an explicit right to know information, individuals lack a mirror right to compel that information.

This rationale has been used in several cases, all involving access to jails or prisons, to deny journalists access to information. In *Pell v. Procunier,* the Supreme Court held that the media has "no constitutional right of access to prisoners or their inmates beyond that afforded the general public."[69] Similarly, in *Saxbe v. Washington*, the majority held that prohibiting interviews between the press and federal inmates was constitutional because it "does not deny the press access to sources of information available to members of the general public."[70] Finally, the Court, in *Houchins v. KQED*, rejected a radio and television broadcaster's request to enter the county jail.[71] Like the *Saxbe* Court, it noted that the press had alternative avenues, such as federal access statutes, to obtain pertinent information.[72] In the plurality opinion, Justice Warren Burger said, "This Court has never intimated a First Amendment guarantee of a right of access to all sources of information within government control."[73] In terms of a right to know, the public and press only have a freedom to "communicate information once it is obtained," not to force information to be revealed.[74]

This rationale has also been used to exclude the press and public from criminal trials. In *Richmond Newspapers v. Virginia,* the Supreme Court evaluated the constitutionality of closed criminal trials and closed records concerning these trials.[75] The Court considered the First Amendment implications of excluding the public and press.[76] The various opinions in this case articulated that the right to attend criminal trials is covered within an existing and protected First Amendment right to know.[77] Criminal trials had historically been open,[78] which helped ensure the veneer of justice because attendees could confirm the fair treatment of accused criminals.[79] Justice Burger also stated that the freedoms of speech and the press entail a right to gather information by attending trials.[80] Under the First Amendment's right to receive information and ideas, the free

[69] Pell v. Procunier, 417 U.S. 817, 834 (1974).
[70] Saxbe v. Washington, 417 U.S. 843, 843 (1974).
[71] Houchins v. KQED, Inc., 438 U.S. 1, 1 (1978).
[72] *Id.* at 14. Additionally, although the conditions in the jail are of great public importance, the media are "ill-equipped" to deal with prison administration. *Id*. at 8.
[73] *Id.* at 9. This quote from the Court implies that there are definitely circumstances where the First Amendment does protect a limited right to know, much like the federal access statutes. This case is just an instance where that right to know does not extend.
[74] *Id.* at 2. Justice Stevens, in a dissent with Justices Brennan and Powell, protested on the grounds that excluding the press and public could raise intermediate scrutiny issues. He acknowledged that the "Court has never intimated that a nondiscriminatory policy of excluding entirely both the public and the press from access to information about prison conditions would avoid constitutional scrutiny." *Id*. 19-27 (Stevens, J., dissenting).
[75] This was the first time that access to trials was specifically examined. The *Richmond* Court discussed *Gannett Co. v. DePasquale ,* 443 U.S. 368 (1979), a similar decision, in which the Supreme Court examined the right of access to hearings and pretrial motions. In *DePasquale*, the trial judge closed the defendant's fourth murder trial at the behest of his defense counsel, who sought to reduce prejudicial publicity. Although the appellant's counsel cautioned that constitutional rights could be implicated in the closure, the trial judge ordered the trial closed and excluded both the press and public. Richmond Newspapers v. Virginia, 488 U.S. 555, 564 (1980).
[76] Richmond Newspapers 488 U.S. at 558.
[77] *Id.* at 556.
[78] *Id.* at 569 (stating that "criminal trials both here and in England had long been presumptively open"). For a more detailed history of openness of trials in England and the U.S., *see id*. at 564-69.
[79] *Id.* at 572. Justice Brennan and Justice Marshall also pointed out the need for ensuring a fair trial in their special concurrence. *Id*. at 557.
[80] *Id.* at 576. Justice Burger also drew upon the right to assemble in conjunction with the free speech and press clauses. *Id*. at 577-78.

speech and press clauses "prohibit [the] government from summarily closing courtroom doors that had long been open to the public at the time the First Amendment was adopted."[81]

In a special concurrence,[82] Justice Stewart wrote that while the First and Fourteenth Amendments gave the public and press the right to attend all trials, both criminal and civil, this right was limited.[83] Some circumstances, including space limitations, safety concerns, and privacy of minors, could warrant limiting the attendance of the press and/or the public at trial.[84]

Justice Stevens, in a regular concurrence, noted the precedential importance of this case: "[F]or the first time, the Court unequivocally holds that an arbitrary interference with access to important information is an abridgement of the freedoms of speech and of the press protected by the First Amendment."[85] This case demonstrates that press members, as representatives of the public, realize rights equal to the public's. *Richmond* does not just grant a First Amendment right to attend criminal trials; it also *creates* a limited First Amendment right to know because it includes access to records related to those trials. Although this First Amendment right to know is limited, previous cases clarify that the Supreme Court intends a reciprocal constitutional protection for access to some categories of government information as well as freedom of expression.

This guarantee of openness also extends to the *voir dire* examination of jurors.[86] In *Press-Enterprise Co. v. Superior Ct. (Press-Enterprise I),* the Court clarified that the principle of openness also covered the records generated during *voir dire*.[87] In this instance, records functionally replace attendance at *voir dire* proceedings, indicating that there should be equal weight given to attendance at meetings and trial proceedings and records from those meetings and proceedings.

Similarly, in *Press-Enterprise Co. v. Superior Ct. (Press-Enterprise II)*, the Supreme Court held that preliminary hearings are "sufficiently like a trial" to justify comparable openness.[88] Although the defendant's right to a fair and impartial trial must be balanced against the public's right of access, the "explicit Sixth Amendment right of the accused is no less protective of a public trial than the implicit First Amendment right of the press and public."[89] This includes access to preliminary hearings in person, and, when these hearings are closed for specific reasons, eventual access to transcripts of these hearings. To withhold even a transcript would "frustrate what [the Court has] characterized as the "community therapeutic value" of openness."[90]

The Supreme Court offers significantly less guidance in determining whether a public official can keep private an otherwise public social media account. There are some limited

[81] *Id.* at 576. This extension of the First Amendment to protection of criminal trials was argued as natural by Justice Burger. Access to trials is an implicit part of the penumbra of the First Amendment. *Id*.

[82] A special concurrence is one where the justice agrees with the Court's disposition but not its opinion. This is in contrast to a regular concurrence, where the justice agrees with the Court's disposition and opinion.

[83] Richmond Newspapers, 488 U.S. at 598-601. In Justice Burger's opinion, the issue of attendance at civil cases was not addressed, but Burger acknowledged that "historically both civil and criminal trials have been presumptively open." *Id.* at 569.

[84] *Id.* at 598-601.

[85] *Id.* at 583.

[86] Press-Enterprise Co. v. Superior Ct., 464 U.S. 501, 501-505 (1984). The process of jury selection is "itself a matter of importance, not simply to the adversaries but to the criminal justice system." In this ruling, Justice Burger echoed the reasoning from *Richmond*, citing the history of openness of trial proceedings as well as the use of openness to enhance the actual and perceived fairness of criminal trials. *Id*. at 501-505

[87] *Id.* at 512 (stating that "[w]hen limited closure is ordered, the constitutional values sought to be protected by holding open proceedings mat be satisfied later by making a transcript of the closed proceedings available").

[88] Press-Enterprise Co. v. Superior Ct., 478 U.S. 1, 12 (1986).

[89] *Id.* at 7.

[90] *Id.* at 13.

circumstances where the Supreme Court has compelled the government to provide information to the public under an extension of the First Amendment, although this extension has been limited to checks on the judicial and criminal process. It is likely that private social media accounts of public officials would not rise to this narrow standard and the expectation is that they could remain semi-private.[91]

Statutory access to government information

Although the overview of relevant Supreme Court cases[92] clarified that the Court recognizes a substantive right to know, there are inadequate discrete mechanisms in place to safeguard that constitutional right.[93] The right to know may be a presumed penumbral right, but it is not explicitly articulated in the First Amendment.[94] To tackle this problem, the federal government has instead relied on statutes to delineate the boundaries of government transparency and outline the precise contours of the public's legal right to know about government affairs.[95]

Reliance on statutes to safeguard these vital rights, however, presents two serious issues. First, statutes are ill-equipped to combat the inertia of long-standing government opacity. Statutory relief can be painfully slow and yield, at best, inconsistent results. Furthermore, statutes are inherently less stable than fundamental constitutional protections. They are more easily altered and subject to political whims. And second, transparency statutes apply only to records under government control. While these statutes may cover many records desired by individuals seeking access, certain critical documents are outside the statute's ambit. This section of the study addresses both issues and ultimately suggests that mutable statutory solutions should be eschewed in favor of strengthened constitutional protections.

---

[91] These accounts could remain only semi-private because the courts have consistently ruled that we do not have an expectation of privacy in a legal sense to most electronic communications, especially on semi-public forums like social networking sites. It is unlikely that a right to know would extend a *requirement* that public officials automatically make public an otherwise private account, or mandate that all constituents be "friended" to access an otherwise private account.

[92] *See* discussion *supra* section "The Supreme Court and the right to know," p. 33.

[93] Kent Cooper, then Director of the Associated Press, stated that the right to know is not explicitly mentioned by the Constitution but that there *should* be a constitutional right to know. KENT COOPER, THE RIGHT TO KNOW: AN EXPOSITION OF THE EVILS OF NEWS SUPPRESSION AND PROPAGANDA 17 (1956). *See, e.g.,* Houchins v. KQED, 438 U.S. 1 (1978); Pell v. Procunier 417 U.S. 817 (1974); Saxbe v. Washington Post Co., 417 U.S. 843 (1974).

[94] These "unenumerated" nature of these rights leave them particularly vulnerable to challenge. For example, the Supreme Court's decision in *Roe v. Wade* has protects a penumbral right of privacy. The resulting opinion rests on a "shaky foundation," which many scholars anticipate will be challenged. *See* Harold R. Demoss, Jr. & Michael Coblenz, *An Unenumerated Right: Two Views on the Right of Privacy*. 40 TEX. TECH L. REV. 249, 258 (2008).

[95] See, e.g., Freedom of Information Act, 5 U.S.C. § 552 (1991 & Supp. 2003); Government in the Sunshine Act, 5 U.S.C. § 552b (2011); Federal Advisory Committee Act, 5 U.S.C. App (1972). State access laws originated much earlier than similar federal laws. Alabama passed the first comprehensive open meetings law in 1915 and was still the only state in 1950 to have one. ANN TAYLOR SCHWING & CONSTANCE TAYLOR, OPEN MEETING LAWS 6-7 (Fathom 1994). Many states that had not yet passed open records laws did so in the wake of the Watergate scandal, as concerns about government transparency grew considerably during this time. State open meetings laws were generally passed later. Florida passed the first state open meeting law in 1967. All fifty states now have some form of open record and meetings laws. *Id.* at 3.

Statutory protection yields inconsistent results

Relying on statutes to protect the right of access has yielded, at best, inconsistent results. These statutes are ill-equipped to tackle the unique challenges presented by entrenched government opacity. This study will use the most prominent federal statute, the Freedom of Information Act (1966) (FOIA), to illustrate the dangers presented by this inconsistency.

In 1955, U.S. Rep. John E. Moss (D-Calif.), the reform-minded chair for the Special Government Information Subcommittee, sought to assess issues regarding government transparency. He launched congressional hearings regarding the Administrative Procedures Act, a predecessor to FOIA.[96] The hearings, which occurred before the eventual enactment of FOIA, lasted for ten years and involved hundreds of witnesses.[97] Not a single agency supported the proposed law.[98] The bill that would eventually become FOIA, S. 1160, painstakingly proceeded through several iterations before its passage by the Senate in 1965 and House in 1966.[99] President Lyndon B. Johnson eventually signed the bill into law – reluctantly.[100] The law's enactment rendered nearly 100 governmental agencies accountable to public demands for information.[101] Still, numerous entrenched institutional barriers perpetuated an atmosphere of secrecy. Many agencies, accustomed to long-standing opacity, were disinclined to produce records that satisfied citizens' requests. And, worse, most agencies assumed that executive privilege would supersede FOIA, an attitude that sustained the government's preferred policy of secrecy.[102]

The dangers of inertia revealed themselves again in 1996 when FOIA was updated and amended by the Electronic Freedom of Information Act (E-FOIA).[103] One significant provision of E-FOIA was that it redefined agency records to include information archived in any format, including electronic documents.[104] Prior to E-FOIA, the guaranteed right of access did not include electronic records.[105]

More clearly than any other amendment, E-FOIA revealed a chasm between innovation – specifically technical innovation – and legislative action. The existence of this gap threatens the

---

[96] JAMES T. O'REILLY, FEDERAL INFORMATION DISCLOSURE 2:02, 2-5 (1994). Congressman Moss was instrumental in establishing the groundwork necessary to document systematic manipulation of governmental transparency by the executive branch. *Id.* at 11.

[97] *Id.* at 2-5. Of all the witnesses representing agencies, none supported the FOIA. *Id.* at 3-8, 3-9.

[98] *Id.* at 3-8-9 (1994).

[99] JAMES T. O'REILLY, FEDERAL INFORMATION DISCLOSURE 2:4 (1990).

[100] President Johnson's signed the bill believing, "[t]his bill in no way impairs the President's power under our Constitution to provide for confidentiality when the national interest so requires. There are some who have expressed concern that the language of this bill will be construed in such a sway as to impair Government operations. I do not share this concern." JAMES T. O'REILLY, FEDERAL INFORMATION DISCLOSURE 2:5 (1990). President Johnson obviously believed that the FOIA would have no real impact on the state of government transparency.

[101] Freedom of Information Act, 5 U.S.C. § 552 (1991 & Supp. 2003). Notably, the FOIA does not apply to records held by Congress, state and local governments, the courts, private individuals and entities, the President and the President's personal staff or advisors. Nine exemptions address certain categories of information that agencies may withhold from public disclosure: (1) classified and national security information; (2) internal agency personnel information; (3) information exempted by statutes; (4) trade secrets and confidential business information; (5) agency memoranda; (6) disclosures of personal privacy; (7) records of law enforcement and investigations; (8) some reports of financial institutions; (9) geological and geophysical information. *Id*.

[102] JAMES T. O'REILLY, FEDERAL INFORMATION DISCLOSURE 15 (1990).

[103] *See* Pub. L. 104-231, 110 Stat. 3048, §§ 1-2 (1996) (amending sections of 5 U.S.C. § 552).

[104] Pub. L. 104-231, 110 Stat. 3048, §§ 1-2 (1996) (amending sections of 5 U.S.C. § 552).

[105] Martin Halstuk & Bill Chamberlin, *Open Government in the Digital Age,* 78(1) JOUR. AND MASS COMM. 45, 45 (2001). Prior to 1996, judges determined appropriateness of access to electronic information, case-by-case. *Id.* at 48.

public's right to access crucial information.[106] Even after E-FOIA's passage, its actual implementation was sluggish. To illustrate, a public interest group examining 57 agencies two full years after passage of E-FOIA showed that not a single agency had fully complied with E-FOIA's provision requiring agencies to publish on the internet.[107] Even in the face of a clear directive, agencies still embraced outmoded mechanisms to support access.

Another issue is that statutes are inherently more susceptible to amendment and political whim than fundamental constitutional protections.[108] For example, the Department of Justice, which is often subject to political pressure from the executive branch, has the statutory responsibility for overseeing FOIA compliance.[109] In reality, federal regulatory and administrative agencies self-regulate. The Supreme Court has been complicit in these agency tactics since the 1970s. In fact, many Supreme Court decisions have clearly contravened FOIA's purpose – reducing the categories of information available, and preferentially balancing competing interests, such as confidentiality and privacy.

Transparency statutes are limited to records under government control

Transparency statutes have always been limited to records under government control. FOIA applies to records held by federal agencies and departments, including the Executive Office of the President,[110] but it does not apply to records held by Congress, the judiciary, private corporations, or private citizens.[111]

During the 1970s and '80s, several Supreme Court decisions limited FOIA to a *reactive* statute. According to the Court, FOIA could not compel government agencies to create documents; it could only require those agencies to release documents already in existence.[112] Even if lawfully created agency records did exist, but were misplaced outside of agency jurisdiction, those records could not be compelled.[113] Furthermore, records generated by private companies that contracted with the government could not be considered agency records unless they were held by federal executive agencies.[114]

---

[106] *Id.* at 57.

[107] Jennifer Henderson & Patrick McDermott, *Arming the People "…With The Power Knowledge Gives": An OMB Watch Report on the Implementation of the 1996 "EFOIA" Amendments to the Freedom of Information Act,* OMB Watch (1998), *cited in* Martin E. Halstuk, *Speed Bumps on the Information Superhighway: A Study of Federal Agency Compliance with the Electronic Freedom of Information Act of 1996,* 5 COMM. L. & POL'Y 423, 424 (2000).

[108] In other words, FOIA is *not* subject to "strict scrutiny" – the highest level of scrutiny required to settle constitutional questions pertaining to free speech, free assembly, and freedom of the press rights. Legal Information Institute, *Strict Scrutiny* (2010), http://www.law.cornell.edu/wex/strict_scrutiny.

[109] Freedom of Information Act, 5 U.S.C. §552 (1991 & Supp. 2003); Government in the Sunshine Act, 5 U.S.C. §552b (2011).

[110] Freedom of Information Act, 5 U.S.C. § 552 (1991 & Supp. 2003). FOIA also covers records of independent regulatory agencies, such as the Federal Communications Commission, the Securities and Exchange Commission, and so on.

[111] *Id*. FOIA also does not apply to state or local governments.

[112] N.L.R.B. v. Sears, Roebuck & Co., 421 U.S. 132, 162 (1975) (holding that an agency cannot be compelled to "produce or create explanatory material" pursuant to a document request).

[113] Kissinger v. Reporters Committee for Freedom of the Press, 445 U.S. 136, 139 (1980) (holding that federal courts have no authority to compel requested documents in the possession of a party that is not an agency).

[114] Forsham v. Harris, 445 U.S. 169, 171-172, 184 (1980) (holding that "written data generated, owned and possessed by a privately controlled organization receiving federal study grants are not 'agency records'" under FOIA, and that the agency must *actually obtain* the record for it to be deemed a record).

Federal employees have taken advantage of this loophole, either inadvertently or intentionally. A 2015 Government Business Council survey of 412 federal employees found that 33% of surveyed employees use personal email at least sometimes.[115] Unless agencies establish specific protocols, email sent using a personal device means that the agency does not have a copy of that record, putting it outside of agency control. Thirty-one percent of respondents indicated that their agency did not archive personal email involving government business; another 47% stated that they did not know their agency policy.[116] Twenty-seven percent of respondents cited "potential FOIA requests" as a reason that inhibits candid internal email communication within their department/agency.[117]

It seems insufficient to use mutable statutory protections to guarantee access to even a retroactive record of public officials' social media accounts. Not only are existing transparency statutes inconsistently used, leading to uneven distribution of public records, the majority of the social media accounts at issue would not even constitute a public record under existing definitions. Social media accounts are owned by private corporations, and the government does not have the power to compel those records to be made publicly available.

Access to public officials' social media accounts

The "right to know" cases addressed thus far in this study[118] analyzed the individual's general right to access information, whether that information is already publicly available or the individual is seeking to compel its release. None of these cases, however, have addressed the specific issue of accessing public officials' speech on social media. And the statutory protections safeguarding access to information are inconsistently applied, inapplicable, or ineffective.

This section analyzes the question of when a public official's social media account should be deemed a public forum. It first discusses the parameters of forum analysis, considering the various guidelines used to ascertain whether a space, whether physical or virtual, qualifies as a public forum. Next, this section briefly addresses, and rejects, the application of the "government speech" doctrine to the issues presented here. Then, it conducts an in-depth analysis of the most salient Supreme Court case, *Packingham v. North Carolina*,[119] in which the Court discussed the status of social media as a public forum. It finally turns to an analysis of the two main factors that courts should consider when assessing the public forum status of a social media account:

(1) Is the account "personal" or "official"?
(2) Does the content posted to the account suggest that it is intended to function as a public forum?

Although these issues are not in and of themselves determinative, they provide guidance to courts considering whether to preserve the right of the public to access the account.

[115] Daniel Pitcairn & Zoe Grotophorst, *The State of Internal Workplace Communication*, GOVERNMENT EXECUTIVE (Mar. 5, 2015), https://www.govexec.com/insights/state-internal-workplace-communication/106737/.
[116] *Id.*
[117] *Id.*
[118] *See* discussion *supra* section "Supreme Court and the right to know," p. 33.
[119] Packingham v. North Carolina, 137 S. Ct. 1730 (2017).

Forum analysis

The question of whether, and to what extent, government officials can block constituents or limit their access to official social media posts depends on how these social media accounts are characterized. The government's authority to restrict or limit speech is defined by the forum in which that speech occurs. There are four types of fora, each of which entails varying levels of First Amendment Protection: nonpublic fora, traditional public fora, designated public fora, and limited public fora.[120] When speech occurs in a public forum, the government's ability to regulate discourse is severely constrained.

Some spaces are nonpublic fora. In these spaces, the government can impose various speech restrictions as long as they are reasonable.[121]

On the opposite end of the spectrum are traditional public fora, which receive the highest level of First Amendment protection. These fora include physical spaces, like streets and parks, that are traditionally used by the public to assemble and discuss public questions.[122] To curb speech in these spaces, the government must demonstrate that the regulation survives strict scrutiny; thus, it must show it has a compelling state interest, and its restriction(s) must be narrowly tailored.[123] The government can also impose content-neutral time, place or manner restrictions.[124]

In the middle are designated public fora and limited public fora. Designated public fora include spaces specifically set aside by the government for public speech and expression. These designated public fora are entitled to the same heightened First Amendment protection as traditional public fora. However, they lack the same robustness of traditional public fora because the government is still entitled to reclassify a designated public forum as a private space.[125] Thus, protecting free speech in these spaces is, to some extent, subject to government whim.[126] Limited public fora are different because they allow enhanced speech restrictions according to "the limited and legitimate purposes for which [the space] was created."[127] The government opens the space for public discourse, but it can limit the content of conversation within that space. In these spaces, the government is only prohibited from engaging in viewpoint discrimination.[128]

Public forum analysis cases often speak in terms of physical space, but the concept of a "public forum" is far broader. In *Rosenberger v. Rector and Visitors of University of Virginia*, the Supreme Court held that the University of Virginia engaged in unconstitutional viewpoint discrimination when it denied a Christian student organization's reimbursement request to the Student Activities Fund ("SAF").[129] Even though the SAF was a forum "more in a metaphysical than in a spatial or geographic sense," the same analysis applies.[130] By opening up SAF funds to

---

[120] *See* Lyrissa Lidsky, *Public Forum 2.0*, 91 B.U. L. REV. 1975 (2011), http://scholarship.law.ufl.edu/facultypub/155. Lidsky's article addresses the "maze of categories" involved in determining what level of scrutiny to apply to government speech restrictions.
[121] Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 46 (1983).
[122] *Id.* at 45.
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] Lyrissa Lidsky refers to designated public fora as "a vexed First Amendment category thanks to an ambiguous footnote in the . . . *Perry* decision." Lidsky, *supra* note 120, at 1983.
[127] Rosenberger v. Rector & Visitors of Univ. of Virginia, 515 U.S. 819, 829 (1995).
[128] *Id.*
[129] *Id.*
[130] *Id.*

student organizations, UVA created a "limited public forum" and was limited by the attendant boundaries, among which is a restriction on viewpoint discrimination.

Lyrissa Lidsky's article, *Public Forum 2.0*, notes that "[b]etween the extremes of no interactivity and full interactivity, it is difficult to predict whether courts will label a government-sponsored social media presence a public forum or not."[131] Certainly, a social media account may qualify as a public forum. As Lidsky noted, "[I]nteractive social media can foster citizens' First Amendment rights to speak, receive information, associate with fellow citizens, and petition government for redress of grievances."[132] However, absent a clear indication from the government official that the account is intended to serve as a public forum, the court will be required to analyze the account's characteristics and use to make this determination. The official's intent can be inferred from "'policy and practice' and whether the property is of a type compatible with expressive activity."[133] If the government official has created a limited public forum, then speakers can be excluded for "reasonable and viewpoint neutral" reasons.[134] This would not protect officials targeting users who express contrary views.

The U.S. Court of Appeals for the Second Circuit, considering the characteristics of Trump's account, determined that it functioned as a public forum:

> The Account was intentionally opened for public discussion when the President, upon assuming office, repeatedly used the Account as an official vehicle for governance and made its interactive features accessible to the public without limitation. We hold that this conduct created a public forum.[135]

It also noted that "[i]f the Account is a forum – *public or otherwise* – viewpoint discrimination is not permitted."[136] Thus, it was unconstitutional for Trump to block users based on viewpoint.

Application of the government speech doctrine

As noted above, the government is prohibited from engaging in viewpoint discrimination in public fora. One exception to this rule is the government speech doctrine. Under this doctrine, "[t]he Free Speech Clause does not require the government to maintain viewpoint neutrality when its officers and employees speak" about official business.[137] When the government is the speaker, it may make "content-based choices" to ensure its message is conveyed properly.[138] This doctrine enables the government to "take legitimate and appropriate steps to ensure that its message is neither garbled nor distorted."[139]

The contours of the doctrine can be seen in cases such as *Walker v. Texas Division, Sons of Confederate Veterans, Inc.*[140] In *Walker*, the Supreme Court held that the Texas Department of Motor Vehicles Board could reject a specialty license plate design featuring a Confederate flag.

---

[131] Lidsky, *supra* note 120, at 1977.
[132] *Id.* at 1978.
[133] *Id.* at 1984.
[134] *Id.* at 1989.
[135] Knight First Amendment Inst. v. Trump, 928 F.3d 226, 237 (2d Cir. 2019) (emphasis added).
[136] *Id.*
[137] Matal v. Tam, 137 S. Ct. 1744, 1757 (2017).
[138] Rosenberger v. Rector and Visitors of Univ. of Virginia, 515 U.S. 819, 833 (1995).
[139] *Id.* (discussing application of the doctrine in situation where the government uses public funds to promote its message), and citing Rust v. Sullivan, 500 U.S. 173, 194 (1991).
[140] Walker v. Texas Div., Sons of Confederate Veterans, Inc., 135 S. Ct. 2239 (2015).

Although individuals order and pay extra for specialty license plates, these plates convey government speech.[141] License plates include messages from and about the states, including pertinent graphics, slogans, and messages.[142] States are not required to adopt various messages with which they prefer not to identify. The state can "choose how to present itself and its constituency."[143] Texas, which retained authority over the license plate designs, clearly did not intend specialty license plates to serve as any type of public forum.[144] Thus, it opted not to issue a license plate bearing a Confederate flag because it did not want to be perceived as embracing that message.

The Supreme Court also considered the issue of government speech in *Matal v. Tam*, which invalidated the disparagement clause of the Lanham Act.[145] In *Matal*, a rock singer sought to trademark his group name, "The Slants," which is a derogatory term aimed at the Asian population.[146] The band members, who are Asian-American, sought to "reclaim" the derogatory term.[147] The U.S. Patent and Trademark Office (PTO) denied the application because it violated a provision of the Lanham Act that prohibited registering trademarks that "disparage" individuals, beliefs, or institutions.[148] The PTO unsuccessfully argued that trademarks constitute government speech, and that by issuing a trademark for "The Slants," it would be perceived as the speaker of a derogatory term.[149] In rejecting the PTO's argument, the Court noted that none of the factors present in *Walker* inhered in *Tam*.[150] A registered trademark is not typically perceived as government messaging, unlike the messages on license plates. The government isn't unwillingly thrust into the role of "speaker" by a trademark.

The government speech doctrine serves two main principles. It protects the government from adopting messages that it does not want to adopt, and it ensures the government's message is insulated from distortion. One measure to achieve the latter goal may ostensibly be curbing criticism that confuses the government's messaging.[151] But can government officials silence critics on social media to ensure the sanctity of their messaging?

Government speech is notably different from the government use of social media. This difference was articulated by the Fourth Circuit in *Davison v. Randall*.[152] When a government official invites discourse and provides a platform for that discourse, there is no danger of garbling or distorting the government's message. First, the constituents' comments are identified by username, and so are clearly *not* government speech.[153] And second, the government official *invited the discourse* and, thus, invited the introduction of nuance and criticism.[154] The messages put forth by commenters on a public official's social media posts are not attributable to, nor viewed as endorsed by, the public official. Therefore, the government speech doctrine is inapposite here.

---

[141] *Id.* at 2246, 2248.
[142] *Id.* at 2248.
[143] *Id.*
[144] *Id.* at 2251.
[145] Matal v. Tam, 137 S. Ct. 1744 (2017).
[146] *Id.* at 1751.
[147] *Id.*
[148] *Id.* at 1753.
[149] *Id.* at 1759.
[150] *Id.*
[151] *See* Lidsky*, supra* note 120, at 1992 (stating that when the government shares its views, "it need not include opposing viewpoints").
[152] Davison v. Randall, 912 F.3d 666 (4th Cir. 2019).
[153] *Id.* at 686.
[154] *Id.*

In considering this issue, the U.S. District Court for the Second Circuit noted that had Trump been engaged in pure government speech, he could have blocked users without running afoul of the First Amendment.[155] His actions, however, went beyond pure government speech:

> It is clear that if President Trump were engaging in government speech when he blocked the Individual Plaintiffs, he would not have been violating the First Amendment. Everyone concedes that the President's initial tweets (meaning those he produces himself) are government speech. But this case does not turn on the President's initial tweets; it turns on his supervision of the interactive features of the Account.[156]

Twitter's interactive features mean that the speech is not solely Trump's government speech; it consists of a myriad of users' "retweets, replies, and likes" that a blocked user cannot access.[157] The Supreme Court recognized that the government speech doctrine was "susceptible to dangerous misuse."[158] Enabling government officials to bar users from this robust discourse would effectively turn the government speech doctrine into a sword. The government would be encouraged to use the government speech doctrine as a mechanism to "silence or muffle the expression of disfavored viewpoints," realizing the Supreme Court's concerns.

Packingham v. North Carolina (2017)

In 2017, after having established that social media accounts can function as "metaphysical" public fora,[159] the Supreme Court turned its attention to speech on social media platforms. *Packingham v. North Carolina*[160] is "one of the first" Supreme Court case that analyzes in depth the First Amendment implications of access to social media.[161]

Lester Packingham, a registered sex offender, was arrested for violating a North Carolina law that prohibited sex offenders from accessing commercial social networking sites where children are known to have profiles or webpages.[162] He argued that the North Carolina statute was unconstitutional, a proposition with which the Supreme Court (9-0) agreed.

The Supreme Court first confirmed that social media is a "metaphysical" public forum, saying, "While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace – the 'vast democratic forums of the Internet' in general."[163] Because it is a public forum, the government must demonstrate a legitimate basis for banning individuals from social media use. Recognizing the content-neutral nature of the prohibition, the Court applied intermediate scrutiny. It determined

---

[155] *Knight First Amendment Inst.*, 928 F.3d at 239.
[156] *Id*.
[157] *Id.*
[158] Matal, 137 S. Ct. at 1758.
[159] As Lidsky noted, the lack of physical space "should not preclude a finding of public forum status. Just as the government can rent a building to use as a forum for public debate and discussion, so, too, can it 'rent' a social media page for the promotion of public discussion." Lidsky, *supra* note 120, at 1996.
[160] Packingham v. North Carolina, 137 S. Ct. 1730 (2017).
[161] According to the Court, "This case is one of the first this Court has taken to address the relationship between the First Amendment and the modern Internet." *Id.* at 1736.
[162] *Id.* at 1734. Eight years after Packingham's original conviction for "an offense against a minor," he accessed Facebook and posted a comment (wholly unrelated to his original conviction) about his experience at traffic court. *Id.*
[163] *Id.* at 1735.

that the law was unconstitutional because it was not "narrowly tailored to serve a significant government interest."[164]

The *Packingham* opinion emphasized equally the right to speak and the right to listen. According to the Court, "A fundamental principle of the First Amendment is that all persons have access to places where they can speak and listen, and then, after reflection, speak and listen once more."[165] The Court was especially troubled by imposing a barrier to access when the internet and social media are involved, stating:

> North Carolina with one broad stroke bars access to what for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge. These websites can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard.[166]

The language in the Court's opinion reflects the rationale in the Court's numerous "right to know" opinions.[167] The Court concerns itself not just with Packingham's right to convey information, but from his right to *receive* it on the social media platform.

The opinion also discussed, at length, the democratic promise of social media, a concern central to the right to know cases addressed in this study.[168] Specifically, the Court recognized the unique potential of the internet for facilitating political participation:

> On Facebook, for example, users can debate religion and politics with their friends and neighbors. … And on Twitter, users can petition their elected representatives and otherwise engage with them in a direct manner. Indeed, Governors in all 50 States and almost every Member of Congress have set up accounts for this purpose. … In short, social media users employ these websites to engage in a wide array of protected First Amendment activity on topics 'as diverse as human thought.'[169]

This language, recognizing the rights of individuals to be fully informed and participate in the democratic process, arguably supports compelled access to government officials' social media accounts. However, this specific issue has not yet been adjudicated by the Supreme Court. In *Packingham*, the Court even decried the severely limited jurisprudence on First Amendment rights and the internet, particularly social media.[170] The analogous situations addressed thus far support finding that the Court would view limiting access to these sites as an impermissible restriction on the First Amendment.

---

[164] *Id.* at 1736.
[165] *Id.* at 1737.
[166] *Id.*
[167] *See* discussion *supra* section "The Supreme Court and the right to know," p. 33.
[168] *See* discussion *supra* section "The right to know furthers the goals of participatory democracy," p. 35.
[169] Packingham v. North Carolina, 137 S. Ct. 1730, 1735-1736 (2017) (capitalization in original; internal citations omitted).
[170] The Court recognized that this is one of the first cases involving the First Amendment protection of access to social media. It said, "As a result, the Court must exercise extreme caution before suggesting that the First Amendment provides scant protection for access to vast networks in that medium." *Id.* at 1736.

The status of public vs. private social media accounts

The parameters of *Packingham v. North Carolina* guide whether an account qualifies as a public forum. However, while the *Packingham* majority concluded that social media is a public forum, three justices in concurrence said the majority's position reflected "undisciplined dicta."[171]

This question – whether social media accounts are, in fact, public fora – has been taken up in a few cases, and discussed by very few scholars and practitioners. Unsurprisingly, given that this question is relatively novel, the conversation is sparse. There is a general acknowledgement that the public forum analysis should be "functional."[172] Overall, there seems to be a consensus about *what* factors courts should consider, although there is disagreement regarding whether the factors are determinative or even what result should entail. This section of the study addresses the factors that courts should consider when assessing whether an account is a public forum.

Courts should consider whether the government official's account is 'personal' or 'official'

By safeguarding Packingham's access to social media, and by extension recognizing the high-value discourse facilitated by preserving social media discourse, the Court broadly proclaimed that social media accounts are public fora. This distinction becomes muddied when considering the fact that the internet, like the physical world, consists of both public and private spaces.

Scholar Rodney Smolla cautioned against reading the language of *Packingham* too broadly and deeming the internet a "modern digital 'public square'" without caveat.[173] Although some spaces are public spaces that naturally warrant robust First Amendment protection, other spaces are private. Smolla suggested that *Packingham* failed to distinguish between the two spaces and incorrectly determined that social media accounts inherently constitute public fora.

According to Smolla, some spaces on the internet, such as official government websites soliciting constituents' feedback, could be designated public fora.[174] These spaces are designed specifically to encourage the exchange of information between public officials and constituents. Similarly, an official's social media account on Facebook or Twitter could "very well become designated public for[a] if there are places on the sites for comments posted by citizens."[175]

In one of the few Court of Appeals decisions evaluating these issues, *Davison v. Randall*, the Fourth Circuit resolved the dispute by considering the government official's actions with respect to her social media account.[176] In that case, Brian Davison brought a 42 U.S.C. §1983 claim against Phyllis Randall, the chair of the Loudon County, Virginia, Board of Supervisors. Randall had blocked Davison from her "Chair Phyllis Randall" Facebook page after he criticized

---

[171] *Id.* at 1738 (Alito, J., concurring).

[172] *See* Lidsky, *supra* note 120 at 2024 (noting that "[t]he public forum inquiry should … be a functional one based on the way citizens actually use the site."

[173] Rodney A. Smolla, *The First Amendment and Public Officials' Social-Media Accounts*, 36-SPG DEL. LAW. 22 (Spring 2018).

[174] *Id.* at 23. Most, if not all, scholars would concur with this position. *See, e.g.,* Brian P. Kane, *Social Media Is the New Town Square: The Difficulty in Blocking Access to Public Official Accounts*, 60-OCT ADVOCATE (Idaho) 31 (October 2017).

[175] Smolla, *supra* note 173, at 23. Smolla also noted that these sites could be "at times classified as organs for the government's own expression, and treated as government speech."

[176] Davison v. Randall, 912 F.3d 666 (4th Cir 2019).

her official actions regarding the school budget and farm inspections.[177] The court found that this ban was improper because not only did Randall use the page to communicate with the public, she had designated the page as belonging to a "government official."[178] Her account became a public forum:

> A private citizen could not have created and used the Chair's Facebook Page in such a manner… Put simply, Randall clothed the Chair's Facebook Page in the 'power and prestige of h[er] state office,' … and created and administered the page to 'perform actual or apparent dut[ies] of h[er] office.'[179]

The analysis becomes cloudier when considering private social media accounts. The designation that an account is "official" signifies that it, much like a dedicated website, is intended to support the back-and-forth exchange of information between the public official and her constituents. The question becomes whether a public official's *private* social media account can ever qualify as a public forum.

Smolla suggests the adoption of a "bright-line rule" stating two things. First, government-held social media platforms and official accounts could be deemed public fora.[180] And second, private social media accounts held by public officials cannot, by definition, qualify as public fora.[181] Public fora are created through specific, intentional governmental action. Private social media accounts, on the other hand, are the property of private social media platforms – not the government. They also reflect the "private choices of political officeholders," and they are governed by different First Amendment principles.[182]

Smolla expressed concern that treating officials' social media accounts as public fora would have deleterious effects. While public fora are neutral by design, officials' private accounts are inherently partisan. Smolla said:

> If a public officeholder is forced to treat his or her social-media page as a public forum, the page will lose its character as the officeholder's own unique, individual, candid and authentic expression, and instead become a bowdlerized platform collecting the random messages of any and all, stripped of any distinctive personality or direction.[183]

Smolla's argument is troubling for two reasons.

First, it is unclear how prohibiting government officials from banning constituents would necessarily result in depriving an account of its "distinctive personality or direction." To illustrate, President Trump's Twitter account – which Smolla concedes "may be the single most notorious use of social media by a public officeholder in American society today"[184] – teems with personality. The tenor of Trump's tweets does not appear to be mediated by the composition of his audience. Even though courts have held that his account is a "public forum" and that he must refrain from banning individual access, the fundamental nature of his tweets remains unchanged. Even a cursory glance at President Trump's Twitter account at any time of the day supports this

[177] *Id.* at 675.
[178] *Id.* at 674.
[179] *Id.* at 681 (internal citations omitted).
[180] Smolla, *supra* note 173, at 23.
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] *Id.*

claim. He still targeted former Senator John McCain seven months after his passing.[185] He still attacks the "Radical Left Democrats" and "Fake News Media."[186] And he still suggests that *Saturday Night Live* is colluding with Democrats to present one-sided coverage of his presidency.[187] What's perhaps more astonishing is that these three tweets reflect a mere one-hour-and-five-minute snapshot of Trump's Twitter account, during which he made numerous other tweets. Smolla's concerns are speculative.

Second, Smolla's asserted concerns are relatively inconsequential when weighed against protecting the constituents' interests in participatory government. He suggests that constituents have "almost infinite channels and platforms" to voice their opinions, but adopting his "bright-line test" would encourage government officials to communicate with constituents via private social media accounts in lieu of government-owned or designated "official" accounts.

Perversely, the more an official seeks to shape the narrative, the more inclined that official would be to use private social media accounts to share critical information. On private platforms, the officials could ban constituents with relative impunity, silencing their contributions to critical political discourse and controlling the story. The result would be severely skewed dialogue and an uninformed populace, the opposite of the "marketplace of ideas" Smolla seeks to perpetuate. Pew Research Internet data even noted a 15% increase (to 75%) in users obtaining their news from Twitter, which may be related to President Trump's use of Twitter to convey information.[188]

Users may have "almost infinite channels and platforms" to air their opinions, as Smolla noted, but this is immaterial. A user who has been blocked by an account on Twitter may have other avenues via which he can receive and comment on the account's tweets, "such as creating new accounts, logging out to view the President's tweets, and using Twitter's search functions to find tweets about the President posted by other users with which they can engage."[189] However, these "workarounds" do not cure the constitutional deficiencies inherent in viewpoint-discrimination-motivated blocking. According to the Supreme Court, "The distinction between laws burdening and laws banning speech is but a matter of degree. The Government's content-based burdens must satisfy the same rigorous scrutiny as its content-based bans."[190] Having other avenues to engage in discourse "does not cure that constitutional shortcoming."[191]

Impeding users' speech conflicts with the tenets of the First Amendment. As the U.S. Court of Appeals for the Second Circuit noted when it held that the @realDonaldTrump account is a designated public forum, "[T]he best response to disfavored speech on matters of public concern is more speech, not less."[192]

---

[185] Donald Trump (@realDonaldTrump), TWITTER (Mar. 17, 2019, 8:41 a.m.). https://twitter.com/realDonaldTrump/status/1107260609974943745 (claiming that John McCain transmitted a dossier to the FBI intending to derail the presidential election). *See* Michael Tackett, *Trump Renews Attacks on John McCain, Months After Senator's Death*, N.Y. Times, Mar. 17, 2019, https://www.nytimes.com/2019/03/17/us/politics/trump-mccain-twitter.html.

[186] Donald Trump (@realDonaldTrump), TWITTER (Mar. 17, 2019, 9:18 AM), https://twitter.com/realDonaldTrump/status/1107269978678611969 (capitalization in original) (asserting that the media targeted Judge Jeanine Pirro, which ultimately led to her suspension from Fox News).

[187] Donald Trump (@realDonaldTrump), TWITTER (Mar. 17, 2019, 8:13 AM), https://twitter.com/realDonaldTrump/status/1107253742271901696.

[188] *See* LoPiano, *supra* note 15, at 547 (discussing Pew Research data in 2017, and stating that "the President's Twitter account, if not a growing news source itself, may actually be responsible for Twitter's increased audience for news").

[189] Knight First Amendment Inst. v. Trump, 928 F. 3d 226, 238 (2d Cir. 2019).

[190] United States v. Playboy Entm't Grp., Inc., 529 U.S. 803, 812 (2000).

[191] *Knight First Amendment Inst.*, 928 F.3d at 239.

[192] *Id.* at 240.

In its determination, the court noted that while Trump's account was private before he assumed the presidency, and will be private again after leaving the presidency, the pertinent consideration is "what the Account is *now*."[193] Trump's account contained numerous indicators that qualify it as a designated public forum:

- Trump uses the account "as a channel for communication and interacting with the public about his administration"[194]
- The "public presentation of the Account and the webpage associated with it bear all the trappings of an official, state-run account," including its registration to "Donald J. Trump '45th President of the United States of America, Washington, D.C.'" and header photographs depicting engagement in official government business, suggest that this account is intended for government business[195]
- Both the President and administration members have described his account use as "official"[196]
- The @realDonaldTrump account is "one of the White House's main vehicles for conducting official business"[197]
- Presidential tweets are presumably official records, according to the National Archives and the Presidential Records Act of 1978.[198]

As noted by the court, the @realDonaldTrump account "was intentionally opened for public discussion" and used "as an official vehicle for governance," and "its interactive features [were] accessible to the public without limitation."[199] Therefore, it is a public forum.

Courts should analyze the content posted by the account

Individual access to public officials' social media accounts arguably turns on the purpose of their use. Some scholars suggest that, in line with *Packingham*, social media is a public forum. Government officials' social media accounts should be deemed public fora when they are used to convey government information to – and receive it from – constituents. Others suggest that this position is unsound because it relies too heavily on *Packingham's dicta*.

Brian Kane, the Deputy Attorney General for the State of Idaho, suggested that an account's public forum status should turn on the extent to which it facilitates the exchange of information between public officials and constituents.[200] Thus, President Trump's private @realDonaldTrump Twitter account is a designated public forum because he uses this account to engage in dialogue about important government information with his constituents. An individual blocked from accessing that social media account would be able to bring a 42 U.S.C. §1983

[193] *Id.* at 6.
[194] *Id.* at 7.
[195] *Id.* at 7, 17.
[196] *Id.*
[197] *Id.* at 8.
[198] *Id.* at 9.
[199] *Id.* at 23.
[200] Kane, *supra* note 174, at 32 (noting that an account that "both distributes information to constituents and receives information from constituents" would likely be deemed a public forum). Kane proposed six factors to consider here, including the reason for the account's creation, the owner's identity, whether public resources are used to maintain the account, the purpose of the account, whether the account is "swathed in the trappings of office," and what content is posted. *Id.*

claim.[201] The aggrieved individual would be required to demonstrate that the ban (1) was imposed under "color of law," and (2) deprived the constituent of his constitutional rights.[202] If the individual can make this showing, then the ban would be held unconstitutional.

Rodney Smolla, on the other hand, disputes the propriety of analyzing public officials' purpose in this way. He asserts that this is "not a sound way to frame or analyze the issue."[203] According to Smolla, "The question of whether an official is acting under 'color of law' or engaged in 'state action' should not be conflated with the separate First Amendment question of how and when a public forum comes into existence."[204]

The few courts analyzing this question have repudiated Smolla's position. In *Davison v. Randall*, the Fourth Circuit evaluated a 42 U.S.C. §1983 claim brought by a constituent who was banned by an elected public official, Phyllis Randall, from her "Chair Phyllis Randall" Facebook page.[205] The court reviewed *de novo* the question of whether Randall used her page in such a way that it became a public forum.[206] This determination hinged on Randall's activities with respect to the Facebook page. The court said that in creating and administering the Facebook account, and banning a constituent, Randall acted under color of state law.[207]

Randall used her page as a "tool of governance," not only by designating the page as belonging to a "government official,"[208] but sharing information with the public, and inviting constituent feedback.[209] These latter two concerns, specifically the encouragement of public comment, were deemed determinative.[210] The court also explicitly rejected Randall's argument that Facebook is private and thus cannot be a public forum.[211] The court raised several examples in which forum analysis had previously extended to private property that was designated for public use or which was controlled by the government.[212]

The *Davison* opinion recognizes that a government official cannot disavow the official capacity of her actions by conveying information via a private social media account. The opinion also refuses to enable government officials to use these accounts to obfuscate criticism of their official actions.

A similar rationale was employed by the U.S. Court of Appeals for the Second Circuit in determining that @realDonaldTrump is a designated public forum.[213] The court considered the numerous capacities in which the account was used to convey information and solicit feedback about various government policies.[214] Trump himself stipulated that he used the account…

---

[201] *Id.*
[202] *Id.*
[203] Smolla, *supra* note 173, at 24.
[204] *Id.*
[205] Davison v. Randall, 912 F.3d 666 (4th Cir. 2019) Although the court ultimately discussed *Packingham*, it correctly noted that no courts had previously considered the specific issue of whether a governmental social media page constituted a public forum. *Id.* at 682.
[206] *Id.* at 681.
[207] *Id.* at 680-81.
[208] *See* discussion *supra* section "Courts should consider whether the government official's account is 'personal' or 'official,'" p. 51. (addressing the impact of Randall designating this account as an "official" account).
[209] *Davison*, 912 F.3d at 674.
[210] Id.
[211] *Id.* at 682-83.
[212] *Id.* at 683.
[213] *Knight First Amendment Inst*., 928 F.3d at 238.
[214] *Id.* at 231-32.

> … [T]o announce, describe and defend his policies; to promote his Administration's legislative agenda; to announce official decisions; to engage with foreign political leaders; to publicize state visits; [and] to challenge media organizations whose coverage of his Administration he believes to be unfair.[215]

The court considered the various official activities Trump used the account to communicate about, including: nominating Christopher Wray as FBI director, announcing the administration's ban on transgender individuals serving in the military, announcing that he fired Chief of Staff Reince Preibus and replaced him with General John Kelly, and updating the public on his discussions with South Korean President Moon Jae-in about North Korea's nuclear capabilities.[216] These uses of the account – "as an important tool of governance and executive outreach"[217] – militates against treating it as a private account.

Furthermore, the account also invites users to "Follow for the latest from @POTUS @realDonaldTrump and his Administration."[218] By its nature, "public interaction [is] a prominent feature of the account."[219]

It should be noted that the court explained that, ordinarily, there may be a fact-specific inquiry when the ways a public official actually uses his account diverge from the ways he characterizes the account.[220] These issues were not present in Trump's case. However, the court suggested that such a determination would depend on the following factors: how the official describes and uses the account; to whom the features of the account are made available; and how others, including government officials and agencies, regard and treat the account.[221]

The general trend suggests that public officials' social media accounts are public fora. By extension, government officials, therefore, cannot engage in viewpoint discrimination to ban or block users. However, the case law and jurisprudence regarding this specific question are sparse. The concerns of scholars such as Rodney Smolla may persuade a court to carve out and define "private" social media spaces based on the characteristics of social media use. Furthermore, the assertion that private social media accounts are not government property, but the property of private social media platforms, should be given special consideration.

Conclusion

The Supreme Court has established that the Constitution includes a penumbral "right to know," which recognizes an individual's interest in securing information about government operations. The relevant case law centered around two themes. The first theme is access to publicly available information. The Court protects an individual's right to access this information, especially where access furthers the goals of a participatory democracy. The Court also has stated that absent a compelling reason, the government is prohibited from contracting available information or propounding any undue burden in obtaining that information. The second theme is

[215] *Id.* at 231.
[216] *Id.*
[217] *Id.* at 236.
[218] *Id.* at 235.
[219] *Id.* at 236.
[220] *Id.*
[221] *Id.*

access to compelled information. The Court has typically declined to force the government to reveal information that is not already known to the public.

Various mechanisms have been put in place to protect and further the right of individuals to access publicly available information. The most obvious of these is the statutory protections afforded by FOIA. Although FOIA includes many important protections for safeguarding access, it comes with some problems that render it ineffective in safeguarding an individual's right of access here. First, statutes involving access yield inconsistent results, especially in the face of government inertia. And second, the statutes' reach is limited, leaving individuals unable to use the statutory mechanisms to secure certain important documents.

This background information raises the question of how courts would evaluate the public's right to access the social media accounts of public officials, particularly their *private* social media accounts. To address this question, the study first discussed forum analysis, determining that certain of the officials' social media accounts would likely be deemed a metaphysical public forum. This determination would limit public officials' ability to curb speech on their accounts.

The study next turned to, and rejected, the government speech doctrine as applied to social media accounts. The doctrine enables government officials to silence certain discourse if it would impede or distort the government speaker's messaging. Had it applied, it could empower officials to silence speech on their social media accounts. However, the rationale behind the government speech doctrine simply does not extend to public officials' social media accounts.

Then, the study considered the most directly relevant Supreme Court case, *Packingham v. North Carolina*, which established the principle that social media accounts are public fora.[222] The Court's position was clear; however, there are reasonable arguments for determining that *Packingham's* reading may be overbroad. Instead, social media consists of various private and public spaces. Public officials' social media accounts may fall in one or the other of these categories, depending on context. It also considered *Knight First Amendment Institute at Columbia University v. Trump*,[223] a U.S. Court of Appeals for the Second Circuit decision that determined that Trump's @realDonaldTrump account, though technically "private," functioned as a public forum; thus, Trump cannot engage in viewpoint discrimination to ban users from interacting with the account.[224]

And finally, the study addressed the account characteristics a court may consider when determining whether individuals can claim a right to access a public official's social media account. The court may consider whether the account is designated as "official" or "private." The former accounts are more likely to be deemed public because their designation suggests that the information includes official government business intended for the public to view and respond to. Scholars differ, however, regarding whether individuals can assert a legitimate right to access the private social media accounts of public officials. On one hand, the "private" designation suggests that the account is not intended for public consumption. This, plus the fact that the accounts are owned by private companies, not the government, weighs against access. On the other hand, the "private" designation shouldn't be used to shield accounts from the public eye, especially if critical government business is being conducted through the private account. This indicates that the court should consider the *content* posted to the social media account. If the account is used to share

[222] 137 S. Ct. 1730 (2017).
[223] 928 F.3d 226 (2d Cir. 2019).
[224] *Id.* at 234.

important government information, and solicit feedback from constituents, then there would be a strong argument for access.

More robust protections for access must be secured. The *Packingham* court did much of the heavy lifting when it comes to paving the way for individual access to public officials' social media accounts. And certainly, the (few) courts that have considered access to these social media accounts have held in line with *Packingham*, supporting broad access. But even with *Packingham's* broad, protective language, there is still room to suggest that public officials are empowered to wield excessive control on social media accounts designated as "private." This result would be a perverse misreading of the law, creating a technicality that furthered the goals of disinformation, misinformation, and censorship. Thus, there should be clear guidelines regarding when social media accounts are public fora. These guidelines would instruct courts not only to consider the account designation, but to engage in a substantive analysis of the nature of the account. If a "private" account is being used to engage in back-and-forth discourse with constituents about official government matters, then it would almost certainly be a public forum, designation notwithstanding.

These rules would ensure two things. It would help protect an individual's right to access important government information and further the principles of participatory democracy. And it and it would help ensure that "private" social media spaces are actually *private* and not being used to conduct government business outside the public's eye.

the journal of CIVIC INFO

The Journal of Civic Information

Volume 1 | Number 1 September 2019

Journal homepage: https://journals.flvc.org/civic/ ISSN (online): 2641-970X

Agency Perspectives on Online Public Records Request Portals

Alexa Capeloto *

Article Information

Received: Jan. 16, 2019

Accepted: Feb. 13, 2019

Published: Sept. 4, 2019

Keywords

Freedom of information
Public records
Government transparency
Online portals

Abstract

Spurred by converging trends facilitated by the interactive web, government agencies are moving to digitize and make more transparent the public record request (PRR) process via dual-facing online portals. Such portals, often provided by third-party vendors as SaaS (Software as a Service) solutions, are built on the premise and promise of helping agencies streamline their internal workflows while aiding requesters through the sometimes labyrinthine process of accessing public records. This research aims to study the effects and efficacy of such portals from the agency perspective, both at the process level and in a broader sense of reshaping the relationship between citizen and government. Set within a contextual framework of the trends from which these portals have emerged, a survey of 54 U.S. public jurisdictions suggests that online portals are significantly improving agencies' internal and external processes of receiving, tracking, and responding to requests for public records, but do not necessarily bring correlative improvement in their overall relationship with citizens for a number of possible reasons.

* Alexa Capeloto, John Jay College of Criminal Justice, City University of New York. Please send correspondence about this article to Alexa Capeloto at acapeloto@jjay.cuny.edu. An earlier version of this work earned top-three paper at the National Freedom of Information Coalition summit FOI Research Competition, April 12, 2019, in Dallas, Texas.

To cite this article in Bluebook: Alexa Capeloto, *Agency Perspectives on Online Public Records Request Portals, 1*(1) J. CIVIC INFO 59 (2019).
To cite this article in APA: Capeloto, A. (2019). Agency Perspectives on Online Public Records Request Portals. *Journal of Civic Information, 1*(1), 59-74.

DOI: https://doi.org/10.32473/joci.v1i1.115659

Introduction

Each year, *Government Technology* magazine publishes its GovTech 100, a list of the top 100 technology companies "focused on, making a difference in, and selling to state and local government agencies across the United States." And each year since the list launched in 2016, the companies GovQA and NextRequest have been included. Chicago-based GovQA was founded in 2002 and offers a variety of software services to public agencies, including subpoena management, inter-agency communications, and a portal for processing public records requests (PRRs). The company has more than 1,000 government clients, and the majority of them utilize the PRR portal, including Dallas, Seattle, and Salt Lake City. NextRequest was founded in 2015 and is focused exclusively on providing agencies with PRR portals. As the San Francisco-based company states on its website: "Public Records Is All We Do." Although newer to the field, NextRequest has quickly amassed a sizeable client list, from small towns, such as Sunny Isles Beach, Florida, and Bourne, Massachusetts, to large cities, including San Francisco, San Diego, and Miami.

Although several other companies exist, GovQA and NextRequest are two of the most common providers of government PRR portals, offering web-based platforms for centralized, automated tracking and processing of information requests submitted by the public under their respective states' freedom of information laws. These services have emerged at the nexus of several digital-age trends, including GovTech, civic tech, operational transparency, and online requester-side PRR aids like MuckRock and iFOIA, yet little has been done to research their impact in the all-important space where transparency is enforced as a means of preserving open, fair government.

To that end, this article examines the effects and efficacy of online freedom of information portals employed by government agencies – with a particular focus on NextRequest as it rapidly builds a client list with the stated goal of restoring trust between citizen and government – and analyzes how such services are in fact reshaping the PRR process for those who manage it day to day.

Background

Help for requesters

Transparency is one of the ideological roots of democracy in the United States, enshrined in federal and state freedom of information laws governing one's right of access to public records. Yet obtaining records at the federal, state, and local levels can be a notoriously difficult process, and the frustration continues. A March 2017 study commissioned by the John S. and James L. Knight Foundation surveyed 228 people, including journalists and members of FOI advocacy organizations, about their experiences with records request processes. About half reported that access to state and local records had gotten worse during the previous four years, and nearly 40 percent reported that denial of records had become more frequent at all levels of government, particularly at the local level (Cuillier, 2017). David Greene, senior staff attorney for the Electronic Frontier Foundation, said "it just takes too long" for agencies to respond to requests (p. 7). The same respondents reported dissatisfaction with technology around the PRR process. A third of responders ranked government technology as very or extremely problematic, and 80 percent said it is at least somewhat of a problem (p. 9).

Identifying a need, several nongovernmental efforts to assist records requesters via technological tools have proven effective. Asked for the Knight Foundation report to identify the most useful FOI digital tool, 27 respondents named MuckRock, by far the most popular answer (Cuillier, 2017, p. 41). MuckRock is a nonprofit news site that aids requesters through the process of filing for information from government agencies, while also providing a repository of responsive documents and conducting original reporting and analysis around those documents. The stated goal is to "mak(e) politics more transparent and democracies more informed" ("About MuckRock," para. 1). As of September 2019, the nonprofit had logged more than 68,000 requests filed with 13,714 agencies, resulting in more than 20,000 fulfilled requests yielding 4.3 million released pages. As *Boston* magazine put it, "the company is doing for public records what TurboTax did for taxes or Change.org did for petitions: making it easier to be an engaged citizen" (Eil, 2016, para. 29).

In 2016, MuckRock took over the records request tool FOIA Machine, which had been seeded by the Knight Foundation and a Kickstarter campaign. While MuckRock offers "full service" assistance for a cost, such as directly filing requests with agencies, conducting follow-ups and digitizing responsive records, FOIA Machine continues to offer free assistance with generating and tracking one's requests (Wang, 2016). Both are built on open-source software, as is Alavateli, a UK-based online tool that helps with making and tracking requests. Other requester-assistance services include iFOIA.org, from the Reporters Committee for Freedom of the Press, and a request-letter generator provided by the Student Press Law Center.

As these services facilitate PRRs filed with public agencies, the agencies must find a way to keep up on their end. This link is mentioned in the Knight Foundation report, attributed to a co-founder of NextRequest:

> As more online tools, such as MuckRock, make it easier for people to request records, it seems likely agencies (especially those that have not digitized operations) will have even greater difficulty responding, said Tamara Manik-Perlman, chief executive officer of NextRequest. "People impute ill will on the state-local level, but most of the time people are just overburdened and just don't have time to do what they need to do," she said. (Cuillier, 2017, p. 25)

Governments get involved

Fulfilling requests on the agency side can be just as frustrating as asking for them on the constituent side. Records managers for this research reported a range of cumbersome processes for handling requests prior to adopting PRR portals. Most involved a mix of paper forms, spreadsheets, and email communication. As one survey respondent described it: "Excel spreadsheets, lots of calendars, a lot more confusion, and missed deadlines." Silo-ization, in which PRR management was left to individual departments, added to the confusion, as another respondent stated:

> Disjointed, to say the least. Anyone within a department would receive a records request and would sometimes coordinate within their own department, and even less frequently they would coordinate with other departments to retrieve responsive records. When there was a request that spanned multiple departments, not only would multiple departments disclose documents, but the requester would receive multiple responses, often times producing duplicate records and conflicting responses as far as exemptions.

Faced with frustration from requesters and hoping to ameliorate a persistent pain point, some agencies adopted a system similar in structure to MuckRock and FOIA Machine but created for the government side of the PRR transaction.

In 2013, fellows with the Code for America program teamed with the city of Oakland to develop RecordTrac, an open-source software tool to help the city manage the voluminous requests filed under the California Public Records Act in the wake of the 2011 Occupy protests. Together they built a dual-facing system that on one side allowed city staffers to receive and track PRRs across departments, and on the other side provided a simple interface for users to make and track their own requests. Users were told who at the city was handling their request and how to contact them. Responsive documents were not only shared with requesters, but published in a searchable repository in a "release to one, release to all" approach. Oakland officials estimated that the number of records requests more than doubled during RecordTrac's first year of operation (Capeloto, 2014). The system was named 2013 Civic App of the Year by GovFresh (Fretwell, 2013), and dubbed America's best FOI website by the New York open-government nonprofit Reinvent Albany ("America's Best," 2014).

Like MuckRock and FOIA Machine, RecordTrac was built on open-source software. The developers put the source code on GitHub for other agencies to adapt and adopt. A web developer with the city of Yakima, Washington, replicated the portal with essentially the same features and functions (Capeloto, 2014). New York City developers rewrote the code to suit their agencies' scale and needs, and launched their own beta version, called OpenRECORDS, in 2015. A newer version, released in 2017, is used by 38 city agencies and counting ("About OpenRECORDS").

The PRR process had been moving online long before this. In a 2011 Electronic Government survey conducted of municipal agencies by the International City/County Management Association, 50 percent of respondents said they allowed for online records requests (Norris & Reddick, 2011, p. 3). In 2017, 44.8% said they provide an "off the shelf" technology solution for public records requests (International City/County Management Association, 2017, p. 5). In addition to GovQA, which began selling its various software suites exclusively to government clients about 10 years ago, several other systems were listed by agencies surveyed for this research, some of them dedicated PRR tools and others used in adapted form for records management.

RecordTrac earned attention as a Code for America project. In general, government technology, or GovTech, is primarily "designed with government as the intended customer or user," while civic technology, or civic tech, is "technology used to inform, engage and connect residents with government and one another to advance civic outcomes" (Knight Foundation and Rita Allen Foundation, 2017, p. 7). GovTech is defined by the intended user (government) and focused on increasing internal operational efficiency, while civic tech usually includes a citizen-facing component (Knight Foundation and Rita Allen Foundation, 2017, p. 7) and understands both government and public to be core partners (Shaw, 2016, para. 12). For a long time, civic tech primarily referred to nongovernmental initiatives, but Code for America allowed for civic citizen-focused technology to be "developed and implemented by and with public bodies themselves in an attempt to reach out to citizens and increase engagement and participation" (Rumbul & Shaw, 2017, p. 1). With RecordTrac, technologists and policymakers worked together to simplify and optimize the PRR process, and developers paid particular attention to user experience just as a service like MuckRock would. The "release to one, release to all" concept, for example, was explained by a RecordTrac developer this way: "Prior to [the project], I didn't know what FOIA

was, so I didn't come in with preconceptions about it. ... I wanted to do the most simple design possible, so that's why everything is public" (Rumbul & Shaw, 2016, p. 22).

Parker Higgins, director of special projects for the Freedom of the Press Foundation, explored RecordTrac in 2015 and described the "very cool" experience of combing through readily available datasets. "If all this seems familiar," he wrote, "it may be because services like Muckrock, where I'm a frequent user, have implemented the same kind of thing on the requester end" (para. 5). He added, "Muckrock definitely makes the public records experience better, and has built an impressive collection of returned documents. But there's an emergent property of the agencies themselves putting all that information online in the first place" (para. 6).

The emergence of NextRequest

Open-source software is free, transparent, and adaptable, but it can languish without proper funding, staffing, or maintenance structures. One Oakland program manager told a researcher that the city's contracting policies are structured around multimillion-dollar deals, not the smaller ongoing maintenance RecordTrac required (Rumbul & Shaw, 2016, pp. 32-33). As an internal city memo noted:

> The City has no in-house capability to maintain the current RecordTrac system. Since our current RecordTrac software is also not supported, it is impossible to make much needed software updates. The lack of support could result in a system-wide failure of the entire public records system. Ultimately, we decided that while we love RecordTrac, we love transparency more. (City of Oakland, n.d.).

Richa Agarwal, Cris Cristina and Sheila Dugan were the Code for America fellows who developed RecordTrac with Oakland in 2013. Also part of the 2013 Code for America cohort, but not part of RecordTrac's creation, were Manik-Perlman, Andy Hull, and Reed Duecy-Gibbs. In late 2014, the latter three announced plans to launch NextRequest, a hosted version of RecordTrac with reworked code (Kanowitz, 2015): "What we've done with NextRequest is build upon the immense amount of work and learning that went into RecordTrac, updating the architecture in order to make the system accessible to governments of all sizes" (Hull, Manik-Perlman & Duecy-Gibbs, 2014). Essentially, the open-source system became a civic tech startup, with investors ("NextRequest," n.d.) and a break-even projection of June 2016 (Matter Ventures, 2015).

Oakland signed on in 2017, stating that "as a company that grew out of the Code for America fellowship, NextRequest is uniquely aligned with our philosophy, values and workflow around transparency and records management" (City of Oakland, n.d.).

The cloud-hosted multi-tenant application relieves agencies of management demands because the company handles all costs of hosting, support, maintenance, and software upgrades (Phillips, 2016). The company provides a free version for small entities that receive 120 or fewer requests per year, and "Enterprise" packages of varying costs to other agencies. When NextRequest launched, the typical range was $2,000 to $50,000 per year depending on agency size (Matter Ventures). The Rhode Island Office of the General Treasurer was quoted $3,000 per year and signed on. San Diego is paying $28,000 for the current fiscal year. The State of Iowa pays about $77,500 per year.

On the agency side, the system offers a centralized cross-departmental dashboard where employees can log and track requests, including assigning them to particular staffers, flagging them for legal review, communicating internally and externally about the request, logging time

spent, filing an invoice for costs, and uploading documents of unlimited file size. Staffers are notified when they are assigned to handle a request and are reminded about the request as the due date approaches. Each request has an audit trail showing how it was handled, and staffers can run reports using various filters (for example, one could automatically generate a biweekly report of all overdue requests). Integrated redaction and payment tools are available for additional fees.

On the public side, users log into the system and file their request through a dashboard. They're given the name and contact information of the staffer(s) handling their request, communications and status updates about the request, and responsive documents. The system tries to avert requests for information already posted online. When a keyword like "budget" is typed into a request field, a yellow banner appears providing a link to existing budget information. Or if a record is requested that is housed with another agency, the system might flash a message to the user directing them to that agency.

As RecordTrac did, the system can provide a public, searchable repository of responsive documents from previous requests; this, in fact, was an initial selling point for the NextRequest system under a "release to one, release to all" ethos – a living archive that provides information before it even needs to be requested. It also coincides with the open-data trend in which agencies across the country are proactively publishing information that can be freely accessed, used, and redistributed in digital form (Noveck, 2016). As of 2017, 105 cities had adopted formal open-data policies that systematize proactive record release, 28 of which adopted policies in that year alone (Stern, 2018, p. 5). As NextRequest's Chief Operating Officer Duecy-Gibbs said, "The old way of doing things isn't viable anymore. We want to help local governments publish info out proactively, and give a way to help people access without having to ask" (Opsahl, 2016, para. 8).

NextRequest has become popular enough that MuckRock noted in March 2018 that part of its recent work included continuing to "tweak and improve MuckRock integration with agencies that use NextRequest portals" (Morisy & Kotler, 2018, para. 4). In 2016, the Sunlight Foundation nodded to RecordTrac and NextRequest in listing recommendations for improving the federal Freedom of Information Act, suggesting that the U.S. government build FOIA software "*with* the people who make requests and process them. Oakland's RecordTrac is a useful model for improving the FOIA process. The national success of PostCode's NextRequest, which built upon that code, is worth studying and scaling" (Howard, 2016, para. 13).

That same year, the Center for Digital Government cited NextRequest as a factor in awarding third place to Sacramento County among its 2016 Digital Counties Survey winners. "A commitment to transparent operations can be seen in several new projects that have come to light in Sacramento County in the past year," including the request portal (Wood et al., 2016, para. 6).

The case for trust

As the 2017 Knight report suggests, people want better digital tools from their governing institutions. In a 2014 survey of 1,095 voting-age Americans, 62 percent said they would have more confidence and trust in government if offered improved digital services. Seventy-two percent said they would be more willing to engage with government, and an equal number said they would feel more overall satisfaction with government (Accenture, 2014, p. 15).

NextRequest's creators promote the portal as a mutually beneficial means of improving the relationship between individual and institution. In early 2016, Manik-Perlman appeared on a podcast called GovLove, produced by Engaging Local Government Leaders (ELGL). She described in detail the various benefits of the portal, including the ability to avert requests for

already published information, the streamlined, customizable workflow management, safeguards against inadvertent publication in the form of a pop-up verification window, and above all, the transparency of allowing the public to see the work staffers are doing via tracking software. Seeing that work helps restore trust between the public and government, she said. "That's what's most important to us, is this sort of increase between empathy and trust, because government is us" (Wyatt, 2016). Later that year, on a different podcast, she reiterated that point: "Ultimately I think that the work we're doing is really about rebuilding trust between the public and government" (Phillips, 2016). One year prior, she told Politico she was already seeing a shift in the dynamic between citizen and institution as a result of her company's system:

> People are entitled to request certain information from the government, and the government just hasn't had the tools they need to make it a simple process. The thing that's been especially interesting is seeing the tone of the discourse and the tone of the relationship between the public and the government change. ("The 60-second interview," 2015)

In an interview with *The Daily Northwestern* in 2016, COO Duecy-Gibbs said the company hoped to "change the tone of the relationship between the government and the public around access to information. It's very adversarial and it doesn't need to be. Technology is one way to make this a win-win for both employees and citizens" (Opsahl, 2016, para. 10).

This type of messaging speaks to the concept of operational transparency, in which oft-hidden processes are made more visible to citizens as a means of increasing engagement and improving public perception. Research by Buell, Porter, and Norton (2018) for a Harvard Business School working paper suggests that the more an agency "shows its work" by providing a public view of its operations, the more people will trust and engage with that agency. In partnership with the city of Boston, they utilized a system not unlike NextRequest to test the correlation between transparency and trust. Selected Boston residents in a "blind" condition (Group 1) were shown a tally of resident-submitted service requests for issues such as illegal graffiti, potholes, and litter. Other residents in a "functional transparency" condition were shown a photo, address, and description of the issue, along with a timestamp indicating when it was submitted and the status of service. Results showed that Group 2, the "participants observing transparency into the work that government was doing, perceived the government more favorably than participants who did not observe the work" (p. 14).

With that in mind, this research aims to assess the effects of NextRequest and other PRR platforms both at the level of functionality for agencies and, in a broader sense, the perceived overall relationship with citizens because of increased transparency.

Methodology

This survey, based on a convenience sample of public record custodians, is meant to collect experiences and opinions among a cross-section of municipalities as such portals increasingly become part of civic life. This is evaluation research, designed to ascertain the effects of a change, but it is not meant to provide a representative sample reflecting all types of agency user experiences with online PRR portals.

A link to an online Qualtrics survey was distributed June 12-15, 2018, via email to public-records officers at 86 municipalities identified through a Google URL reverse-search as having NextRequest or GovQA records portals. The link was also shared via the social media channels of the National League of Cities, and emailed to the presidents of all state municipal clerks'

associations in the U.S., with a request to forward to their members. Respondents were asked their names, titles, and jurisdictions. Though some declined to provide their names, all but one of the jurisdictions were identified by name and all were verified through Qualtrics location data, and they represent geographic diversity on a national scale, with concentrations in particular states where the association presidents opted to forward the link. Responses were accepted until March 25, 2019.

The survey consisted of 23 questions, including 6 identification/demographic queries, 13 multiple-choice questions primarily with item-specific response options, and four text-entry questions in which respondents were invited to elaborate or provide descriptions. Text-entry responses were evaluated for similarities and grouped accordingly to identify trends.

Findings

Of 127 respondents, 73 (57 percent) said their agencies do not use an online PRR portal while 54 (43 percent) said theirs do. Among those that do have online portals, answers ranged as to how many requests come to the agency each month, with a tendency toward higher volume: more than 60 requests per month (43 percent); 20 to 60 requests per month (33 percent); fewer than 20 requests per month (24 percent). All but 10 of the 73 who do not have online portals said they receive fewer than 20 records requests per month, suggesting the need for technology is correlative with the demand for public records. One respondent from a municipal fire and medical agency in Arizona wrote that he is interested in an online system for easier payment and better coordination across departments, but "our volume does not yet justify the cost."

All but three of total respondents, and all respondents who have an online PRR portal, said they are the ones who manage public-records requests for their agency, positioning them as reliable sources of information about their records request and fulfillment systems. Among those who have an online portal, NextRequest (50 percent) and GovQA (20 percent) were the most common providers named by respondents, but a series of other providers/systems were identified under "Other": JustFOIA (named by four respondents), SeamlessGov, OnBase, AgendaQuick, iCompass, QAlert, Vision, RecordTrac, CivicPlus, and three internally created systems.

Online portals rated highly among those who have them, with 72 percent saying they were "extremely satisfied" and 19 percent "somewhat satisfied." Several reasons were provided in written responses, sometimes more than one within a single response, with some trends identifiable across jurisdictions. The three most common reasons, listed by frequency of mention, are:

1. Centralization/consolidation of request management: The ease of centralizing management across departments and having one main hub, resulting in more efficient workflow, was cited 30 times as a benefit of an online portal.
2. Tracking: Twenty-one responses cited automated tracking of requests, with an emphasis on internal tracking for agency staff.
3. Ease of use for requesters: Twelve answers cited ease of use, increased access, and an overall better experience for members of the public.

Other benefits listed include speed, transparency, compliance, cost, redaction tool, and proactive release, in that order.

Nine percent of respondents said they were "neither satisfied nor dissatisfied" with their portals. None reported dissatisfaction. Respondents were also asked to name the greatest disadvantage or challenge of having an online PRR portal. Ten said they could find no

disadvantage. Of those who provided answers, the three most common issues cited, in order of frequency of mention, were:

1. System limitations: Twelve respondents named various system-specific limitations, including lack of mobile access, manual uploading of emailed or hardcopy requests and, in the case of OnBase, lack of a payment module.
2. Digital divide: Seven answers mentioned various challenges around requesters' reluctance or inability to use a digital system. A respondent in one city (population 180,000) reported "some user-friendliness issues. Tutorials and 'how-to' explanations are not helpful for individuals in our municipality who are not tech savvy and have issues learning new technologies."
3. Staff buy-in and requester abuse were each cited five times as concerns. One respondent cited "revenge requests" as a problem, in which the ease of use prompts requesters to file frivolous requests out of anger at a particular department. A second agency originally published all requests and responsive records "but shut public access down due to irresponsible use by some community members." In a third jurisdiction, records requests were published to the portal that were in fact not requests, but advertisements for business loans.

Other disadvantages listed include system bugs, slow bandwidth for uploading, and the cost of additional modules.

Nearly 41 percent of respondents with an online records portal, 22 of 54, reported receiving more requests since adopting the portal. One respondent noted that in her city, "the number of requests are rising regardless of technology, but tech helps us respond more efficiently." Only one respondent to this survey said it takes more time to fulfill requests with a portal in place. Many more, 29, said it take less time to fulfill a request, and 20 said it takes about the same amount of time. Twenty-one said the costs associated with fulfilling requests are about the same, compared with 13 who said costs have decreased, five who reported an increase, and 14 who didn't know whether there was any change.

The portals rate highly among respondents when it comes to ease of use for agency staff and the overall effect on internal processes. Seventy-two percent said the portals are "extremely easy" for agency staff to use, and 67 percent said the portals have "vastly improved" the internal process while another 22 percent said they "somewhat improved" the internal process. No respondents stated that the portals are difficult to use or that they have adversely affected internal processes.

On the external side, such as interaction with members of the public, respondents also reported improvement. Fifty-seven percent reported that the portals "vastly improved" the external process of working with requesters, while 26 percent said they "somewhat improved" the process. No one reported adverse effects on the external side.

Respondents were then asked how the portals affected the "overall relationship" between their agency and members of the public. This is broader than the external process and gets at the stated goal of services like NextRequest – to improve the relationship between government and citizen. Twenty-two percent said the relationship was "vastly improved," while 43 percent said it was "somewhat improved." Twenty-six percent reported no real difference. No one reported adverse effects on the relationship, but five respondents (9 percent) checked "Other" and wrote answers such as "too soon to tell" or "I was not here before implementation." There were no discernible trends when it came to linking these responses to providers. In other words, the choice

of provider (NextRequest, GovQA, JustFOIA or the others) did not seem predictive in determining how respondents viewed the effect on the overall relationship with the public.

Respondents were asked to elaborate via text entry on whether/how their portals have affected their agency's overall relationship with the public, and they provided a range of answers. Most continued to focus on process-level improvement for users, including easier submission, faster service, and increased transparency. Some commented on how this has positively affected the relationship with constituents: "I believe the portal has improved the relationship between the public and the agency because it has made it easier to be transparent." Similarly, "a greater sense of trust from the public to the governmental body due to efficiency, time management, and a commitment to transparency."

Others used the space to describe new or continuing challenges related to the overall relationship with constituents. Some commonalities among responses include:

1. Lack of public awareness/interaction: Relationships with citizens can be hard to gauge. Likewise, some residents do not notice changes in service. Representative comments included:
    - "The public does not seem aware of the change. In addition, we cannot require requestors [*sic*] to use a certain method of requesting (the Texas PIA only requires that the request be in writing, so can be lipsticked on a napkin, painted on a rock, email, anything in writing), so there's been no massive transfer in how requests are received."
    - "a large majority of our request [*sic*] are from business entities seeking leads. Typically they are not located locally and do not benefit our residents or the public in general."
    - "We haven't received direct feedback from citizens but hope that the ease of making a request and increased access to records will foster trust."
2. Heightened expectations: A faster, easier system has in some cases raised expectations among users. For example:
    - "Some complex requests still take a long time to process. Customer expectations are for instant access."
    - "Because the portal is 'live' requesters expect immediate responses which is problematic when public records officers are juggling multiple requests. The result is that they are suspicious of responses that are not 'immediate.'"
    - "Easy access does not equate easy work, but gives impression [*sic*] to users that finding records is easy."
3. Technology/format concerns: One respondent noted that some residents prefer "the old way" of doing things. Other quotes:
    - "Some people appreciate the responses electronically and other [*sic*] do not."
    - "The Gov QA Records Request Portal requires customes [*sic*] to create accounts and log in. Not all are pleased with this. Some customers have trouble downloading productions or reading messages."

As previously mentioned, most respondents said they rarely, if ever, opt to make responsive documents publicly available. Of the 54 who reported having an online PRR portal, 24 said they never publish responsive documents for public view, while 11 said they rarely do. Fourteen reported sometimes or often sharing responsive documents, and only 5 said they always do. However, five respondents noted that they are considering or working toward making requests

and/or responsive documents available to the public, in keeping with the "release to one, release to all" and open data trends.

Similar to those that don't publish responsive records, 26 agencies said they never publish the actual records requests, while 11 said they always do. Sixteen said they also make public the identities of requesters. Fourteen said they do not. Twenty-four said they will reveal requesters' identities only if that information is requested by PRR.

Discussion

Although the sample is but a fraction of the hundreds of agencies that use online PRR portals, let alone the nearly 90,000 local governments that exist in the U.S. by last Census count, this research suggests a strong favorable view toward PRR portals, with approximately 9 out of 10 records managers expressing satisfaction with them, 7 expressing extreme satisfaction. Likewise, approximately 9 out of 10 report improvement in their agency's internal process of managing and responding to records requests, with three-quarters of that group reporting vast improvement. Slightly fewer, 8 of 10, report improvement in their external process of working with requesters, also with three-quarters reporting vast improvement. When it comes to the portals' effect on the overall relationship between citizen and institution, 6.5 of 10 report improvement. However only one-third of that group report a vastly improved relationship versus a somewhat improved relationship.

There could be several reasons for this deviation. The most obvious is that agency staff are primarily concerned with the job before them, and they operate from the perspective of managing complex PRR systems. The text-entry comments reflect this, as the majority of praise focuses on the centralization and efficiency of one digital hub for PRR processing. Ease of use for the requester is also frequently mentioned but less than half as often. As some express in their answers, they hope a more efficient system will result in higher user satisfaction, but that is the order in which the benefits flow – from agency to citizen.

Also, a digital platform can only do so much. Manik-Perlman made this point herself during the GovLove podcast. "It really is not just software, it's really a process. Technology is not going to solve other problems in process that an agency might have" (Wyatt, 2016).

A PRR portal, like any system, still relies on people to complete the work involved. One survey respondent noted this in describing the challenges she faces even with a portal: "To locate a record, it still requires corresponding with the department that is the custodian of the record. The lenght [*sic*] of the process is dependant [*sic*] upon the ablity [*sic*] of the staff to locate the record, not the request platform."

If there are flaws or failings in the realms of policy or personnel, a digital system might highlight those shortcomings and erode any gains in goodwill. Recall that the Harvard Business School paper on occupational transparency compared the responses of Group 1, the Boston residents were given only a tally of service requests, with those of Group 2, who received specific operational details. Yet a third group was provided all of that information, plus the substantial backlog of service requests that had not yet been resolved. The results showed that participants in Group 3 "were no more trusting of government nor more supportive of government programs" than those in Group 1 (Buell, Porter & Norton, 2018, p. 14).

In the case of PRR portals, increased transparency can raise difficult policy questions, including what information should be shared and how to safeguard information that shouldn't be available. Would an agency bear greater liability if redactable information is accidentally included

in a published document? Should requesters be identified? Just how much should an internal process be laid bare?

In spring 2017, Evanston, Illinois's newly elected city clerk, Devon Reid, opted to make public all requests and responsive documents on the city's NextRequest platform. That fall, city leaders voted to take the portal offline for review after the names of a juvenile and a sexual assault victim were made visible in published records (the victim's name was redacted in all areas of a police document except one, while Reid said he did not redact the juvenile's name because the 12-year-old boy had spoken publicly and received media attention) (Bookwalter, 2017). In December 2017, the leaders unanimously approved a new policy that keeps all requests and responsive documents private, despite Reid's claim that making them public relieved his staff's workload (Bookwalter, 2018). As of March 2019, requests were once again visible on the site, dating back to October 2018, but responsive documents remain private, shared only with requesters.

Another consideration, albeit a waning one as digital natives predominate, is the reluctance or inability of some members of the public to use digital services. As one respondent noted, jurisdictions are still required to accept PRRs in various forms, including paper. Records managers in several agencies said they upload those requests to the portals to ensure internal tracking and provide an audit trail. But on the external side, any requester who is unable or unwilling to use the portal is not provided the same range of communication and service as those who are, potentially creating a disproportionate benefit. One of the challenges in the development of e-participation in government has been the inclusion of low-income, older, and technology-challenged citizens (Bailey & Ngwenyama, 2011), and this area is no exception.

Potentially more consequential than a citizen's distance from digital, either voluntary or involuntary, is one's fervent embrace of it. As reflected in the survey, several agencies are dealing with more requests as the portals – not to mention nongovernmental services like MuckRock – make the request process easier and faster.

San Diego provides an illustrative example. Ten years ago, in 2009, the city received 344 requests under the California Public Records act, according to public records. That number grew to 1,210 in 2013, and ballooned once the city adopted a NextRequest portal in late 2015. Despite providing a searchable repository of responsive documents, the city received 2,928 requests in 2016, 3,792 in 2017, and 4,752 in 2018. City spokeswoman Katie Keach said staffers were striving to keep up:

> but the fact is the NextRequest system has been extremely popular because of how easy it is to use and we've seen a significant increase in requests over the past couple years as a result. The volume, complexity and number of departments involved in the request can all contribute to the amount of time it takes to collect the responsive documents, conduct a legal review if necessary, and then distribute to the requester. (Schroeder, 2017, para. 9)

Reid, Evanston's city clerk, also attributed an increase in PRRs to the digital portal, now averaging about 100 per month compared to 50 per month pre-portal (Kanowitz, 2017):

> I did notice that during the period we took the NextRequest system down to have a review of it, that we actually decreased the number of FOIAs that were coming in, so having a site that is easily accessible for folks actually increases the requests. (Baim, 2017, para. 11)

Conclusion

These findings reflect a strongly positive view of the effects and efficacy of online PRR portals by record custodians, with the greatest derived benefits for internal processes and agency staff. External processes are also improved, though slightly less so. Improvement is also reported in the overall relationship between public and agency, but to an even lesser degree.

This could be for several reasons, including insufficient metrics for measuring that relationship or an overall difficulty in communicating with citizens beyond process-level interactions, plus tangible factors such as heightened expectations, a reluctance or inability to embrace digital systems among some constituents, increased demand that can strain agency resources, and other challenges. In other words, online PRR portals appear to significantly ameliorate a longstanding pain point, but could raise other challenges unique to digitized, transparent systems, challenges that require a rethinking of policies and processes. So far, it appears the benefits outweigh drawbacks for agency staffers.

This is only a step toward what should be a full examination of online PRR portals. This research was done with the employees who work with and manage these portals on the agency side, so the views reflected will naturally skew toward their priorities. Clearly more can be done to gauge the requester experience with these portals, including qualitative and quantitative data collection. Civic tech companies earn government clients by promising cost-savings, efficiency, and solutions, but also quite often an improved relationship with citizens. Given the ramifications of a system that operates to guarantee and preserve transparency, an underpinning of any healthy democracy, that side of the equation deserves further study as more and more agencies adopt online PRR portals.

References

2019 GovTech 100. (n.d.). *Government technology*. Retrieved from https://www.govtech.com/100/2019

About MuckRock. (n.d.). *MuckRock*. Retrieved from https://www.muckrock.com/about

About OpenRECORDS. (n.d.). *OpenRECORDS*. Retrieved from https://a860-openrecords.nyc.gov/about

Accenture. (2015). *Digital government: Your citizens are ready, willing… and waiting*. Retrieved from https://www.accenture.com/t20170228T002251Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_16/Accenture-Your-Digital-Citizens-Ready-Willing-Waiting-2.pdfla=en

America's Best Open FOIL Web Site: Oakland's RecordTrac. (2014, February 18). *Reinvent Albany*. Retrieved from https://reinventalbany.org/2014/02/americas-best-open-foil-web-site-oaklands-recordtrac

Bailey, A., & Ngwenyama, O. (2011). The challenge of e-participation in the digital city: Exploring generational influences among community telecentre users. *Telematics and Informatics, 28*(3), 204-214.

Baim, N. (2017, November 8). Evanston residents urge city clerk to adjust FOIA process. *The Daily Northwestern*. Retrieved from https://dailynorthwestern.com/2017/11/08/city/evanston-residents-urge-city-clerk-adjust-foia-process

Buell, R. W., Porter, E., & Norton, M. I. (2018). *Surfacing the submerged state: Operational transparency increases trust in and engagement with government*. Retrieved from the Harvard Business School website: https://www.hbs.edu/faculty/Publication%20Files/14-034%20(5)_92766f66-c1b7-459d-825f-fe9fc1231197.pdf

Capeloto, A. (2014, October 27). This open-source app could make the FOI process less terrible. *Columbia Journalism Review*. Retrieved from https://archives.cjr.org/united_states_project/recordtrac_making_the_foia_process_less_terrible.php

City of Oakland. (n.d.). *Justification: NextRequest*. [Internal memo].

Cuillier, D. (2017). *Forecasting freedom of information*. Retrieved from the Knight Foundation website: https://knightfoundation.org/reports/forecasting-freedom-of-information

Eil, P. (2016, July 3). MuckRock's approach is working, one FOIA at a time. *Boston*. Retrieved from https://www.bostonmagazine.com/news/2016/07/03/muckrock-foia-turns-50

Fretwell, L. (2014, January 21). 2013 GovFresh awards winners. *GovFresh*. Retrieved from https://govfresh.com/2014/01/2013-govfresh-awards-winners

Higgins, P. (2015, May 4). Oakland's awesome public records request system. *Parker Higgins dot net*. Retrieved from https://parkerhiggins.net/2015/05/oaklands-awesome-public-records-request-system/

Howard, A. (2016, June 24). 7 ideas to make the Freedom of Information Act better. *Sunlight Foundation*. Retrieved from https://sunlightfoundation.com/2016/06/24/7-ideas-to-make-the-freedom-of-information-act-better

Hull, A., Manik-Perlman, T., & Duecy-Gibbs, R. (2014, October 27). *Welcome to NextRequest, the open public records portal*. Retrieved from

http://blog.postcode.io/post/101138657517/welcome-to-nextrequest-the-open-public-records

International City/County Management Association (2017). *2017 Government technology solutions survey*. Retrieved from https://icma.org/sites/default/files/2017%20Government%20Technology%20Solutions%20Survey.pdf

Kanowitz, S. (2015, August 6). Public record requests made easy (for government). *GCN*. Retrieved from https://gcn.com/articles/2015/08/06/nextrequest-public-records.aspx?admgarea=TC_Cloud

Kanowitz, S. (2017, February 28). Digging out from under records requests. *GCN*. Retrieved from https://gcn.com/Articles/2017/02/28/managing-records-requests.aspx?Page=1

Knight Foundation and Rita Allen Foundation. (2017). *Scaling civic tech: paths to a sustainable future*. Retrieved from https://s3.amazonaws.com/kf-site-legacy-media/feature_assets/www/civictechbiz/assets/Scaling_Civic_Tech_final.pdf

Manik-Perlman, T. (2017, March 28). City of Oakland NextRequest proposal.

Matter Ventures (2015, June 23). *Matter Four Demo Day NextRequest* [Video file]. Retrieved from https://vimeo.com/131581512

Morisy, M., & Kotler, M. (2018, March 12). MuckRock release notes: Confidently leaping ahead into Sunshine Week. *MuckRock*. Retrieved from https://www.muckrock.com/news/archives/2018/mar/12/mrn-sw

NextRequest (n.d.) *Crunchbase*. Retrieved from https://www.crunchbase.com/organization/nextrequest#section-overview

Norris, D. F., & Reddick, C. (2011). *Electronic government 2011*. Retrieved from the International City/County Management Association website https://icma.org/sites/default/files/302947_E-Government%202011%20Survey%20Summary.pdf

Noveck, B. S. (2016). Is open data the death of FOIA? *Yale Law Journal*, *126*(2), 273.

Opsahl, R. (2016, February 1). Evanston launches online public records portal, database. *The Daily Northwestern*, p. 1.

Phillips, M. (2016, July 12). *GovTech: Disrupting government through access and transparency.* [Audio podcast]. Retrieved from https://www.sparkpluglabs.co/powerful-conversations/episode53

Rumbul, R., & Shaw, E. (2016). [The role of civic technology in e-government evolution]. Unpublished raw data.

Rumbul, R., & Shaw, E. (2017). *Civic tech cities*. Retrieved from mySociety website: http://research.mysociety.org/publications/civic-tech-cities

Schroeder, L. (2017, November 22). Access to city records can take weeks with new online portal. *The San Diego Union-Tribune*. Retrieved from https://www.sandiegouniontribune.com/news/watchdog/sd-me-nextrequest-database-2017122-story.html

Shaw, E. (2016, April 11). Why civic technologists should still care about e-gov. *Civicist*. Retrieved from https://civichall.org/civicist/why-civic-technologist-should-still-care-about-egov

Stern, A. (2018). *Open data policy and FOI law*. Retrieved from the Sunlight Foundation website: http://sunlightfoundation.com/wp-content/uploads/2018/10/alena-white-paper-PDF.pdf

The 60-second interview: Tamara Manik-Perlman, C.E.O. and cofounder of NextRequest. (2015, July 29). *Politico*. Retrieved from https://www.politico.com/media/story/2015/07/the-60-second-interview-tamara-manik-perlman-ceo-and-cofounder-of-nextrequest-004006

Wang, S. (2016, November 29). Twice the FOIA fun: MuckRock bulks up its records request resources with the free FOIA Machine tool. *Nieman Lab*. Retrieved from http://www.niemanlab.org/2016/11/twice-the-foia-fun-muckrock-bulks-up-its-records-request-resources-with-the-free-foia-machine-tool

Wood, C., Knell, N., Pittman, E., Newcombe, T., Eidam, E., McCauley, R., & Mulholland, J. (2016, July 20). Digital counties survey 2016: Winners make collaboration, innovation, civic engagement top priorities. *Government Technology*. Retrieved from https://www.govtech.com/dc/articles/Digital-Counties-Survey-2016-Results.html?page=2

Wyatt, K. (2016, February 5). *Local government technology, NextRequest and Seneca Systems.* [Audio podcast]. Retrieved from https://medium.com/@ELGL50/podcast-intersection-of-local-government-and-technology-cd90ca5a3ba0

the journal of CIVIC INFO

The Journal of Civic Information

Volume 1 | Number 1 September 2019

Journal homepage: https://journals.flvc.org/civic/ ISSN (online): 2641-970X

Tracing Home Address Exemptions in State FOI Laws

Jodie Gil *

Article Information

Received: Jan. 2, 2019

Accepted: Feb. 13, 2019

Published: Sept. 4, 2019

Keywords

Freedom of information
Public records
Personally identifying information
Personnel records
Home addresses
Privacy

Abstract

Privacy concerns have prompted many states to close off once-public information from release through the freedom of information process. This study looks at the personal privacy exemptions for home addresses in 50 states and Washington, D.C., in both 2011 and 2019. There were 16 instances of a change in state law during that time – only three toward more transparency. Voter registration records were the most open of the three categories reviewed, with more than half the states requiring disclosure of home addresses in 2019. This study can help guide journalists, policy makers and records holders as they navigate proposed changes to FOI laws.

* Jodie Gil, Southern Connecticut State University. Please send correspondence about this article to Jodie Gil at gilj4@southernct.edu. An earlier version of this work was presented at the National Freedom of Information Coalition summit FOI Research Competition, April 12, Dallas, Texas.

To cite this article in Bluebook: Jodie Gil, *Tracing home address exemptions in state FOI laws,* 1(1) J. CIVIC INFO 75 (2019).
To cite this article in APA: Gil, J. (2019). Tracing home address exemptions in state FOI laws. *Journal of Civic Information, 1*(1), 75-118.

DOI: https://doi.org/10.32473/joci.v1i1.115660

Introduction

In a December 2018 editorial, the *New York Times* declared that the public availability of home addresses has become a potential tool to harm people. "Times have changed," the editorial board wrote, "and the information provided by these new online databases aren't weaponized only by trolls, but also by stalkers, domestic abusers and criminals" ("Opinion: Home Addresses," 2018). It's an example of a once-public record being reconsidered in the Internet era – and a hot-button issue among privacy advocates and those who fear government is becoming too closed off.

In an age of big data and easy access to information online, personal information gathered by governmental agencies has the potential to become public in ways previously unimaginable. With changes in technology, more information has become searchable and widely accessible. Databases and algorithms make it easier than ever to match up discrete pieces of information with identifying details, further adding to privacy concerns. This growing access has been met with growing apprehension about personal privacy (McCall, 2018; McDermott, 2017). The more concerned about privacy the public becomes, the more likely officials will respond by closing off open records laws (Cuillier, 2004, 2017).

Because of the complex nature and variety of state laws, however, limited research has compared the text of state laws across the country (Chamberlin, Popescu, Weigold, & Laughner, 2007). This study looks at open records laws in the context of personal privacy – specifically how state laws deal with the disclosure of home addresses. This information has traditionally been seen as basic directory information (Byrne, 2010; Harper, 2006), and therefore serves as a proxy for growing concerns about personal privacy. Using a color scale to measure the approach to public records, this study provides a quick comparison guide for journalists, policymakers and records-holders to understand exactly how states treat home addresses for three records types: Personnel Records, Firearms Applications and Permits, and Voter Registration Lists. The results provide important context for why certain records are exempt from disclosure, and a comparison for how states approach the balance of private versus public information. That context can help states make more careful decisions about records dealing with personal information, so as to more appropriately balance the public's right to know with the individual need for personal privacy.

Literature review

Freedom of information laws

The 1966 federal Freedom of Information Act gives the public the "right to request access to records from any federal agency" (Department of Justice, n.d., "About page"), where the Constitution and the First Amendment don't explicitly allow for it (Schauer, 2018). When members of the public seek information about state or municipal governments, however, they must turn to one of 51 different laws covering open government in 50 states and the District of Columbia. These laws (herein referred to under the umbrella of "freedom of information (FOI)" laws) dictate access to records and meetings within the respective states. Despite the adoption of FOI laws in each state and at the federal level, the public does not have completely open access to records. Each law comes with some form of exemptions – scenarios where public officials can or must withhold information. These exemptions range from general to specific, depending on the state, and include topics ranging from trade secrets to personal information (Reporters Committee for Freedom of the Press, 2019). Public officials routinely take advantage of the exemptions

outlined in state laws, according to a survey of 228 Freedom of Information experts, which found about 87% had some problem with agencies overusing exemptions to the laws: 23% called it "somewhat problematic," 30.5% called it "very problematic" and 34.3% called it "extremely problematic" (Cuillier, 2017).

Personal privacy

Personal privacy is multifaceted and complex, and no single definition fully serves the different perspectives. Smith, Dinev, and Xu (2011) distinguish between physical privacy, such as concerns about others seeing into personal space, and information privacy, regarding communications from, and details about, a person. Even under the umbrella of information privacy, different disciplines have different definitions of privacy, including privacy as a right, privacy as a commodity, privacy as a state of being, and privacy as a form of control over information about oneself (Smith et al., 2011, p. 994-995).

It is problematic to define control over information because sometimes a person might want to keep information private, but there are legitimate reasons to disclose that information to the public (Swanson, 2009). At the same time, the perception of what should remain private varies from person to person. Lane (2009) notes Americans' different levels of disclosure on early communication platforms, such as postcards and telegrams. "The sheer variety of personal disclosures makes it clear that it is next to impossible to create a 'right to privacy' that encompasses every type of personal disclosure; what one person might consider a trivial disclosure, another might find mortifying" (Lane, 2009, p. 32).

Since Warren and Brandeis (1890) outlined a right to personal privacy, countless articles have addressed privacy concerns and the potential conflict with open government. Some (Solove, 2002) argue that personal information contained within public documents is not necessary to release in order to allow for transparent actions from governmental agencies. The way information is stored may prompt privacy concerns as well, such as when information from several different records is compiled into a single database (DOJ v. Reporters Committee, 1989). Others look at the public good that can come from knowing even personal details. For example, Boles (2012) argues that access to death certificates helps the public by allowing closure for extended family members, giving the public a chance to review trends in deaths and medical malpractice, and allowing for historical research. Swanson (2009) argued for the need for some personal information to become public, and proposed a balancing test for disclosure rather than a test for withholding that information. "Personal information allows people to make judgments about whether to trust or associate with someone; more truthful information leads to more informed decisions" (p. 1607). Her balancing test gives preference to the public use of the information, and the impact it has on others. Records that "substantially impacts others" and do not "conflict with the primary purpose of the practice at issue with the record" should be disclosed under the test (p. 1603).

Several states address privacy in their FOI laws with catchall exemptions that balance personal privacy with the public's right to know. The definitions often include phrases such as "clearly unwarranted invasion of personal privacy," and "highly personal or objectionable to a reasonable person and in which the subject's right to privacy outweighs any legitimate public interest in obtaining the information," such as in Illinois' law (Illinois). In Kansas, privacy is defined as "revealing information that would be highly offensive to a reasonable person, including information that may pose a risk to a person or property and is not of legitimate concern to the

public" (KSA 45-217(b)). These definitions leave the interpretation to the records holders, or ultimately, the courts.

Personally identifying information

When dealing with privacy, often the issue concerns personally identifying information, such as address, phone number, and Social Security Number. Some researchers (Byrne, 2010; Harper, 2006) consider personally identifying information such as home addresses as basic directory information. However, there is a growing sentiment that access to such information has a potential for harm (McCall, 2018; "Opinion: Home Addresses," 2018), or at a minimum, is not publicly necessary to release (Department of Defense, 1994).

The 1994 Driver's Privacy Protection Act was an early recognition by governmental agencies that releasing private citizens' personally identifying information could lead to stalking and harassment (Karras, 1999). More recently, in a December 2018 report, the Oregon Public Records Advocate outlined three main concerns – identity theft, doxxing, and swatting – to releasing personally identifiable information (McCall). In particular, doxxing and swatting relate to home addresses. Doxxing is collecting and publishing documents about a person, often revealing personal information (McNealy, 2018). The act can result in threats to the individual, including those where people show up at the address of the victim (McCall, 2018). Swatting involves calling 911 to send police or SWAT teams to a person's home when there is no real emergency (FBI, 2013). Because of these concerns, many states allow residents to opt out of disclosure of their home addresses for specific reasons, including concerns about personal safety (Shoemyer, 2009).

Based on the concerns by the public and policymakers of the release of home addresses in government records, and concern by FOI advocates that closure of this very information can harm the public good, this study seeks to answer the following two questions:

RQ1: How do states treat home addresses as a publicly disclosable record?

RQ2: At the state level, what changes have occurred between 2011 and 2019?

Methodology

Comparing individual aspects of open records laws across states is difficult because of the unique way each state handles its law. Appeals court decisions, state statutes and state constitutions each impact the final interpretation and implementation of individual state laws. Additionally, some states have exemptions that provide a balancing test for records. Meanwhile, not all states require record holders to withhold all documents listed in the exemption sections. For example, in North Dakota exempt records "may be withheld at the discretion of the public entity" while confidential records "cannot be released" (North Dakota Office of Attorney General, 2016, p. 2).

Because of these complications, past comparisons of state FOI laws typically fall into four categories: Rankings based on selected criteria (Better Government Association, 2008, 2013); in-depth reviews of individual state laws and their connection to personal privacy (Byrne, 2010; Farro, 2014; Rydell, 2011); cross-state FOI compliance checks, (Fink, 2018); and analyses of a narrow exemption from a sample of state laws (Boles, 2012; Swanson, 2009). This review seeks to expand on this last category by looking at exemptions for three record types across all 50 states and the District of Columbia. While this slice of information may seem limited, it provides a glimpse at how all states handle the same information.

To address the research questions, this study used three phases of analysis, relying primarily on the Open Government Guide published by the Reporters Committee for Freedom of the Press in 2011, and the updated guide published in January 2019. First, the laws in 50 states and Washington, D.C., were reviewed through thematic analysis, which is "useful for summarizing key features of a large data set" (Nowell et al, 2017, p.2) and provides flexibility for situations such as the comparison of disparate state laws. The thematic analysis helped organize the different approaches states take to disclosure or exemptions in all records. More specifically, states can always exempt release of a record, have a balancing test to determine if a record should be disclosed, exempt the release of a record in certain specific situations or for specific people, or always require the release of a record.

Second, using those themes, a content analysis of each individual law, as published in the 2011 and 2019 Open Government Guides, was conducted. This content analysis quantified how states specifically approach disclosure of home addresses for Personnel Records, Firearms Permits, and Voter Registration Lists. These records were chosen for two reasons. First, the Open Government Guide specifically analyzes each type of record, which helped make a comparison across states. Second, the three types of records represent different types of home address disclosure. For Personnel Records, the home addresses are included in records that do not necessarily deal with public actions or decisions. With Firearms Permits, home addresses are included with records as a basis of governmental regulation of a matter of public concern. Firearms Permits straddle the balance of public concern over who has been granted access to legally use weapons and the individual desire for privacy about a tool used for personal protection (Swanson, 2009). Voter Registration Lists include information of the highest level of democratic value, as they deal directly with the public's ability to weigh in on decisions of elected officials and public spending. Especially in light of recent concerns about voter registration (Wines, 2016; Graham, 2016; Farley & Robertson, 2018), home addresses in these records are arguably more important for the public to access than, say, Personnel Records.

Finally, the completed list of exemptions for each state was sent to an FOI expert in that state for verification. The experts included lawyers, journalists, and other open government advocates. They were chosen from the contact information listed on the National Freedom of Information Coalition website under each state's FOI resources. In some cases, the request for verification was forwarded to another expert not listed on the website. A total of 17 responses were received, and in some cases, information in the data was updated to reflect more nuanced details than those that were available in the Reporters Committee Open Government Guide. When information was added to the analysis, a note is included in the comments in the appendix.

The access to home addresses for the three record types was measured on a scale represented by four colors – green, light yellow, dark yellow, and red. The data are available in tables by record type and also by state, in the appendices. Green represents a law that allows access to home addresses for the record. Light yellow indicates a state that has a balancing test for release of home addresses in the particular record. Past court cases related to the release of the record are noted in the comments column of the tables in the appendix. Dark yellow indicates a law that limits access based on the individual or person listed in the record. Red indicates home addresses are explicitly exempt from release for the record. (See appendices A and B for color-coded results.) Three states did not have a 2019 Open Government Guide published by the Reporters Committee for Freedom of the Press as of July 1, 2019, when the review was conducted. In each case, requests for additional details were sent to FOI representatives from that respective state. Updated information was added to one of the states through these requests.

Results

Overall, the largest group of records (63) fell under the classification of always exempt, while the smallest group of records (20) fell under the classification of balancing test. See Table 1. The type and frequency of exemptions largely depended on the type of record. For example, home addresses from Personnel records and Firearms records were most often always exempt from disclosure, while for Voter Registration records, the majority of states allow for disclosure of home addresses, or allowed for only some individuals to be exempt from the disclosure.

Table 1
2019 Home Address Exemptions

Type of exemption	Personnel	Firearms	Voter Registration	Total
Always disclosable	3 (5.9%)	3 (5.9%)	34 (66.6%)	40
Balancing test	14 (27.5%)	6 (11.8%)	0 (0%)	20
Individual exemptions	8 (15.7%)	1 (2%)	12 (23.5%)	21
Always exempt	24 (47.0%)	36 (70.6%)	3 (5.9%)	63
No data available	2 (3.9%)	5 (9.8%)	2 (3.9%)	9
Total	**51**	**51**	**51**	**153**

Personnel records

In 2019, only three states (Alaska, New Mexico, and Tennessee) listed home addresses as always disclosable, while 24 always exempted the information. Eight states had exemptions for specific individuals, and 14 required some sort of balancing test or agency interpretation before disclosure. Two states did not have data available for 2019. Both states always exempted the information in 2011. See Table 2 on the next page. Several states list specific personnel details that can be publicly disclosed, and most deal with information related to the task of the employee's job. For example, in Idaho, Indiana, Iowa, Minnesota, Nebraska, New Jersey, North Carolina, and Wyoming, the laws specifically list only job-related information as disclosable. This information includes salary, qualifications for employments, routine work-related directory information, length of service, title, position, and employment dates. Other states, such as Arkansas, Delaware, Georgia, Maine, Maryland, and Oklahoma, specifically exempt personal details such as home address, telephone number, and Social Security Number. In Rhode Island, an employee's city or town or residence is public, but not the specific home address.

Table 2
Personnel Record Exemptions

Type of exemption	2011	2019
Always disclosable	4	3
Balancing test	14	14
Individual exemptions	9	8
Always exempt	24	24
No data available	0	2
Total	**51**	**51**

States with individual exemptions most often included public safety officers and court employees as exempt from home address disclosure. In Florida, the list of employee types exempt increased from 2011 and 2019, to include tax collectors, inspectors general, investigators in the Department of Business and Professional Regulation, certain Department of Health employees, and U.S. military service members. Connecticut includes in its home address exemptions banking employees and those working for the Department of Children and Families. In Louisiana, any public employee may request his or her home address be kept confidential. In Alaska, personal information is defined in the law, and home addresses are specifically excluded.

Firearms applications and permits

In 2019, only three states (Idaho, Mississippi, and New York) listed firearms applications and permits as always disclosable, while 36 listed the records as always exempt from disclosure. Six states required some sort of interpretation or balancing test, and one – California – had exemptions for specific public safety officers. Some states, including Colorado and Vermont, do not require residents to register firearms or receive permits, so there is no list of addresses to be disclosed or exempt from disclosure. They are among five states without data for 2019. See Table 3, next page.

Table 3
Firearms Permits and Licenses Exemptions

Type of exemption	2011	2019
Always disclosable	15	3
Balancing test	7	6
Individual exemptions	1	1
Always exempt	27	36
No data available	1	5
Total	**51**	**51**

Most of the changes in law between 2011 and 2019 came in this records category – and most often toward less transparency. Iowa, Kansas, Louisiana, Maryland, North Carolina, Oklahoma, Oregon, Tennessee, Virginia, and West Virginia all made changes that exempted firearms permits, specifically home addresses, from disclosure, after previously having more open laws. For example, in Virginia, firearms permits were completely open prior to 2008, when the law changed to only allow review at a local courthouse. Then in 2013, the legislature changed the law to prohibit release of permit information at courthouses, essentially closing off the records to the public (Rhyne, M., personal communication, Jan. 18, 2019). In West Virginia, the state legislature amended the open records law in 2015 to specifically exempt firearms application information, but then later removed the requirements to carry a permit, leaving the exemption moot (Reporters Committee, 2019).

Voter registration records

Voter Registration records were the most open of the three categories reviewed, with two thirds of the states requiring disclosure of the records, including home addresses, in 2019. See Table 4. Three states – Kentucky, Michigan, and Vermont – changed their laws between 2011 and 2019 to make the records more accessible to the public. Only Oklahoma made a change toward more privacy, allowing the state election board to keep confidential the home addresses of certain victims and public safety or court employees. Twelve states allow residents to keep their home addresses confidential, particularly if they are victims of domestic violence. In Alaska, any resident can request his or her address be kept confidential on Voter Registration records. In Virginia, anyone using a P.O. Box address on the Voter Registration record can be exempt from home address disclosure (Rhyne, M., personal communication, Jan. 18, 2019).

Table 4
Voter Registration Exemptions

Type of exemption	2011	2019
Always disclosable	33	34
Balancing test	0	0
Individual exemptions	12	12
Always exempt	6	3
No data available	0	2
Total	**51**	**51**

Overall changes

State laws changed in 16 instances during the review time frame. See Table 5 below. In only three instances was that change toward more transparency – all of those being for Voter Registration records. In the other 13 instances, the laws were changed to put more limits on access to the public records. In particular, the majority of those limits were found in firearms permits and applications records.

Table 5
Change in home address exemptions from 2011- 2019

Record Type	More transparent	Less transparent
Personnel records	0	2
Firearms permits	0	10
Voter registration	3	1
Total	**3**	**13**

Discussion

The December 2018 editorial in the *New York Times* was surprising, not because it advocated for more privacy for home addresses – that is a standpoint that has been growing since the 1994 Driver's Privacy Protection Act. The editorial is interesting in its source – a journalistic outlet that typically fights for open records, indicating a growing shift in how home addresses are perceived as a public record. That most of the records reviewed here are always exempt from disclosure is not surprising in light of the literature, which shows concerns about personal privacy, including home addresses. Likewise, the areas of change found in this review are expected within the context of two national conversations taking place: Allegations of potential voter fraud after national elections, and debates about gun control in the wake of several high-profile shootings.

When claims of voter fraud are alleged, advocates seek to prove the claims through comparisons of voter registration records, including home addresses (Levitt, 2007). After claims of voter fraud in the 2016 presidential election, and 2018 midterm elections (Wines, 2016; Graham, 2016; Farley & Robertson, 2018), then, it stands to reason that this record type is valued as open to provide a measure for checking voter rolls after contentious elections. The law changes to make this record type more open happened before the 2018 midterm elections, but the continued debate around the topic indicates that this record may continue this same trend.

Gun control has been a national debate for years, one that intensified after the 2012 shooting at Sandy Hook Elementary School in Connecticut. In some cases, that debate brought to light the public nature of firearms permits. For example, in New York, the *Journal News* published a list of gun permit owners in two New York counties and a map of their home addresses to inform the public about who in their communities owned guns (Maas & Levs, 2012). New York gun owners were outraged. In response, addresses of journalists working for the newspaper were published online, and the staff was harassed and threatened (Haughney, 2013). The following year, the state passed the New York Secure Ammunition and Firearms Enforcement Act, which among other features, allowed gun permittees to opt out of disclosure of their home address, which more than 15,000 had done a little over a year later (Worley, 2014). Arguments against disclosure of firearms records include owner concerns about gun theft and personal safety of the permittees. Swanson (2009), on the other hand, argues that firearms permits, and the personally identifying information included in them, should remain public because they reveal important public safety role of government agencies in deciding who should be allowed to own or carry firearms. In general, it seems, the concerns about personal safety of gun owners has had more impact on state laws.

Limitations

As with any study, there are some limitations here. While an effort for external validation was made, and about a third of the FOI experts queried responded, that leaves two thirds of the state evaluations unchecked by an outside source. The feedback from the 17 FOI experts, however, validated the data with only some clarifications. This lends confidence to the rest of the data contained in the appendix. Another limitation is the lack of 2019 data for two states, which makes an overall comparison difficult.

Future research on this topic could add the data from the two missing states if the Reporters Committee updates its Open Government Guide, or by using the most recent FOI laws in those

states. Researchers may also look to expand on the categories of record exemption reviewed to get a bigger picture sense of how states handle other types of information, or compare home address exemptions in other countries' FOI laws.

Recommendations

With growing privacy concerns prompting many to reconsider what personal information should be publicly disclosable, this review of home addresses exemptions can help guide strategic response to proposed changes to state FOI laws. Considering widespread concerns about home address information being made public, including from organizations that typically advocate for government transparency, it makes sense to work toward a middle ground when changes to open records laws are proposed. That middle ground can come from laws that provide flexibility in balancing tests or limited exemptions based on the individuals in question. A balancing test will require an outside agency or judge to weigh in on the release of records, adding an extra step to release. While this may become cumbersome and problematic based on the viewpoint of those in charge of evaluating release, the practice would be better than an all-or-nothing view of records release.

References

Better Government Association and Alper Services Inc. (2008). *Integrity index*. Chicago, IL.

Better Government Association and Alper Services Inc. (2013). *Integrity index*. Chicago, IL.

Boles, J. R. (2012). Documenting death: Public access to government death records and attendant privacy concerns. *Cornell Journal of Law & Public Policy*, *22*(2), 237-288.

Byrne, D. (2010). Access to online government public records: The privacy paradox. *Legal Reference Services Quarterly, 29*(1), 1-21.

Chamberlin, B. F., Popescu, C., Weigold, M. F., & Laughner, N. (2007). Searching for patterns in the laws governing access to records and meetings in the fifty states by using multiple research tools. *University of Florida Journal of Law & Public Policy,18*, 415-455.

Cuillier, D. (2004). Public support for press access declines as personal privacy concerns increase. *Newspaper Research Journal*, *25*(4), 95-103.

Cuillier, D. (2017). Forecasting freedom of information: Why it faces problems – and how experts say they could be solved. John S. and James L. Knight Foundation study. Retrieved from https://kf-site-production.s3.amazonaws.com/publications/pdfs/000/000/232/original/FOI-final-unlink.pdf

Department of Defense v. FLRA. (1994). Retrieved from https://supreme.justia.com/cases/federal/us/510/487/

Department of Justice. FOIA.gov - Retrieved from https://www.foia.gov/about.html

DOJ v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

Farley, R., & Robertson, L. (2018). Bogus voter fraud claims. FactCheck.org Retrieved from https://www.factcheck.org/2018/11/bogus-voter-fraud-claims/

Farro, K. (2014). Managing the tension between open records laws and personal privacy in Ohio the wake of growing internet accessibility. Retrieved from https://ssrn.com/abstract=2467583

FBI. (2013). The crime of 'swatting.' fake 911 calls have real consequences. FBI.gov news stories. Retrieved from https://www.fbi.gov/news/stories/the-crime-of-swatting-fake-9-1-1-calls-have-real-consequences1

Fink, K. (2018). State FOI laws: More journalist-friendly, or less? In Pozen, D., & Schudson, M. (Eds.), *Troubling transparency: The history and future of Freedom of Information.* (pp. 91-115). New York, N.Y.: Columbia University Press.

Graham, D. (2016, November 28) The lasting damage from Trump's false 'voter fraud' allegations. *The Atlantic*. Retrieved from https://www.theatlantic.com/

Harper, J. (2006). *Identity crisis: How identification is overused and misunderstood*. Washington, D.C.: Cato Institute.

Haughney, C. (2013, January 6). After pinpointing gun owners, paper is a target. *The New York Times*. Retrieved from https://www.nytimes.com/

Illinois Compiled Statutes. 5 ILCS 140/1. Ch. 116.

Kansas State Statutes. §45-217.

Karras, A. (1999) The constitutionality of the Driver's Privacy Protection Act: A fork in the information access road. *Federal Communications Law Journal*, *52*(1), 125-153

Lane, F. (2007). *American privacy: The 400-year history of our most contested right*. Boston, Mass.: Beacon Press.

Levitt, J. (2007). The truth about voter fraud. *Brennan Center for Justice*. Retrieved from

https://www.brennancenter.org/sites/default/files/legacy/The%20Truth%20About%20Voter%20Fraud.pdf

Maas, K., & Levs, J. (2012, December 27). Newspaper sparks outrage for publishing names, addresses of gun permit holders. *CNN*. Retrieved from https://www.cnn.com/

McCall, G. (2018). Survey of the treatment of personal information by federal and state public records laws and by private businesses. A report compiled by the Oregon Office of Public Records Advocate. Retrieved from https://www.doj.state.or.us/wp-content/uploads/2018/12/OSC_2019-01-23_Report_from_Public_Records_Advocate.pdf

McDermott, Y. (2017). Conceptualizing the right to data protection in an era of Big Data. *Big Data & Society*, *4*(1), 1-7.

McNealy, J. (2018, May 16). What is doxxing and why is it so scary? *The Conversation*. Retrieved from http://theconversation.com/

North Dakota Office of Attorney General. (2016). Open records guide. Retrieved from https://attorneygeneral.nd.gov/sites/ag/files/documents/Open-Records-Guide.pdf

Nowell, L., Norris, J., White, D., & Moules, N. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*(1), 1-13.

Opinion: Home addresses are up for sale. Time to take back your privacy. (2018, December 16). *The New York Times.* Retrieved from https://www.nytimes.com

Reporters Committee for Freedom of the Press. (2011). Open government guide. Retrieved from https://www.rcfp.org/open-government-guide/

Reporters Committee for Freedom of the Press. (2019). Open government guide. Retrieved from https://www.rcfp.org/open-government-guide/

Rydell, M. L. (2011). Transparency in the balance: An examination of the implementation of the open meetings law in the state of South Dakota. Graduate Theses and Dissertations. Paper 12085. Retrieved from http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3101&context=etd

Schauer, F. (2018). Positive rights, negative rights, and the right to know. In Pozen, D. & Schudson, M. (Eds.), *Troubling transparency: The history and future of Freedom of Information.* (pp. 34-51). New York, N.Y.: Columbia University Press.

Shoemyer, W. (2009). Address confidentiality programs: Helping victims of abuse feel safe at home. *American Journal of Family Law*, *22*(4), 214–216.

Smith, H., Dinev, T. & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1015.

Solove, D. (2002). Access and aggregation: Privacy, public records, and the Constitution. *Minnesota Law Review*, *86*, 1137-1209.

Swanson, K. M. (2009). The right to know: An approach to gun licenses and public access to government records. *UCLA Law Review, 56*(5), 1579-1628.

Wines, M. (2016, December 18) All this talk of voter fraud? Across the U.S., officials found next to none. *The New York Times.* Retrieved from https://www.nytimes.com

Worley, D. (2014, August 30). SAFE Act: Gun permit records sealed by the thousands in N.Y. *The Journal News*. Retrieved from https://www.lohud.com

Appendix A
Home address exemptions, by record type

Always disclosable	
Balancing test	
Individual exemptions	
Always exempt	

Personnel records (* indicates a state where FOI expert verified results)	**2011**	**2019**	**Comments**
Alabama		No data	"Sensitive personnel records" are not open to public disclosure.
Alaska			2011 & 2019: 1990 FOI law amendment defined personal information, and specifically excludes names, addresses, and phone numbers from that definition, unless otherwise exempted in the law.
Arizona			2011 & 2019 - Exemptions for law enforcement and domestic violence victims.
Arkansas			2011 & 2019: As amended in 2001, the FOIA exempts "home addresses of non-elected state employees contained in employer records."
California			2011 & 2019: California has a catchall exemption that creates a balancing test between the public interest in withholding vs. disclosure. However, disclosure of home addresses was not prohibited under the state's right of privacy.
Colorado *			2011 & 2019: Personnel files, including home addresses, are specifically exempt from the act.
Connecticut *			Home addresses of various federal, state and local government employees are exempt, depending on the type of employee, including DCF, banking employees, and public safety employees.
Delaware			2011 & 2019 - Attorney General opinion allows home address to be redacted from personnel records before release.
District of Columbia			2011 & 2019: Information "of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy" is exempt from disclosure.
Florida *			2011: Home address exemptions for various officials are outlined by type, including law enforcement personnel, firefighters, judges, attorneys, employees charged with hiring or firing, code enforcement officers, guardians ad litem, probation officers, and their families. 2017 (based on 2017 Government in the Sunshine Manual): County tax collectors, domestic violence victims, hospital employees, impaired practitioner consultants, inspectors general, investigators of the Department of Business and Professional Regulation, certain Department of Health employees, and U.S. military service members added to list of exemptions.

Georgia			2011: 50-18-72 (13) Home address exemptions specified for employees of the Department of Revenue, law enforcement officers, firefighters, judges, emergency medical technicians and paramedics, scientists employed by the Division of Forensic Sciences of the Georgia Bureau of Investigation, correctional employees, prosecutors, teachers, and employees of a public school. 2019: 50-18-72 (21) Records concerning public employees that reveal the public employee's home address, except that it does not apply to public records that do not specifically identify the public employee or job.
Hawaii *			2011 & 2019: Government records, which if disclosed, would constitute a clearly unwarranted invasion of personal privacy, are exempt. As part of the "information in an agency's personnel file" is included, but not specified. (Per Civil Beat Law Center for the Public Interest:) While there may technically be a balancing test, home address information has been historically considered private.
Idaho			2011 & 2019: All personnel records of a current or former public official except employment history, salary, and workplace details.
Illinois			Private information is exempt from disclosure, including home addresses.
Indiana *			2011 & 2019: All personnel records of a current or former public official except employment history, salary, and workplace details may be exempted at the discretion of the public agency.
Iowa *			2011 & 2019: All personnel records of a current or former public official are private except for employment history, salary, and workplace details.
Kansas *			2011 & 2019: Personnel files are exempt. Information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy is exempted. Defined as "revealing information that would be highly offensive to a reasonable person, including information that may pose a risk to a person or property and is not of legitimate concern to the public."
Kentucky *			2011 & 2019: Records act exempts "records containing information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy" which has been used to redact home address information.
Louisiana			2011 & 2019: Home address and telephone number of public employees when the employee requests that they be confidential.
Maine *			2011 & 2019: A public employee's personal contact information, including home address, is confidential.
Maryland			2011 & 2019: Personal identification information, including address, is considered sociological data. If the agency has adopted rules or regulations that define sociological information, then inspection of that information shall be denied. Information that identifies an individual by an "identifying factor," including address, are exempt, except for research purposes. Home address is exempt unless the employee gives permission.
Massachusetts			2011 & 2019: A balancing test to determine if a record invades privacy (disclosing "intimate details" of a "highly personal nature"), or has a "public interest in obtaining information substantially outweighs the seriousness of any invasion of privacy." 1987 court case found name, address and pay were "payroll" records not exempt from personnel records exemption. Public Safety personnel are exempt from address disclosure.

Michigan			2011 & 2019: Specific employees exempt from address disclosure, including active or retired law enforcement officers and their families.
Minnesota			2011 & 2019: All information except salary, benefits, title, job details, and employment dates, is exempt from disclosure.
Mississippi			2011 & 2019: Home address of law enforcement officer, criminal private investigator, judge, district attorney, or spouse/child is exempt from disclosure. Other addresses should be disclosed.
Missouri			2011 & 2019: Home addresses not specifically exempt, but "individually identifiable personal records may be closed."
Montana *			2011 & 2019: Presumed open as not specifically closed in any way. Only specific personally identifying information to be redacted is SSN and birthdates. However, Supreme Court decision in 1982 exempts personnel records including information "most individuals would not willingly disclose publicly."
Nebraska			2011 & 2019: Exempts "personal information in records regarding personnel of public bodies other than salaries and routine directory information."
Nevada			2011 & 2019: Generally redacted pursuant to Donrey v. Bradshaw 1990, which found if a particular record is not specifically declared open, a balancing test must be applied, beginning with the presumption the record is public, then weighing the public's interest in the document vs. privacy or confidentiality interests asserted by the keeper of the record.
New Hampshire			2011 & 2019: The statute does not refer to personally identifying information in personnel documents, but a catchall exemption requires a balancing test to determine if personnel files would constitute an invasion of privacy. A 1974 case found names and addresses of substitute teachers were specifically public.
New Jersey			2011 & 2019: All information except for name, title, position, salary, length of service, and other job-specific details, is exempt from disclosure.
New Mexico			2011 & 2019: Presumed open because not specifically exempted. Records contained in personnel files will be publicly available to the extent they do not involve "matters of opinion" or fall under another exemption. Personally identifying information is defined as only SSN, license numbers, and birthdate.
New York			2011 & 2019: Often this type of information will be redacted from records under FOIL's invasion of privacy exemption. Releasing addresses for commercial purposes is considered an invasion of privacy under the definition. Also, information of a personal nature that is not relevant to the ordinary work of the agency.
North Carolina			2011 & 2019: Exempt, except for specific records dealing with name, age, date of employment, contract, position, title, salary, promotions, and other work related details.
North Dakota			2011 & 2019: Personal information in a personnel record is exempt from disclosure. The definition includes home address.
Ohio			2011 & 2019: Court interpretations have held federal right to privacy bars release of some personally identifying information to some kinds of requesters. Home addresses of law enforcement, emergency responders, court employees, and youth services employees - and their families - are exempt, but a journalist may request the information if it is in the public interest.

Oklahoma			2011 & 2019: Home address, telephone number, and SSN of any current or former employee shall be kept confidential.
Oregon*			2011 & 2019: 2011 & 2019: ORS 192.355(3) Exempts public body employee or volunteer residential addresses.
Pennsylvania *			2011: Home addresses of law enforcement officers or judges are specifically exempt. Private employees of organizations contracting with government agency may be redacted. 2019: (Per Pennsylvania Freedom of Information Coalition): Home addresses of law enforcement officers or judges as well as minors under age 17 are specifically exempt. Private employees of organizations contracting with government agency may be redacted. Due to a Supreme Court ruling, home addresses are generally exempt under privacy guarantees in the Constitution, unless a stronger public interest would be served by their release.
Rhode Island			2011 & 2019: Only information related to the employment, including city or town of residence, but not the specific address, can be released.
South Carolina			2011 & 2019: The exemptions for "unreasonable invasion of personal privacy" only specify home address for people with disabilities and for commercial uses, so a determination would need to be made before releasing an employee's address to the public.
South Dakota			2011 & 2019: Confidential other than salaries and routine directory information.
Tennessee			2011: Generally open, but not Social Security Numbers. 2019: Court interpretations have gone back and forth. 2013 case ruled residential addresses of third party contractors was public. 2017 case ruled all residential addresses were confidential information. Legislature later amended the code to eliminate addresses from category of protected information. TCA 10-7-504(f) - Telephone numbers, residential addresses, Social Security Numbers, bank account numbers, and driver's license information of public employees or their immediate family members is exempt from disclosure.
Texas			2011 & 2019: Information revealing home addresses, home telephone numbers, and SSN of current or former governmental officials and employees, as well as certain peace and security officers, is protected.
Utah			2011 & 2019: Records concerning a current or former employee of, or applicant for employment with, a government entity "that would disclose the individual's home address, home telephone number, Social Security number, insurance coverage, marital status, or payroll deductions" are exempt.
Vermont			2011 & 2019: Personal documents are exempt. Defined as information relating to "personal finances, medical, or psychological facts" or that "reveal intimate details of a person's life, including any information that might subject that person to embarrassment, harassment, disgrace, or loss of employment or friends."
Virginia *			2011 & 2019: Personnel records containing identifiable individuals are excluded. State statutes define "personal contact information" as including home address or telephone number. The exemption is discretionary, so a government may choose to release a file or some part of a file. (Virginia Coalition for Open Government)

Washington *			2011 & 2019: Residential addresses, telephone numbers, wireless numbers, personal e-mail addresses, SSN, and emergency contact information of employees or volunteers of a public agency are exempt from disclosure.
West Virginia			2011: Facts – such as an individual's name and residential address – which "are not 'personal' or 'private' facts but are public in nature in that the constitute information normally shared with strangers and are ascertainable by reference to publicly obtainable books and records" are disclosable without a balancing test. 2019: Under the Public Records Management and Preservation Act, personal information of state officers, employees, and retirees – including home addresses – is confidential.
Wisconsin		No data	2011: Certain employee personnel records, including home address, is exempt.
Wyoming			2011 & 2019: Personnel files are closed, except for qualifications for employment and salary.

Firearms permits (* indicates a state where FOI expert verified results)	**2011**	**2019**	**Comments**
Alabama		No data	2011: Presumably open, as copies of pistol permits are public records.
Alaska			2011 & 2019: The list of concealed handgun permittees, and all applications, are not public records.
Arizona			2011 & 2019: Information and records maintained by the Department of Public Safety on applicants for a concealed weapon permit "shall not be available to any other person or entity except on an order from a state or federal court."
Arkansas			2011 & 2019: Records are exempt from FOIA, except the name and zip code for licensee may be released upon request by a citizen of Arkansas.
California			2011 & 2019: While firearms licenses are public, the home address of peace officers, judges, court commissioners, and magistrates are exempt from release.
Colorado *	N/A	N/A	2011 & 2019: Colorado does not require firearms to be registered, and prohibits law enforcement from maintaining a list of people who buy or sell or transfer firearms. (per Colorado Freedom of Information Coalition)
Connecticut *			2011 & 2019: Names and addresses of people with permits to carry pistols and revolvers are exempt from FOIA.
Delaware			2011 & 2019: Any records that disclose the identity or address of any person holding a permit to carry a concealed deadly weapon are exempt.
District of Columbia			2011 & 2019: Privacy exemption may apply. 1993 case refused to release names and addresses of gun owners on privacy grounds.
Florida *			2011 & 2019: Personal identifying information of an individual who has applied for or received a license to carry a concealed weapon is confidential and exempt from disclosure.
Georgia			2011 & 2019: The FOI act does not apply to weapons carry licenses.

Hawaii *			2011 & 2019: Firearm permit information that identifies an individual permit by name or address is exempt.
Idaho			2011 & 2019: Presumed open. "Once a permit is issued, it is open to the public."
Illinois			2011 & 2019: Private information is exempt from disclosure, and includes home addresses. Gun permits are also closed.
Indiana *			2011 & 2019: Applications for gun permits and permits are confidential, except for law enforcement personnel seeking to determine the validity of a license to carry a handgun, or to persons conducting journalistic or academic work, but only if all personal identifying information is redacted.
Iowa *			2011: Presumed open. "There is no specific statutory provision covering gun permits and there are no reported cases." 2019: A 2017 law was passed, requiring the commissioner of public safety "shall keep confidential personally identifiable information of holders of professional and nonprofessional permits to carry weapons and permits to acquire pistols or revolvers…"
Kansas *			2011: Presumed open. "No applicable law." 2019: Records related to persons licensed to carry concealed handguns are confidential and may not be disclosed.
Kentucky *			2011: While a list of names of every individual in Kentucky licensed to carry a firearm is open to public to inspect in hard copy, it can contain no other identifying information other than names. 2019: Information concerning individuals licensed in Kentucky to carry a concealed firearm is generally closed from the public.
Louisiana			2011: Presumed open. No specific exemption in the law. 2019: Information in an application for a concealed handgun permit is exempt from disclosure.
Maine *			2011 & 2019: While the applications to carry concealed firearms are confidential, the actual permits are considered public record. However, only the municipality of residence, date of issuance, and expiration date are public.
Maryland			2011: Presumed open. No statutory or case law addressing the issue. 2019: A custodian shall deny inspection of records of a person authorized to sell, purchase, rent, or transfer regulated firearms or to carry, wear, or transport a handgun.
Massachusetts			2011 & 2019: Names and addresses exempt from disclosure on applications, permits and sales or transfers.
Michigan			2011 & 2019: Courts have ruled the names and addresses of persons who owned registered handguns should be exempt under the law's privacy exemption.
Minnesota			2011 & 2019: All data pertaining to the purchase or transfer of firearms and applications for permits to carry firearms, which are collected by state agencies, political subdivisions, or statewide systems, are classified as private.
Mississippi			2011 & 2019: Addresses presumed public, as no specific exemption exists. However, permits are closed for 45 days after issuance or denial.
Missouri			2011 & 2019: Records of permits are closed to the public.

Montana *			2011 & 2019: Open unless the demands of individual privacy clearly exceed the merits of public disclosure.
Nebraska			2011 & 2019: Information concerning the applicant or permitholder is not public.
Nevada			2011 & 2019: The Nevada Supreme Court held firearms permits are public, even though applications are not. However, if otherwise confidential information is included in the permit, that can be redacted. Confidential information is defined in state statutes, not cross listed with the act.
New Hampshire			2011 & 2019: Gun permits not specifically addressed, but New Hampshire has a catch-all exemption that could be used to withhold "confidential, commercial or financial information."
New Jersey			2011: The licenses/permits are public records, but they are not open to inspection. They are exempt from disclosure by attorney general regulations. 2019: More specifically exempt. Government record should not include any personal firearms record, including names, address, SSN, phone number, e-mail, social media address, or driver's license number.
New Mexico*			2011 & 2019: Permits are exempted from the general right to inspect public records.
New York			2011 & 2019: According to the express terms of N.Y. Penal Law 400.00(5), "the name and address of any person" who has been granted a pistol permit license "shall be a public record." This was backed up by 1998 case, and affirmed in a 1999 case.
North Carolina*			2011: Address presumed public as "permits for handguns and other weapons issued by sheriffs … are public records." 2019: In 2014, the North Carolina General Assembly enacted legislation to make information provided in applying for a concealed handgun permit and the names of people obtaining permits from sheriff's offices no longer public.
North Dakota			2011 & 2019: Information collected from an applicant for a license to carry a firearm or dangerous weapon concealed is confidential.
Ohio			2011 & 2019: Records related to license to carry concealed handgun are not public records.
Oklahoma			2011: Not mentioned in the report, so presumed open. 2019: The Oklahoma State Bureau of Investigation maintains a list of all persons issued a handgun license under the Oklahoma Self-Defense Act, but the list is available only to law enforcement agencies.
Oregon			2011: Oregon's appellate court has held that records of concealed handgun licenses are public records, and that exceptions for personal privacy do not generally apply. 2019: In 2012, the Oregon Legislature passed what is now ORS 192.374, which expressly prohibits disclosure of records or information identifying holders of concealed handgun licenses, except in certain circumstances.
Pennsylvania			2011: While the act does not specifically address gun permits, they are presume public, with certain personal information redacted. Addresses were specifically exempt from disclosure under previous versions of the FOI act. 2019: (Per Pennsylvania Freedom of Information Coalition): All information regarding firearms applications and permits, including addresses, are exempt from public disclosure under PA Title 37 chapter 33 section 33.103.

Rhode Island			2011 & 2019: Gun permit records are public, but all exempt portions must be redacted. What those portions are, is not specified, and would therefore require interpretation.
South Carolina			2011 & 2019: A list of persons with permits to carry concealed weapons may only be released to law enforcement or in response to a court order.
South Dakota			2011 & 2019: State law is designed to prevent release of information concerning those licensed to owning a firearm or carrying a concealed pistol.
Tennessee			2011: There is no restriction on public access to gun permits, although certain information in the application for the permit might be kept confidential by other provisions of the law. 2019: Information in an application for a handgun permit are confidential.
Texas			2011: Addresses presumed open because gun permits are not specifically addressed in the law. 2019: Information on individuals licensed to carry concealed handguns is confidential and not subject to requests under the act.
Utah			2011 & 2019: Names, addresses, telephone numbers, dates of birth, and SSN are classified as protected records.
Vermont		N/A	2011: Addresses presumed open, as gun permits are not specifically addressed in the law. 2019: Gun permits are not required in Vermont, so no such records exist.
Virginia *			2011: Information from the concealed carry permit database should be limited to law-enforcement personnel for investigative purposes. Always individually disclosable at courthouses. 2019: In 2013, the legislature prohibited release of the permit information at courthouses. (Virginia Coalition for Open Government) The Department of State Police receive all orders issuing concealed handgun permits, but the information is withheld from public disclosure.
Washington *			2011 & 2019: License applications for concealed pistols are exempt from public disclosure.
West Virginia		N/A	2011: Addresses presumed public, as there is no provision in state law exempting information from the licenses. 2019: In 2015, the state legislature amended FOIA to exempt gun license application information. But then in 2016, the legislature removed requirements to have a permit to carry a hidden firearm, so the exemption is moot.
Wisconsin *		No data	2011: Concealed carry license records are not public except in the context of a prosecution.
Wyoming			2011 & 2019: Concealed carry permits are confidential.

Voter registration (* indicates a state where FOI expert verified results)	**2011**	**2019**	**Comments**
Alabama		No data	2011: While the list of names and precincts are open, home address is not.

Alaska			2011 & 2019: Individual voters may request their home address be kept confidential.
Arizona			2011 & 2019: Certain public officials and victims of domestic violence can prevent the public from accessing their residential address, telephone number, and precinct.
Arkansas			2011 & 2019: Voter registration lists are open.
California			2011 & 2019: Personal information, including home address, may be disclosed to "any person for election, scholarly, journalistic or political purposes, or for governmental purposes."
Colorado *			2011 & 2019: While voter registration records are public, any person may request that the home address be exempt from public disclosure.
Connecticut *			2011: Addresses presumed open because preliminary and final voter registry lists are available for public use.
Delaware			2011 & 2019: Addresses presumed open because not specified in the law.
District of Columbia			2011 & 2019: Addresses presumed open because not specified in the law.
Florida *			2011 & 2019: Although citizens may examine the registration books, copying of such books is prohibited.
Georgia			2011 & 2019: Voter registration lists are subject to the act's disclosure requirements. Place where person registered to vote is exempt, but home address is not exempt.
Hawaii *			2011 & 2019: A voter's full name, district, and status are open to the public. All other information, including the voter's address, is confidential except for "election or government purposes."
Idaho			2011: Upon a showing of good cause, a voter's physical residence address may be exempt from the voter registration database. 2019: Upon showing of a good cause by the voter to the county clerk in consultation with the county prosecuting attorney, the physical residence address of the voter may be exempt. "Good cause" shall include protection of life and property and protection of victims of domestic violence and similar crimes.
Illinois			2011 & 2019: While voter registration databases are considered open, private information is exempt from disclosure, including home addresses.
Indiana *			2011 & 2019: Presumed open.
Iowa *			2011 & 2019: May only be used for voter registration purposes.
Kansas *			2011 & 2019: Voter registration records are public. Voter registration lists is one of the items specifically outlined as available for release even for commercial purposes.
Kentucky *			2011: May be closed to some requesters under Ky. Rev. Stat. 61.878(1)(1), which exempts records made confidential by an enactment of the General Assembly, but available to media using the records for "publication, broadcast or related use." 2019: Ky. Rev. Stat. 116.095 provides that "[t]he county clerk shall permit any citizen, at all reasonable hours, to inspect or make copies of any [voter] registration record, without a fee. He or she shall, upon request, furnish to any citizen a copy of the registration records, for which he or she may charge necessary duplicating costs not to exceed fifty cents per page."

Louisiana			2011 & 2019: Voter registration records are subject to the Act, except for the "name and address of a law enforcement officer in the custody of the registrar of voters or the secretary of state, if certified by the law enforcement agency employing the officer that the officer is engaging in hazardous activities to the extent that it is necessary for his name and address to be kept confidential."
Maine *			2011 & 2019: Voter registration information does not include those who enroll in the Address Confidentiality Program.
Maryland			2011 & 2019: Addresses presumed open because no specific mention in the law.
Massachusetts			2011 & 2019: While the Central Voter Registry is open to the public, the names and addresses listed therein are not public records and are only open to statewide committees.
Michigan *Needs clarification*			2011: Voter registration records were exempt from disclosure under Mich. Comp. Laws 168.495a(2) 2019: Not addressed in act, but Michigan Election Law 168.509ff seems to say they are public.
Minnesota			2011 & 2019: A public information list of voter registration records may be made available to the public.
Mississippi			2011 & 2019: Addresses public. Voter registration records are open except for SSN, phone numbers, age, and date of birth.
Missouri			2011 & 2019: Voter registration records are open, but cannot be used for commercial purposes.
Montana *			2011 & 2019: All records pertaining to voter registration and elections are public.
Nebraska			2011 & 2019: Voter registration records are available for inspection, but may not be copied. A list of registered voters minus personal identification information is available for sale by the Secretary of State.
Nevada			2011 & 2019: Addresses presumed open as there is no specific exemption listed.
New Hampshire			2011 & 2019: Addresses presumed open as there is no specific exemption listed.
New Jersey			2011 & 2019: Victims of domestic violence or stalking can omit their home addresses from voter registration.
New Mexico			2011 & 2019: Voter registration lists are public. Only SSN, agency where voter registered, birthdates, and telephone numbers are exempt.
New York			2011 & 2019: Presumed open because not specifically exempt. 1984 state Supreme Court case granted access to computer tapes with voter telephone numbers and voter histories.
North Carolina			2011 & 2019: Individual voter registration information is public except for SSN, birthdates, driver's license numbers, and agency where voter registered.
North Dakota			2011 & 2019: Though North Dakota does not have voter registration, a central voter file and voter list are both public, except for the voter's birthdate and state identification number. Records for people with restraining or protective orders are protected and not disclosable.

Ohio			2011 & 2019: Voter registration records, including home addresses, are public.
Oklahoma			2011: Voter registration records may be obtained for a fee. 2019: Voter registration records may be obtained for a fee. The state election board may promulgate rules to keep confidential the residence and mailing address of voters who are members of certain classes, including judges, district attorneys, and persons protected by victim's protective orders.
Oregon			2011: The residence address of an elector where a showing of a reasonable threat to personal safety is present is exempt from release. Also exempt: public safety officers.
Pennsylvania *			2011: Records of the voter registration commission are open to public inspection and copying. 2019: (Per Pennsylvania Freedom of Information Coalition): Records of the voter registration commission are open to public inspection and copying, including addresses. Social Security numbers are exempt from disclosure. One must sign an affidavit that voter registration information will only be used for political or other related purposes.
Rhode Island			2011: Voter registration records are public, but nothing contained in them shall indicate the particular place at which the voter was registered. 2019: Presumably open. No specific exemption.
South Carolina			2011 & 2019: Official registration records are public records subject to inspection of any citizen at all times.
South Dakota			2011 & 2019: Voter registration records are open.
Tennessee			2011 & 2019: Voter registration records are open.
Texas			2011 & 2019: Applications to register to vote on file with a county registrar are public.
Utah			2011: Voter registration records, including a person's voting history, are public except for those parts "identifying a voter's driver license or ID card number." 2019: Adds e-mail address and date of birth to exempt details.
Vermont			2011: Records of a registered voter's birthdate, driver's license number, SSN, and street address are exempt. 2019: Telephone number and e-mail address now listed, but home address no longer on the list.
Virginia *			2011 & 2019: Voter registration documents are covered by state Election Code, which says they are open to inspection by the public. If voter has provided a P.O. box address instead of home address, there is a prohibition against releasing home address from record. (per Virginia Coalition for Open Government)
Washington *			2011 & 2019: The voter registration list, including addresses, is available for download from the Secretary of State website, but cannot be used for commercial purposes. The state has a voter address confidentiality program for some crime victims. (per Washington Coalition for Open Government)
West Virginia			2011 & 2019: While there are no cases construing FOIA in the context of voter registration records, such records have been routinely made available to the public upon request.

Wisconsin *		No data	2011: Addresses presumed open as election records are open to public inspection.
Wyoming			2011 & 2019: While some personally identifying information is confidential, names, gender, and addresses are not exempt.

Appendix B
Home address exemptions, by state

(* indicates a state where FOI expert verified results)

Always disclosable	
Balancing test	
Individual exemptions	
Always exempt	

Alabama	**2011**	**2019**	**Comments**
Personnel files		No data	"Sensitive personnel records" are not open to public disclosure.
Firearms applications and permits		No data	2011: Presumably open, as copies of pistol permits are public records.
Voter registration documents		No data	2011: While the list of names and precincts are open, home address is not.

Alaska	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: 1990 FOI law amendment defined personal information, and specifically excludes names, addresses, and phone numbers from that definition, unless otherwise exempted in the law.
Firearms applications and permits			2011 & 2019: The list of concealed handgun permittees, and all applications, are not public records.
Voter registration documents			2011 & 2019: Individual voters may request their residential address be kept confidential.

Arizona	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019 - Individual exemptions for law enforcement/public safety and domestic violence victims.
Firearms applications and permits			2011 & 2019: Information and records maintained by the Department of Public Safety on applicants for a concealed weapon permit "shall not be available to any other person or entity except on an order from a state or federal court."
Voter registration documents			2011 & 2019: Certain public officials and victims of domestic violence can prevent the general public from accessing their residential address, telephone number, and voting precinct.

Arkansas	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: As amended in 2001, the FOIA exempts "home addresses of non-elected state employees contained in employer records."
Firearms applications and permits			2019: Records are exempt from FOIA, except the name and zip code for licensee may be released upon request by a citizen of Arkansas.
Voter registration documents			2019: Voter registration lists are open.

California	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: California has a catchall exemption that creates a balancing test between the public interest in withholding vs. disclosure. However, disclosure of home addresses was not prohibited under the state's right of privacy.
Firearms applications and permits			2011 & 2019: While firearms licenses are public, the home address of peace officers, judges, court commissioners, and magistrates are exempt from release.
Voter registration documents			2011 & 2019: Personal information, including home address, may be disclosed to "any person for election, scholarly, journalistic, or political purposes, or for governmental purposes."

Colorado *	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Personnel files, including home addresses, are specifically exempt from the act.
Firearms applications and permits	N/A	N/A	2011 & 2019: Colorado does not require firearms to be registered, and prohibits law enforcement from maintaining a list of people who buy, sell, or transfer firearms. (per Colorado Freedom of Information Coalition)
Voter registration documents			2011 & 2019: While voter registration records are public, any person may request that the home address be exempt from public disclosure.

Connecticut*	**2011**	**2019**	**Comments**
Personnel files			Home addresses of various federal, state, and local government employees are exempt, depending on the type of employee, including DCF, banking employees, and public safety employees.
Firearms applications and permits			2011 & 2019: Names and addresses of people with permits to carry pistols and revolvers are exempt from FOIA.
Voter registration documents			2011: Addresses presumed open because preliminary and final voter registry lists are available for public use.

Delaware	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019 - Attorney General opinion allows home address to be redacted from personnel records before release.
Firearms applications and permits			2011 & 2019: Any records which disclose the identity or address of any person holding a permit to carry a concealed deadly weapon are exempt.
Voter registration documents			2011 & 2019: Addresses presumed open because not specified in the law.

District of Columbia	**2011**	**2019**	**Comments**
Personnel files			Information "of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy" is exempt from disclosure.
Firearms applications and permits			2011 & 2019: Privacy exemption may apply. 1993 case refused to release names and addresses of gun owners on privacy grounds.
Voter registration documents			2011 & 2019: Addresses presumed open because not specified in the law.

Florida *	**2011**	**2019**	**Comments**
Personnel files			2011: Home address exemptions for various officials are outlined by type, including law enforcement personnel, firefighters, judges, attorneys, employees charged with hiring or firing, code enforcement officers, guardians ad litem, probation officers, and their families. 2017 (based on 2017 Government in the Sunshine Manual): County tax collectors, domestic violence victims, hospital employees, impaired practitioner consultants, inspectors general, investigators of the Department of Business and Professional Regulation, certain Department of Health employees, and U.S. military service members added to list of exemptions.
Firearms applications and permits			2011 & 2019: Personal identifying information of an individual who has applied for or received a license to carry a concealed weapon is confidential and exempt from disclosure.
Voter registration documents			2011 & 2019: Although citizens may examine the registration books, copying of such books is prohibited.

Georgia	**2011**	**2019**	**Comments**
Personnel files			2011: 50-18-72 (13) Home address exemptions specified for employees of the Department of Revenue, law enforcement officers, firefighters, judges, emergency medical technicians and paramedics, scientists employed by the Division of Forensic Sciences of the Georgia Bureau of Investigation, correctional employees, prosecutors, teachers, and employees of a public school. 2019: 50-18-72 (21) Records concerning public employees that reveal the public employee's home address… except that it does not apply to public records that do not specifically identify the public employee or job.
Firearms applications and permits			2011 & 2019: The FOI act does not apply to weapons carry licenses.
Voter registration documents			2011 & 2019: Voter registration lists are subject to the act's disclosure requirements. Place where person registered to vote is exempt, but home address is not specifically exempt.

Hawaii *	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Government records, which if disclosed, would constitute a clearly unwarranted invasion of personal privacy, are exempt. "Information in an agency's personnel file" is included in the list of information where a person may have a significant privacy interest, but home address is not specified. (Per Civil Beat Law Center for the Public Interest:) While there may technically be a balancing test, home address information has been historically considered private.
Firearms applications and permits			2011 & 2019: Firearm permit information that identifies an individual permit by name or address is exempt.
Voter registration documents			2011 & 2019: A voter's full name, district, and status are open to the public. All other information, including the voter's address, is confidential except for "election or government purposes."

Idaho	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: All personnel records of a current or former public official except employment history, salary, and workplace details.
Firearms applications and permits			2011 & 2019: Presumed open. "Once a permit is issued, it is open to the public."
Voter registration documents			2011: Upon a showing of good cause, a voter's physical residence address may be exempt from the voter registration database. 2019: Upon showing of a good cause by the voter to the county clerk in consultation with the county prosecuting attorney, the physical residence address of the voter may be exempt. "Good cause" shall include protection of life and property and protection of victims of domestic violence and similar crimes.

Illinois	**2011**	**2019**	**Comments**
Personnel files			Private information is exempt from disclosure, and includes home addresses.
Firearms applications and permits			2011 & 2019: Private information is exempt from disclosure, and includes home addresses. Gun permits are also closed.
Voter registration documents			2011 & 2019: While voter registration databases are considered open, private information is exempt from disclosure, and includes home addresses.

Indiana *	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: All personnel records of a current or former public official except employment history, salary, and workplace details may be exempted at the discretion of the public agency.
Firearms applications and permits			2011 & 2019: Applications for gun permits and permits are confidential, except for law enforcement personnel seeking to determine the validity of a license to carry a handgun, or to persons conducting journalistic or academic work, but only if all personal identifying information is redacted.
Voter registration documents			2011 & 2019: Presumed open.

Iowa *	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: All personnel records of a current or former public official are private except for employment history, salary, and workplace details.
Firearms applications and permits			2011: Presumed open. “There is no specific statutory provision covering gun permits and there are no reported cases.” 2019: A 2017 law was passed, requiring the commissioner of public safety “shall keep confidential personally identifiable information of holders of professional and nonprofessional permits to carry weapons and permits to acquire pistols or revolvers…”
Voter registration documents			2011 & 2019: May only be used for voter registration purposes.

Kansas *	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Personnel files are exempt. Information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy is exempted. Defined as "revealing information that would be highly offensive to a reasonable person, including information that may pose a risk to a person or property and is not of legitimate concern to the public."
Firearms applications and permits			2011: Presumed open. "No applicable law." 2019: Records related to persons licensed to carry concealed handguns are confidential and may not be disclosed.
Voter registration documents			2011 & 2019: Voter registration records are public records. Voter registration lists is one of the items specifically outlined as available for release even for commercial purposes.

Kentucky *	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Records act exempts "records containing information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy" which has been used to redact home address information.
Firearms applications and permits			2011: While a list of names of every individual in Kentucky licensed to carry a firearm is open to public to inspect in hard copy, it can contain no other identifying information other than names. 2019: Information concerning individuals licensed in Kentucky to carry a concealed firearm is generally closed from the public.
Voter registration documents			2011: May be closed to some requesters under Ky. Rev. Stat. 61.878(1)(1), which exempts records made confidential by an enactment of the General Assembly, but appear to be available to media using the records as part of a "publication, broadcast or related use." 2019: Ky. Rev. Stat. 116.095 provides that "[t]he county clerk shall permit any citizen, at all reasonable hours, to inspect or make copies of any [voter] registration record, without a fee. He or she shall, upon request, furnish to any citizen a copy of the registration records, for which he or she may charge necessary duplicating costs not to exceed fifty cents per page."

Louisiana	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Home address and telephone number of public employees are exempt when the employee requests that they be confidential.
Firearms applications and permits			2011: Presumed open. No specific exemption in the law. 2019: Information in an application for a concealed handgun permit is exempt from disclosure.
Voter registration documents			2011 & 2019: Voter registration records are subject to the Act, except for the "name and address of a law enforcement officer in the custody of the registrar of voters or the secretary of state, if certified by the law enforcement agency employing the officer that the officer is engaging in hazardous activities to the extent that it is necessary for his name and address to be kept confidential."

Maine *	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: A public employee's personal contact information, including home address, is confidential.
Firearms applications and permits			2011 & 2019: While the applications to carry concealed firearms are confidential, the actual permits are considered public record. However, only the municipality of residence, date of issuance, and expiration date are public.
Voter registration documents			2011 & 2019: Voter registration information does not include those who enroll in the Address Confidentiality Program.

Maryland	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Personal identification information, including address, is considered sociological data. If the agency has adopted rules or regulations that define sociological information, then inspection of that information shall be denied. Information that identifies an individual by an "identifying factor," including address, are exempt, except for research purposes. Home address is exempt, unless the employee gives permission for the inspection.
Firearms applications and permits			2011: Presumed open. No statutory or case law addressing the issue. 2019: A custodian shall deny inspection of records of a person authorized to sell, purchase, rent, or transfer regulated firearms or to carry, wear, or transport a handgun.
Voter registration documents			2011 & 2019: Addresses presumed open because no specific mention in the law.

Massachusetts	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: A balancing test to determine if a record invades privacy (disclosing "intimate details" of a "highly personal nature"), or has a "public interest in obtaining information substantially outweighs the seriousness of any invasion of privacy." 1987 court case found name, address, and pay were "payroll" records not exempt from personnel records exemption. Public safety personnel are exempt from address disclosure.
Firearms applications and permits			2011 & 2019: Names and addresses exempt from disclosure on applications, permits, sales, or transfers.
Voter registration documents			2011 & 2019: While the Central Voter Registry is open to the public, the names and addresses listed therein are not public records and are only open to statewide committees.

Michigan	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Specific employees exempt from address disclosure, including active or retired law enforcement officers and their families.
Firearms applications and permits			2011 & 2019: Courts have ruled the names and addresses of persons who owned registered handguns should be exempt under the law's privacy exemption.
Voter registration documents			2011: Voter registration records were exempt from disclosure under Mich. Comp. Laws 168.495a(2) 2019: Not addressed in act, but Michigan Election Law 168.509ff seems to say they are public.

Minnesota	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: All information except salary, benefits, title, job details, and employment dates, is exempt from disclosure.
Firearms applications and permits			2011 & 2019: All data pertaining to the purchase or transfer of firearms and applications for permits to carry firearms are classified as private.
Voter registration documents			2011 & 2019: A public information list of voter registration records may be made available to the public.

Mississippi	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Home address of law enforcement officer, criminal private investigator, judge, district attorney, or spouse/child is exempt from disclosure. Other addresses should be disclosed.
Firearms applications and permits			2011 & 2019: Addresses presumed public, as no specific exemption exists. However, permits are closed for 45 days after issuance or denial.
Voter registration documents			2011 & 2019: Addresses public. Voter registration records are open except for SSN, phone numbers, age, and date of birth.

Missouri	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Home addresses not specifically exempt, but "individually identifiable personal records may be closed."
Firearms applications and permits			2011 & 2019: Records of permits are closed to the public.
Voter registration documents			2011 & 2019: Voter registration records are open, but cannot be used for commercial purposes.

Montana *	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Presumed open as not specifically closed in any way. Only specific personally identifying information to be redacted is SSN and birthdates. However, Supreme Court decision in 1982 exempts personnel records including information "most individuals would not willingly disclose publicly."
Firearms applications and permits			2011 & 2019: Open unless the demands of individual privacy clearly exceed the merits of public disclosure.
Voter registration documents			2011 & 2019: All records pertaining to voter registration and elections are public.

Nebraska	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Exempts "personal information in records regarding personnel of public bodies other than salaries and routine directory information."
Firearms applications and permits			2011 & 2019: Information concerning the applicant or permitholder is not a public record.
Voter registration documents			2011 & 2019: Voter registration records are available for inspection, but may not be copied. A list of registered voters minus personal identification information is available for sale by the Secretary of State.

Nevada	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Generally redacted pursuant to Donrey v. Bradshaw 1990, which found if a particular record is not specifically declared open, a balancing test must be applied, beginning with the presumption the record is public, then weighing the public's interest in the document vs. privacy or confidentiality interests asserted by the keeper of the record.
Firearms applications and permits			2011 & 2019: The Nevada Supreme Court held firearms permits are public, even though applications are not. However, if otherwise confidential information is included in the permit, that can be redacted. Confidential information is defined in state statutes, not cross listed with the act.
Voter registration documents			2011 & 2019: Addresses presumed open as there is no specific exemption listed.

New Hampshire	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: The statute does not refer to personally identifying information in personnel documents, but a catchall exemption requires a balancing test to determine if personnel files would constitute an invasion of privacy. A 1974 case found names and addresses of substitute teachers was specifically public.
Firearms applications and permits			2011 & 2019: Gun permits not specifically addressed, but New Hampshire has a catch-all exemption that could be used to withhold "confidential, commercial or financial information."
Voter registration documents			2011 & 2019: Addresses presumed open as there is no specific exemption listed.

New Jersey	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: All information except for name, title, position, salary, length of service, and other job-specific details, is exempt from disclosure.
Firearms applications and permits			2011: The licenses/permits are public records, but they are not open to inspection. They are exempt from disclosure by attorney general regulations. 2019: More specifically exempt. Government record should not include any personal firearms record, including names, address, SSN, phone number, e-mail, social media address, or driver's license number.
Voter registration documents			2011 & 2019: Victims of domestic violence or stalking can omit their home addresses from voter registration.

New Mexico*	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Presumed open because not specifically exempted. Records contained in personnel files will be publicly available to the extent they do not involve "matters of opinion" or fall under another exemption. Personally identifying information is defined as only SSN, license numbers, and birthdate.
Firearms applications and permits			2011 & 2019: Permits are exempted from the general right to inspect public records.
Voter registration documents			2011 & 2019: Voter registration lists are public. Only SSN, agency where voter registered, birthdates, and telephone numbers are exempt.

New York	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Often this type of information will be redacted from records under FOIL's invasion of privacy exemption. Releasing addresses for commercial purposes is considered an invasion of privacy under the definition. Also, information of a personal nature that is not relevant to the ordinary work of the agency.
Firearms applications and permits			2011 & 2019: According to the express terms of N.Y. Penal Law 400.00(5), "the name and address of any person" who has been granted a pistol permit license "shall be a public record." This was backed up by 1998 case, and affirmed in a 1999 case.
Voter registration documents			2011 & 2019: Presumed open because not specifically exempt. 1984 state Supreme Court case granted access to computer tapes with voter telephone numbers and voter histories.

North Carolina*	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Exempt, except for specific records dealing with name, age, date of employment, contract, position, title, salary, promotions, and other work-related details.
Firearms applications and permits			2011: Address presumed public as "permits for handguns and other weapons issued by sheriffs … are public records." 2019: In 2014, the North Carolina General Assembly enacted legislation to make information provided in applying for a concealed handgun permit and the names of people obtaining permits from sheriff's offices no longer public.
Voter registration documents			2011 & 2019: Individual voter registration information is public except for SSN, birthdates, driver's license numbers, and agency where voter registered.

North Dakota	**2011**	**2019**	**Comments**
Personnel files		No data	2011: Personal information in a personnel record is exempt from disclosure. The definition includes home address.
Firearms applications and permits		No data	2011: Information collected from an applicant for a license to carry a firearm or dangerous weapon concealed is confidential.
Voter registration documents		No data	2011: Though North Dakota does not have voter registration, a central voter file and voter list are both public, except for the voter's birthdate and state identification number.

Ohio	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Court interpretations have held federal right to privacy bars release of some personally identifying information to some kinds of requesters. Home addresses of law enforcement, emergency responders, court employees, and youth services employees – and their families – are exempt, but a journalist may request the information if it is in the public interest.
Firearms applications and permits			2011 & 2019: Records related to license to carry concealed handgun are not public records.
Voter registration documents			2011 & 2019: Voter registration records, including home addresses, are public.

Oklahoma	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Home address, telephone number, and SSN of any current or former employee shall be kept confidential.
Firearms applications and permits			2011: Not mentioned in the report, so presumed open. 2019: The Oklahoma State Bureau of Investigation maintains a list of all persons issued a handgun license under the Oklahoma Self-Defense Act, but the list is available only to law enforcement agencies.
Voter registration documents			2011: Voter registration records may be obtained for a fee. 2019: Voter registration records may be obtained for a fee. The state election board may promulgate rules to keep confidential the residence and mailing address of voters who are members of certain classes, including judges, district attorneys, and persons protected by victim's protective orders.

Oregon*	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: ORS 192.355(3) Exempts public body employee or volunteer residential addresses.
Firearms applications and permits			2011: Oregon's appellate court has held that records of concealed handgun licenses are public records, and that exceptions for personal privacy do not generally apply. 2019: In 2012, the Oregon Legislature passed what is now ORS 192.374, which expressly prohibits disclosure of records or information identifying holders of concealed handgun licenses, except in certain circumstances.
Voter registration documents			2011: The residence address of an elector where a showing of a reasonable threat to personal safety is present is exempt from release. Also exempt: public safety officers

Pennsylvania *	**2011**	**2019**	**Comments**
Personnel files			2011: Home addresses of law enforcement officers or judges are specifically exempt. Private employees of organization contracting with government agency may be redacted. 2019: (Per Pennsylvania Freedom of Information Coalition): Home addresses of law enforcement officers or judges, as well as minors under age 17, are specifically exempt. Private employees of organizations contracting with government agency may be redacted. Due to a Supreme Court ruling, home addresses are generally exempt under privacy guarantees in the Constitution, unless a stronger public interest would be served by their release.
Firearms applications and permits			2011: While the act does not specifically address gun permits, they are presumed public, with certain personal information redacted. Addresses were exempt from disclosure under previous versions of the FOI act. 2019: (Per Pennsylvania Freedom of Information Coalition): All information regarding firearms applications and permits, including addresses, are exempt from public disclosure under PA Title 37 chapter 33 section 33.103.
Voter registration documents			2011: Records of the voter registration commission are open to public inspection and copying. 2019: (Per Pennsylvania Freedom of Information Coalition): Records of the voter registration commission are open to public inspection and copying, including addresses. Social Security numbers are exempt from disclosure. One must sign an affidavit that voter registration information will only be used for political or other related purposes.

Rhode Island	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Only information related to the employment, including city or town of residence, but not the specific address, can be released.
Firearms applications and permits			2011 & 2019: Gun permit records are public, but all exempt portions must be redacted. What those portions are, is not specified, and would therefore require interpretation.
Voter registration documents			2011: Voter registration records are public, but nothing contained in them shall indicate the particular place at which the voter was registered. 2019: Presumably open. No specific exemption.

South Carolina	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: The exemptions for “unreasonable invasion of personal privacy” only specify home address for people with disabilities and for commercial uses, so a determination would need to be made before releasing an employee’s address to the public.
Firearms applications and permits			2011 & 2019: A list of persons with permits to carry concealed weapons may only be released to law enforcement or in response to a court order.
Voter registration documents			2011 & 2019: Official registration records are public records subject to inspection of any citizen at all times.

South Dakota	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Confidential other than salaries and routine directory information.
Firearms applications and permits			2011 & 2019: State law is designed to prevent release of information concerning those licensed to owning a firearm or carrying a concealed pistol.
Voter registration documents			2011 & 2019: Voter registration records are open.

Tennessee	**2011**	**2019**	**Comments**
Personnel files			2011: Generally open, but not Social Security Numbers. 2019: Court interpretations have gone back and forth. 2013 case ruled residential addresses of third-party contractors was public. 2017 case ruled all residential addresses were confidential information. Legislature later amended the code to eliminate addresses from category of protected information. TCA 10-7-504(f) - Telephone numbers, residential addresses, Social Security Numbers, bank account numbers, and driver's license information of public employees or their immediate family members is exempt from disclosure.
Firearms applications and permits			2011: There is no restriction on public access to gun permits, although certain information in the application for the permit might be kept confidential by other provisions of the law. 2019: Information in an application for a handgun permit are confidential.
Voter registration documents			2011 & 2019: Voter registration records are open.

Texas	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Information revealing home addresses, home telephone numbers, and SSN of current or former governmental officials and employees, as well as certain peace and security officers, is protected.
Firearms applications and permits			2011: Addresses presumed open because gun permits are not specifically addressed in the law. 2019: Information on individuals licensed to carry concealed handguns is confidential and not subject to requests under the act.
Voter registration documents			2011 & 2019: Applications to register to vote on file with a county registrar are public information.

Utah	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Records concerning a current or former employee of, or applicant for employment with, a government entity "that would disclose the individual's home address, home telephone number, Social Security number, insurance coverage, marital status, or payroll deductions" are exempt.
Firearms applications and permits			2011 & 2019: Names, addresses, telephone numbers, dates of birth, and SSN are classified as protected records.
Voter registration documents			2011: Voter registration records, including a person's voting history, are public except for those parts "identifying a voter's driver license of ID card number." 2019: adds e-mail address and date of birth to exempt details.

Vermont	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Personal documents are exempt. Defined as information relating to "personal finances, medical or psychological facts" or that "reveal intimate details of a person's life, including any information that might subject that person to embarrassment, harassment, disgrace, or loss of employment or friends."
Firearms applications and permits		N/A	2011: Addresses presumed open, as gun permits are not specifically addressed in the law. 2019: Gun permits are not required in Vermont, so no such records exist.
Voter registration documents			2011: Records of a registered voter's birthdate, driver's license number, SSN, and street address are exempt. 2019: Telephone number and e-mail address now listed, but home address no longer on the list.

Virginia *	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Personnel records containing identifiable individuals are excluded. State statutes define "personal contact information" as including home address or telephone number. The exemption is discretionary, so a government may choose to release a file or some part of a file.
Firearms applications and permits			2011: Information from the concealed carry permit database should be limited to law-enforcement personnel for investigative purposes. Always individually disclosable at courthouses. 2019: In 2013, the legislature prohibited release of the permit information at courthouses. (Virginia Coalition for Open Government) The Department of State Police receive all orders issuing concealed handgun permits, but the information is withheld from public disclosure.
Voter registration documents			2011 & 2019: Voter registration documents are covered by state Election Code, which says they are open to inspection by the public. If voter has provided a P.O. box address instead of home address, there is a prohibition against releasing home address from record. (per Virginia Coalition for Open Government).

Washington *	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Residential addresses, telephone numbers, wireless numbers, personal e-mail addresses, SSN, and emergency contact information of employees or volunteers of a public agency are exempt from disclosure.
Firearms applications and permits			2011 & 2019: License applications for concealed pistols are exempt from public disclosure.
Voter registration documents			2011 & 2019: The voter registration list, including addresses, is available for download from the Secretary of State website, but cannot be used for commercial purposes. The state has a voter address confidentiality program for some crime victims. (Per Washington Coalition for Open Government)

West Virginia	**2011**	**2019**	**Comments**
Personnel files			2011: Facts – such as an individual's name and residential address – which "are not 'personal' or 'private' facts but are public in nature in that they constitute information normally shared with strangers and are ascertainable by reference to publicly obtainable books and records" are disclosable without a balancing test. 2019: Under the Public Records Management and Preservation Act, personal information of state officers, employees, and retirees – including home addresses – is confidential.
Firearms applications and permits			2011: Addresses presumed public, as there is no provision in state law exempting information from the licenses. 2019: In 2015, the state legislature amended FOIA to exempt gun license application information. But then in 2016, the legislature removed requirements to have a permit to carry a hidden firearm, so the exemption is moot.
Voter registration documents			2011 & 2019: While there are no cases construing FOIA in the context of voter registration records, such records have been routinely made available to the public upon request.

Wisconsin *	**2011**	**2019**	**Comments**
Personnel files		No data	2011: Certain employee personnel records, including home address, is exempt.
Firearms applications and permits		No data	2011: Concealed carry license records are not public except in the context of a prosecution.
Voter registration documents		No data	2011: Addresses presumed open as election records are open to public inspection.

Wyoming	**2011**	**2019**	**Comments**
Personnel files			2011 & 2019: Personnel files are closed, except for qualifications for employment and salary.
Firearms applications and permits			2011 & 2019: Concealed carry permits are confidential.
Voter registration documents			2011 & 2019: While some personally identifying information is confidential, names, gender, and addresses are not exempt.