

REGULATING PUBLIC RECORDS REQUESTS FOR ELECTION TECHNOLOGY RELATED MATERIALS

Risa Nakagawa*

Advancements in election technology have led to both administrative convenience and greater levels of skepticism of electoral fraud. While election technology is promising, it is critical for voters to trust the system in order to have an effective, democratic election. This Note argues that there is no “right” answer to the question: what is the perfect balance between transparency and security for elections? Rather, this Note shows that to improve voter confidence and election security while being consistent with the trend of improving government transparency, there must be nationwide, uniform treatment of public records requests for election technology material. Although elections are run on a state level and operate under state laws, this Note argues that the potential for public disclosure of election technology material poses an unprecedented ability to harm the electoral process, such that it requires election offices across every state to have a consistent response.

* Georgetown Law J.D. Candidate 2024; Georgetown University B.S. 2019.

TABLE OF CONTENTS

INTRODUCTION	154
I. BACKGROUND TO PUBLIC RECORDS REQUESTS IN ELECTIONS	156
A. What are the Public Records Act and Freedom of Information Act?	156
B. The Purpose of Public Disclosures in Elections.....	158
C. Current Trend of Public Records Requests	160
II. CURRENT EXEMPTIONS/EXCLUSIONS FROM PUBLIC RECORDS ACTS ...	163
A. Past Court Cases Regarding Public Records Requests for Election Material	164
B. Current Grounds for Denying an an Election Technology Related Public Records Request	166
1. <i>State-Specific Exemptions: Election Technology Infrastructure.</i>	166
2. <i>State-Specific Exemptions: Technology Infrastructure</i>	167
3. <i>Detrimental to Public Welfare</i>	168
4. <i>Not Reasonably Described</i>	169
III. HOW ELECTION TECHNOLOGY DIFFERS FROM OTHER TYPES OF ELECTION MATERIALS.....	170
A. Recyclability of Election Technology Materials	170
B. Use of Election Technology Across State Borders.....	171
C. Opaqueness of the Election Technology Industry	172
D. Market Concentration within the Election Technology Industry	172
IV. TRANSPARENCY IN GOVERNMENTS AND THE ELECTORAL PROCESS	173
A. History of the FOIA and its Current Exemptions.....	174
B. Transparency in the Electoral Process	176
C. Federal Role in Elections.....	177
D. Finding the “Right” Balance.....	178
CONCLUSION.....	178

INTRODUCTION

The 2020 U.S. elections, including for the Presidency and Congress, faced strong allegations of voter fraud, in part due to their great reliance on election technology. Since the publication of its results, election offices across the nation have experienced a dramatic increase in public records requests. These requests are made pursuant to each state’s version of a Public Records Act (PRA) (also

called a Freedom of Information Act, Open Records Act, etc.), which mandates public disclosure of certain governmental records upon citizen request. State PRAs are modeled off the federal Freedom of Information Act (“FOIA”), which serves the same function for federal-level agencies. Both PRAs and the FOIA are intended to increase government transparency and accountability. Both represent a right that originated from and evolved through eras of intense government secrecy, such as the Cold War and the Watergate scandal. As such, legal requests for election-related materials are not only within the public’s rights but are also an important part of the democratic, electoral process.

Although PRAs and the FOIA serve important functions in the political sphere, election offices have recently reported citizens attempting to weaponize the right provided by these laws. Since the 2020 elections, county clerks have been overloaded with frivolous requests, overwhelming county clerks with labor-intensive, or duplicative requests. Such requests detract from the time clerks have to prepare for upcoming elections, and offices across the nation have reported difficulties in retaining election workers to keep up with the workload.

In addition to the issue of abusive public records requests, there is another lingering question concerning one specific category of requests: requests for election technology-related materials. Although it is a relatively new and undiscussed topic, this category has the potential to make up a large bulk of future requests as reliance on technology continues to increase. Considering the security concerns that public disclosure of election technology materials can pose for the electoral process, should there be an exemption from PRAs for election technology materials? This Note shows that a broad exemption for all election technology materials would be inconsistent with the federal government’s efforts to increase transparency and, therefore, would be an unfavorable policy decision. Nonetheless, this Note argues that election technology materials should be treated differently from requests for non-technology election materials with the creation of a federal law that creates uniformity across states regarding what is and is not publicly disclosed.

This Note is structured as follows: Part I lays out the background of PRAs and their purpose in the realm of elections and looks at the current trends of requests being made at election offices. Then, Part II analyzes past court cases on PRAs and compares how those analyses may fit with public records requests for election technology material. This Part will also examine current PRAs to see if there are any effective exemptions for election technology already in place. Part III follows with an analysis of how election technology materials differ from other types of public records requests for non-technology

election materials such that it justifies different—and nationally consistent—treatment. Lastly, Part IV will consider the potential effects a broad exemption on election technology can have on voter confidence and election integrity. The conclusion will argue not for a broad exemption on requests for election technology materials, but instead advocate for a federally imposed, bright-line rule that applies to all states.

I. BACKGROUND TO PUBLIC RECORDS REQUESTS IN ELECTIONS

A. What are the Public Records Act and Freedom of Information Act?

A Public Records Act (PRA) allows members of the public to request public information that a governmental agency does not offer as part of normal business services.¹ Each state has its own version—generally called a Public Records Act, Freedom of Information Act, or Open Records Act—that is modeled off the Freedom of Information Act (FOIA), a federal law enacted on July 5, 1966, to provide the public with the right to request access to records from any federal agency.² The FOIA provides that any person has a right, enforceable in court, to obtain access to federal agency records subject to the FOIA, except to the extent that any portions of such records are protected from public disclosure by one of the nine explicit statutory exemptions or if disclosure is otherwise prohibited by law.³

The United States Supreme Court has explained that the “basic purpose” of the FOIA is to “ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed.”⁴ The U.S. government has further elaborated that the workable balance between “ensuring transparency, accessibility, and accountability in government” and the need of the government to

¹ See *What Is a Public Records Act Request*, L.A. CNTY. REGISTRAR’S OFF., <https://www.lavote.gov/contact-us/public-records-act-requests/what-is-a-public-records-act-request> [<https://perma.cc/4586-4CZB>]; see also David E. Pozen, *Freedom of Information Beyond the Freedom of Information Act*, 165 U. PA. L. REV. 1097, 1099 (2017).

² Freedom of Information Act, 5 U.S.C. § 552(a)(3)–(4) (“[E]ach agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules stating the time, place fees, and procedures to be followed, shall make the records promptly available to any person.”).

³ See *id.* § 552(a).

⁴ *N.L.R.B. v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978).

keep the information confidential is a “presumption of openness.”⁵ To overcome the presumption of openness and to withhold information, the federal agency must show that it has addressed three key questions (unless disclosure is prohibited by law, which preempts the presumption entirely): 1) Does the information being requested fall within one of the nine exemptions?; 2) Would providing the information requested lead to reasonably foreseeable harm?; and 3) Is partial disclosure possible and if so, what are the reasonable steps to segregate and release nonexempt information?⁶ While the practical execution of the FOIA and its presumption of openness is an issue that has received many criticisms,⁷ the message from Congress has consistently been about improving governmental transparency.⁸ This emphasis on creating a more transparent government, also highlighted by President Obama,⁹ is an idea that has been echoed by state governments in their PRAs.¹⁰

At the state level, while many PRAs use similar definitions and statutory language, each state has its specifications regarding various topics. Such distinctions can be seen in how states treat requests for

⁵ See Memorandum from Att’y Gen. Merrick Garland to the Heads of Exec. Dep’ts & Agencies 1 (Mar. 15, 2022), <https://www.justice.gov/ag/page/file/1483516/download> [<https://perma.cc/BF8Z-67BQ>] [hereinafter Garland Memorandum].

⁶ See *id.*

⁷ See David S. Jackson, *Privacy and Ohio’s Public Records Act*, 226 CAP. U. L. REV. 107, 111 (1997) (arguing that the broadening of the public’s right to access “the enormous databases maintained by government” acted as a catalyst for the privacy concerns “advanced in the modern setting”); see also Seth F. Kreimer, *The Freedom of Information Act and the Ecology of Transparency*, 10 U. PA. J. CONST. L. 1011, 1013–15 (2008) (discussing the ineffectiveness and lack of necessity of the FOIA).

⁸ See DANIEL J. SHEFFNER, CONG. RSCH. SERV., R46238, THE FREEDOM OF INFORMATION ACT (FOIA): A LEGAL OVERVIEW 49, 49 n.388 (2020) (citing S. REP. NO. 4, at 2-3 (2015) and H.R. REP. NO. 1441, at 14 (1976) (Conf. Rep.) as examples of Congress amending FOIA in order to advance executive branch transparency in response to judicial and agency actions). See also *The Freedom of Information Act: Improving Transparency and the American Public’s Right to Know for the 21st Century: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. (2022) (statement of Chuck Grassley, Member, S. Comm. on Judiciary) (“Government transparency is fundamental to good governance. The Freedom of Information Act, or FOIA, is supposed to help ensure this transparency. Congress has a responsibility to ensure that both the letter and spirit of FOIA are being faithfully carried out . . .”).

⁹ See Memorandum on Transparency and Open Government, 2009 DAILY COMP. PRES. DOC. (Jan. 21, 2009).

¹⁰ See, e.g., California Public Records Act, CAL. GOV’T CODE §§ 6250–70 (2021).

election material. What election material is prohibited from disclosure, what is preemptively published, and what is available upon request varies significantly from state to state. For example, for voter registration lists, each state specifies what specific information, to whom, for what purpose, and at what cost such data may be made public.¹¹ There are generally five possible outcomes to a public records request for information that is not preemptively disclosed: unrestricted disclosure, disclosure after a certain number of days after the close of an election, discretionary disclosure upon court decisions, disclosure subject to redaction, or denied disclosure.¹² While the variations in PRAs' statutory language often lead to different results for election-related requests, there has been a trend in statutory interpretation by district courts that indicates some form of uniformity. Coinciding with the federal movement in improving government transparency, some state governments and state courts have mandated liberally construing PRAs in favor of disclosure.¹³ Since President Obama issued a memorandum to federal agencies in 2009 for a "new era of open government," many district courts have reinforced this idea upon appeal of public records requests and have favored disclosure.¹⁴

B. The Purpose of Public Disclosures in Elections

Voter confidence is crucial in the US election system.¹⁵ Having confidence in the system that elects its leaders is one of the "most fundamental aspect[s] of [a] representative democracy," because the

¹¹ *Access To and Use of Voter Registration Lists*, NAT'L CONF. OF STATE LEGIS., <https://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx> [<https://perma.cc/F7WP-W3DC>].

¹² Using Oregon as an example, section 1.002(3) of Title 1 explicitly prohibits disclosure of personal identifying information from FOIA requests. OR. REV. STAT. § 1.002(3) (2021). Section 254.535 of Title 23 mandates the county clerk to destroy ballots and written challenge statements unless "otherwise ordered by the court." OR. REV. STAT. § 245.535 (2021). Section 247.940 of Title 23 permits a delivery of a statewide list of electors with certain information redacted. OR. REV. STAT. § 247.940 (2021).

¹³ See Memorandum on Transparency and Open Government, *supra* note 9.

¹⁴ See Dep't of Info. Pol'y, *Creating a "New Era of Open Government"*, DEP'T OF JUST.: OFF. OF INFO. POL'Y, <https://www.justice.gov/oip/blog/foia-post-2009-creating-new-era-open-government> [<https://perma.cc/E6HC-DC5K>].

¹⁵ Lonna Rae Atkeson & Kyle L. Saunders, *The Effect of Election Administration on Voter Confidence: A Local Matter?*, 40 PS: POL. SCI. & POL. 655, 655 (2007).

system serves as the link between citizens and their elected officials.¹⁶ Voter confidence is tied to the belief that the election system resulted in the outcome that accurately reflects the will of the people.¹⁷ Consequently, voter confidence is enhanced by election security and transparency.¹⁸ State election offices have taken various measures in an attempt to increase voter confidence, one of which has been the application of PRAs. In the hopes of increasing transparency and accountability of election workers, PRAs provide a way for voters to self-audit the election process by permitting the public disclosure of certain information. However, transparency and security are often at odds with each other.¹⁹ On one level, a democratic electoral process must preserve the secret ballot, which requires voter-identifying information to be kept undisclosed.²⁰ Another limitation posed on states is the fact that transparency can reveal vulnerabilities in the election system and put election integrity at risk. As such, states are faced with the challenge of striving for maximum transparency while not sacrificing the security of the system. Too much transparency can lead to malicious attackers successfully finding ways to attack the electoral system. Or, even if

¹⁶ *Id.*; see also LEE C. BOLLINGER, MICHAEL A. MCROBBIE, ANDREW W. APPEL, JOSH BENALOH, KAREN COOK, DANA DEBEAUVOIR, MOON DUCHIN, JUAN E. GILBERT, SUSAN L. GRAHAM, NEAL KELLEY, KEVIN J. KENNEDY, NATHANIEL PERSILY, RONALD L. RIVEST & CHARLES STEWART III, NAT'L ACADS. SCIS, ENG'G & MED., COMM. ON THE FUTURE OF VOTING: ACCESSIBLE, RELIABLE, VERIFIABLE TECH., SECURING THE VOTE: PROTECTING AMERICAN DEMOCRACY 12 (2018) [hereinafter SECURING THE VOTE] (“Representative democracy only works if all eligible citizens can participate in elections, have their ballots accurately cast, counted, and tabulated, and *be confident* that their ballots have been accurately cast, counted, and tabulated.” (emphasis added)).

¹⁷ Research indicates only a “weak causal connection between voter confidence and voter turnout, and it does not show clear causal links between certain high-profile election administration practices, such as voter ID laws, and voter confidence.” *Voter Confidence*, MIT ELECTION DATA AND SCI. LAB, <https://electionlab.mit.edu/research/voter-confidence> [<https://perma.cc/QGC7-2HAX>]. For the purposes of this paper, however, it is assumed that voter confidence is tied to election integrity and transparency of the electoral process. For further information on the correlation between the factors, see *id.* See generally SECURING THE VOTE, *supra* note 16.

¹⁸ See generally SECURING THE VOTE, *supra* note 16, at 73, 100, 111 (“The transparency provided by the availability of [information] increases confidence that the software functions as intended.”).

¹⁹ See Michael Halberstam, *Beyond Transparency: Rethinking Election Reform from an Open Government Perspective*, 37 SEATTLE U. L. REV. 1007, 1041–42 (2015).

²⁰ See generally SECURING THE VOTE, *supra* note 16, at 87–88, 100.

there are no actual malicious attackers, voter confidence may be at risk from the mere belief that attackers *could* utilize public disclosure to find vulnerabilities in the system.²¹ On the other hand, prohibiting transparency, or only allowing minimal amounts of it, may lead to a false sense of security and increase voter skepticism in the electoral process and its results.

C. Current Trend of Public Records Requests

In recent years, election officials have faced an “overwhelming” number of requests for election-related materials.²² Election officials report that most of these requests come from “amateur fraud hunters looking for proof of debunked conspiracy theories.”²³ It has reached a level where public records requests are reportedly becoming “weaponized” and overloading offices that oversee smaller populations so that the officials have less time to prepare for the upcoming election.²⁴ This flood of requests has led to harmful impacts on election workers, including increased burnout and

²¹ *See id.* at 92 (“Even if actual failures or compromises do not occur, there is a risk that public confidence in the electoral process could be undermined by the possibility of such compromise . . .”).

²² As of August 2022, many counties had surpassed the number of requests they had for all of 2021. For example, Maricopa County, Arizona, had an increase of 135%, and Washoe County, Nevada, had an increase of 150%. Andrew Selsky, *Flood of Records Requests Hampers Oregon Election Officials*, ASSOCIATED PRESS (Sept. 19, 2022, 7:02 PM), <https://apnews.com/article/2022-midterm-elections-oregon-portland-government-and-politics-29d7e97c8e0448b4c1128761fc7a0a75> [<https://perma.cc/87A9-P3VD>]; *see also* Nathan Layne, *Pro-Trump Activists Swamp Election Officials with Sprawling Records Requests*, REUTERS (Aug. 3, 2022, 7:04 AM), <https://www.reuters.com/world/us/pro-trump-activists-swamp-election-officials-with-sprawling-records-requests-2022-08-03/> [<https://perma.cc/NA55-MYF9>].

²³ Wesley Wilcox, the supervisor of elections in Marion County, Florida, has reported spending over a third of his time responding to public records requests. Jane C. Timm, *Amateur Fraud Hunter Bury Election Officials in Public Records Request*, NBC NEWS (Feb. 12, 2022, 5:00 AM), <https://www.nbcnews.com/politics/elections/amateur-fraud-hunters-bury-election-officials-public-records-requests-rcna15432> [<https://perma.cc/5BV8-YKYV>]. Arizona Secretary of State, Katie Hobbs, has reported not having enough funding or staffing to timely address the “broad fishing expeditions that require extensive resources.” *Id.*

²⁴ Election offices in Pennsylvania, Michigan, Florida, Arizona, and Virginia all report significant increases in public records requests. Timm, *supra* note 23.

turnover and a general decrease in people interested in election worker positions.²⁵

A majority of these requests ask for records associated with the 2020 elections.²⁶ Examples of frivolous requests regarding the 2020 elections include copy-and-paste inquiries, petitions to see “all records” in association with the election, and requests seeking prohibited materials such as identifying information.²⁷ These requests are often aggressive in tone, such as the following:

I am asking for a complete copy of the Tally machines from the November election. I will contact a lawyer if I have to. The public has a right to these records. I want a complete copy of the Tally tapes and machine tally totals from the November election in 2020. I am urging the American people to do the same. If cheating was involved people will be going to prison. Every American has a right to these records from the 2020 election.²⁸

One of the reasons behind this increase in demanding and often frivolous requests is traceable to Mike Lindell, an advocate for suspending voting machines that he claims denied Trump the 2020 election results.²⁹ In his “Moment of Truth Summit” campaign, Lindell encouraged people to seek more information about voting machines and ballots, as well as “any information they [could] get their hands on.”³⁰

In light of the issues facing election offices, officials have looked to the state legislature for assistance and guidance. For example, in North Carolina, in an attempt to ease the burden on election workers, the State Board of Elections issued guidance to local clerks that

²⁵ Layne, *supra* note 22.

²⁶ Timm, *supra* note 23.

²⁷ See *Search Results for “Election”*, CITY OF SAN DIEGO PUB. REC. REQUESTS, https://sandiego.nextrequest.com/requests?search_term=election [<https://perma.cc/J4LE-S5UT>].

²⁸ *Request 21-1767*, CITY OF SAN DIEGO PUB. REC. REQUESTS (Apr. 10, 2021, 10:37 PM), <https://sandiego.nextrequest.com/requests/21-1767> [<https://perma.cc/N6KR-CYCL>].

²⁹ JW August, *Vote Records Requests Deluge San Diego Registrar After MyPillow CEO’s Pitch*, TIMES SAN DIEGO (Sept. 24, 2022), <https://timesofsandiego.com/politics/2022/09/24/vote-records-requests-deluge-san-diego-registrar-after-mypillow-ceos-pitch/> [<https://perma.cc/6KNK-U6PZ>].

³⁰ *Id.*

ballots and cast vote records are confidential under state law.³¹ However, this has done little to slow the number of public requests coming in.³² In one county that allows voters to view ballots, the clerk still gets “hundreds and hundreds” of calls and public records requests about the 2020 election.³³

Despite the widespread issues facing election workers across the nation, the topic of requests for election technology-related materials has been relatively new and undiscussed. However, not only is this issue increasingly more relevant as elections rely more heavily on technology, but it also has the potential to pose a great challenge to election integrity if not handled properly. Oregon was one of the first state courts to address this issue when an Oregon resident, Tim Sippel, made a public records request for the Structured Query Language (SQL) file used to create and modify the content of a database for the public test conducted in the May 2021 election system.³⁴ The elections division of Washington County of Oregon, where the request was made, denied the request.³⁵ Mr. Sippel appealed the decision, and the County District Attorney concluded that the files were public and ordered Washington County to provide them.³⁶ Washington County went to court to block Mr. Sippel from receiving the file on the grounds that:

³¹ Fredreka Schouten, *Election Officials Confront Waves of Public Records Request from Trump Supporters*, CNN (Sept. 21, 2022, 7:13 AM) <https://www.cnn.com/2022/09/21/politics/public-records-requests-trump-supporters> [<https://perma.cc/CM2R-FALN>].

³² *Id.*

³³ The county clerk of El Paseo, Colorado made the ballot and the corresponding recorded vote by the tally machine publicly available in an effort to get in front of the issue that is burdening the election workers. Nonetheless, the county clerk has reported that this seems to have had little effect. Schouten, *supra* note 31.

³⁴ Oregon Secretary of State’s Pre-Trial Brief at 1, *Washington County v. Sippel*, No. 22-07782 (Or. Cir. Sept. 19, 2022) [hereinafter Pre-Trial Brief].

³⁵ The grounds on which the County denied the request were state exemptions for files that constitute trade secrets, are a computer program developed or purchased by an agency, or are a computer program that can identify security measures, weaknesses, or potential weaknesses. *Id.* at 2.

³⁶ While the DA concluded the files to be public, Deputy District Attorney David Pitcher advised the matter to be handled in court. Julia Shumway, *Oregon Records Dispute Plays Out Against Backdrop of Election Fraud ‘Big Lie,’* OR. CAPITAL CHRON. (June 14, 2022, 5:45 AM), <https://oregoncapitalchronicle.com/2022/06/14/oregon-records-dispute-plays-out-against-backdrop-of-election-fraud-big-lie/> [<https://perma.cc/KRS2-SD5W>].

[D]isclosure of the internal components of the voting system . . . can allow for malicious actors to identify additional ways to attack the elections system and compromise Washington County's elections infrastructure specifically, and Oregon elections infrastructure more broadly . . . [which] creates risks to elections infrastructure to any jurisdiction nationally using this system.³⁷

This ongoing case exemplifies the underlying issue behind public records requests for election technology materials. These types of requests will force states to address the issue of how to ensure election integrity while providing transparency. While this is a topic that is new to the discussion of PRAs, it is possible that future public records requests will consist more heavily of election technology materials. As such, state legislatures need to be prepared with a response to these types of public records requests. The following Parts will outline one possible solution to this issue.

II. CURRENT EXEMPTIONS/EXCLUSIONS FROM PUBLIC RECORDS ACTS

Washington County v. Sippel demonstrates what is at stake with a public records request for election technology materials. As Washington County argued, the release of the SQL architecture has the potential to reveal vulnerabilities not only specific to Washington County's election but to any states and counties that use similar systems.³⁸ This means that the inverse is also true: if a different county allows for the public disclosure of the architecture of its SQL database, then Washington County may have nothing to protect, assuming that the two counties use similarly structured databases. This Part looks to explain why the development of and reliance on election technology requires a reevaluation of how to respond to public records requests. Furthermore, it will show that inconsistent treatment leading to disclosure in some states and non-disclosure in others will lead to increased risk of harm to the election process. This key difference between non-election technology information and election technology materials is such that it requires election

³⁷ Pre-Trial Brief, *supra* note 34, at 2. Oregon Secretary of State, Shemia Fagan, intervened to support the County, arguing that if a computer used to create a file that tells tabulation machines how to read the races is compromised, a hacker can disrupt the election. Oregon Secretary of State's Motion to Intervene at 1, *Washington County v. Sippel*, No. 22-07782 (Or. Cir. Mar. 21, 2022).

³⁸ Pre-Trial Brief, *supra* note 34, at 5–7.

technology be placed in a separate category that is not ruled by state law, but by a law that applies across the nation.

A. Past Court Cases Regarding Public Records Requests for Election Material

Since PRAs vary by state, it is unsurprising that state courts use different arguments to reject or accept public records request appeals. A court's interpretation of presumption of openness similarly varies, with some states having a stronger preference for disclosure while others favor a more concealed approach. One common factor with these decisions is that they are decided on narrow grounds that point to specific state statutes. To give a glimpse into some of these cases, some examples include:

- In *Price v. Town of Fairlee*, the Vermont Supreme Court ruled that the disclosure of ballots after the statutory preservation period has expired is permissible, on the grounds that once election results are finalized, the purpose of maintaining the ballots under seal is no longer applicable.³⁹ The court specified that the PRA “must be construed narrowly to implement the strong policy in favor of disclosure.”⁴⁰
- In *White v. Skagit County*, a Washington Court of Appeals decided that ballots, including their copies, are exempt in their entirety from public disclosure on the ground that they are “necessary to protect the vital government function of secret ballot elections.”⁴¹
- In *White v. Clark County*, the Washington Court of Appeals ruled that since voters are provided “absolute secrecy” in their votes, public disclosure of ballots—even three years post-election—need the requestor to show that withholding the ballots is “clearly unnecessary” in order to protect any individual's right

³⁹ *Price v. Town of Fairlee*, 26 A.3d 26, 33 ¶ 19 (Vt. 2011) (holding that “no legislative policy is...furthered by maintaining [the] confidentiality” after the finalization of election results).

⁴⁰ *Id.* ¶ 17 (“[The] express, overarching goal of ensuring public access to review and criticize the performance of our public officials even though such examination may cause inconvenience or embarrassment plainly must take precedence.”).

⁴¹ *White v. Skagit*, 355 P.3d 1178, 1184, ¶ 28 (Wash. Ct. App. 2015) (holding that ballots “in their entirety” are prohibited from public disclosure because redaction will “not eliminate the risk that disclosing copies of ballots will reveal the identity of individual voters.”).

to privacy or any vital governmental function.⁴²

- In *Madison Teachers, Inc. v. Scott*, the Supreme Court of Wisconsin found that if and when intimidation in an election is a potential threat as a result of public disclosure, then the “public interest in election that are free from intimidation and coercion outweighs the public interest in favor of open public records.”⁴³
- In *Trout v. Bucher*, the Fourth District Court of Appeal of Florida concluded that fees on a public records request must be “reasonable because an excessive charge could well serve to inhibit the pursuit of rights conferred by the Public Records Act.”⁴⁴

As these examples show, while PRAs are modeled off the same federal legislation, their application results in different outcomes.⁴⁵ Depending on the state, certain election-related materials are permissible for public disclosure while others are prohibited. This seems to suggest that election technology-related material will be treated similarly—some states will prohibit public disclosure on the grounds of ensuring election integrity while others may permit public disclosure on the grounds of favoring transparency. Giving discretion to state election offices and district courts to determine what election technology materials should and should not be disclosed is dangerous, for the reasons stated above. The idea that election technology-related material will be treated similarly, however, presumes that state law does not already have statutory exemptions for election technology information. The next Part will look at various public records acts and exemptions to examine how

⁴² *White v. Clark County*, 401 P.3d 375, 380 (Wash. Ct. App. 2022) (holding that though the PRA must be liberally construed in favor of disclosure to protect the public interest in full disclosure of public information, since “preserving the integrity and secrecy of votes and the security of election ballots clearly is a vital government function,” scanned images of pre-tabulated ballots cannot be publicly disclosed).

⁴³ *Madison Teachers, Inc. v. Scott*, 906 N.W. 2d 436, 445 (2018) (arguing that while the public's right to access public records is very strong, it is not unrestricted).

⁴⁴ *Trout v. Bucher*, 205 So. 3d 876, 879 (Fla. Dist. Ct. App. 2016).

⁴⁵ John Kreienkamp, *The Meaning of Creation: Electronic Databases and Creating a Record to Fulfill a Public Records Request*, 47 RUTGERS COMPUT. AND TECH. L.J. 197, 201 (2021) (“Although the country’s public records laws vary widely depending on the state or jurisdiction and the language in the specific statute, all are premised on the idea that the public is entitled to the greatest possible information regarding the affairs of government.”).

public records requests for election technology would be treated given the current state of the law.

B. Current Grounds for Denying an an Election Technology Related Public Records Request⁴⁶

In order to reach a conclusion as to how election technology should be treated with respect to PRAs, it is necessary to first look into how it would be treated under the current statutory exemptions. As such, this Part looks at various public records request exemptions that could apply to election technology. As it will show, the current state of the laws could allow for public disclosure in some states and prohibit disclosure in others.⁴⁷

1. State-Specific Exemptions: Election Technology Infrastructure

The most compelling statutory exemption for prohibiting public disclosure of election technology materials is state-specific exemptions for technology.⁴⁸ There are generally two types of state-specific exemptions that can apply to election technology material:

⁴⁶ In an attempt to streamline the process and provide easier access to public records requests, many cities and counties have made public records requests publicly available on a database website called NextRequest. Alexa Capeloto, *Agency Perspectives on Online Public Records Request Portals*, 1 J. CIVIC INFO. 59, 60 (2019). Advertised as a “FOIA Management Software,” the platform is intended to give the government an easier method to track requests while it gives the public a way to access previously made requests. *See id.* at 64; *Open Records Request Platform*, CIVICPLUS, <https://www.nextrequest.com/> [<https://perma.cc/GUS2-G9XV>]. Even with only a limited number of counties and cities adopting this platform, NextRequest has released over 2.5 million public documents and has over 10,200 users. *Open Records Request Platform*, *supra* note 44. While this convenience has added “a greater sense of trust from the public to the governmental body due to efficiency, time management, and a commitment to transparency,” it also invites misuse and abuse by individuals seeking to bury a public agency under a mountain of paperwork and put a strain on their budgets. Capeloto, *supra* note 46, at 66–68, 70 (describing the effects and efficacy of public records request process portals from the agency perspective).

⁴⁷ This analysis did not review every state's PRA. Instead, it looked to common exemptions that would be applicable to election technology material. While this broad analysis of exemptions to PRAs provides a general view of how election technology material will be treated upon request, a more detailed analysis is recommended for a state-specific approach.

⁴⁸ *See generally* Kreienkamp, *supra* note 45 (explaining that specific exemptions to PRAs vary from jurisdiction to jurisdiction).

an exemption for “election infrastructure” and an exemption for “technology infrastructure.”

The first tier of exempting election technology infrastructure is unique to a number of states, including Arizona and Washington. Arizona specifically exempts “election programs” and “computer election programs” from public disclosure.⁴⁹ The Washington statute exempts “information about election infrastructure, election security, or potential threats to election security, the public disclosure of which may increase risk to the integrity of election operations or infrastructure.”⁵⁰ Under a plain meaning rule of statutory interpretation, this exemption prohibits public disclosure of election technology material on the grounds that public disclosure of source code or software architecture would allow malicious attackers to identify vulnerabilities and would increase the risk to election integrity.⁵¹ Under this type of statutory language, election technology will very likely be kept confidential and exempted from public record requests.

2. *State-Specific Exemptions: Technology Infrastructure*

The second tier—exempting “technology infrastructure”—is a more common exemption seen in state PRAs. An example of this type of statutory language is the Oregon Public Records Act, which exempts records that, if disclosed, would allow a person to “identify those areas of structural or operational vulnerability that would permit unlawful disruption to, or interference with, services.”⁵² This is a broader version of the Washington legislation, and applies an exemption more generally to technology without specifying the elections context. While this type of exemption may not specify election technology materials, it does not automatically mean that election-related materials are not exempted. Utilizing the same plain meaning rule of statutory interpretation as above,⁵³ a “technology

⁴⁹ ARIZ. REV. STAT. ANN. § 16-445(d) (2022) (“All materials submitted to the secretary of state (including election programs, computer programs, electronic signatures) . . . shall not be disclosed.”).

⁵⁰ WASH. REV. CODE § 42.56.420(7)(ii) (2021).

⁵¹ For more information on the plain meaning rule, see Arthur W. Murphy, *Old Maxims Never Die: The Plain-Meaning Rule and Statutory Interpretation in the Modern Federal Courts*, 75 COLUM. L.J. 1299, 1231 (1975) (explaining how plain meaning rule in statutory interpretation is used to interpret unambiguous language).

⁵² OR. REV. STAT. § 192.345(22)(b) (2021).

⁵³ The plain meaning rule interpretation would be that exposing vulnerabilities in the electoral systems can lead to an increased potential for malicious attackers to disrupt the electoral process, and as such election technology will be within this category of exemptions.

infrastructure” exemption is likely to apply to election technology because election technology is just that—a technology. Various states apply this type of statutory exemption, including Tennessee,⁵⁴ Colorado,⁵⁵ and California.⁵⁶

3. *Detrimental to Public Welfare*

An even broader form of exemption that could serve as the grounds for exempting election technology materials is one that considers impacts on public welfare. These exemptions, such as the one in Alabama, prohibit the public disclosure of records that could reasonably lead to detrimental impacts on public welfare if disclosed.⁵⁷ Although this exemption is not specific to technology or elections, the same logic would apply. Public disclosure of election technology can foreseeably lead to a detrimental impact on public welfare by exposing vulnerabilities to malicious attackers and increase the risk of attacks on the electoral process. The plain meaning of this category of exemption, however, allows an argument to be made *for* public disclosure of election technology. Such an argument would be on the grounds that transparency is a competing public welfare interest that should be weighed more heavily.⁵⁸ Since the security concerns posed by transparency can be mitigated by imposing penalties for harmful use of the data or by redacting highly sensitive information, the argument would be that public welfare would not foreseeably be harmed by the public disclosure of election technology material.⁵⁹ As such, it is unclear whether election

⁵⁴ TENN. CODE ANN. § 10-7-504(i)(1)(B) (2021) (exempting “information that would identify those areas of structural or operational vulnerability that would permit unlawful disruption to, or interference with, the services provided by a governmental entity.”).

⁵⁵ COLO. REV. STAT. § 24-72-204(2)(a)(VIII)(A) (2016) (exempting “critical infrastructure...that would be useful to a person in planning an attack on critical infrastructure” since it is contrary to public interest).

⁵⁶ CAL. GOV’T CODE § 7929.210 (2023) (exempting “record [that] would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency”).

⁵⁷ ALA. CODE § 36-12-40 (2006) (“The public disclosure of which could reasonably be expected to be detrimental to the public safety or welfare, and records the disclosure of which would otherwise be detrimental to the best interests of the public shall be exempted.”).

⁵⁸ See generally Rebecca Green, *Rethinking Transparency in U.S. Elections*, 75 OHIO ST. L.J. 779, 789–92 (2014) (arguing that states should increase government transparency in the electoral process to ensure public confidence in election outcomes, and combat the harm it brings to security by posing penalties for harmful uses of election data).

⁵⁹ *Id.*

technology-related public records requests would be denied or approved under a “detrimental to public welfare” type of statutory exemption.

4. *Not Reasonably Described*⁶⁰

Section 552(a)(3)(A) of the FOIA requires that all requests be “reasonably describe[d].”⁶¹ To satisfy this element, the request must be sufficiently detailed to “[enable] a professional employee of the agency who was familiar with the subject area of the request to locate the record with a reasonable amount of effort.”⁶² This requirement is designed to prevent agencies from having to respond to “general fishing expedition[s].”⁶³ However, not only does this exemption not apply to state-level agencies, but it also does not apply to election technology-related requests that are narrowly described. Although this federal exemption does not provide an adequate response to public records requests that pose a security threat, it can mitigate the burden on election workers overwhelmed with broad requests.

* * * *

In conclusion, nearly every state has an exemption that has the *potential* to apply to election technology materials. However, only a few states have exemptions that specifically prohibit election technology from being publicly disclosed. This confirms that these requests may be treated inconsistently nationwide, similar to how other election materials are disclosed in some states and kept

⁶⁰ This exemption is a federal statutory exemption and is not applicable to state PRAs. However, since this paper will call for federally imposed limitations on public disclosure of election technology materials, the paper examined possible exemptions outlined in the current FOIA that could serve this function. This subsection is to primarily show there are no current federal exemptions that can adequately respond to election technology material.

⁶¹ Freedom of Information Act, 5 U.S.C. § 552(a)(3)(A) (2016) (“Except with respect to the records made available under paragraphs (1) and (2) of this subsection, and except as provided in subparagraph (E), each agency, upon any request for records which (i) *reasonably describes such records* and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.” (emphasis added)).

⁶² H.R. REP. NO. 93-876, at 125–126 (1976) (Conf. Rep.).

⁶³ *Hudgins v. I.R.S.*, 620 F. Supp. 19, 22 (D.D.C. 1985) (dismissing the plaintiff’s request since employees of the agency could not comprehend the nature of any records responsive to the request, “as discernible from a general fishing expedition”).

confidential in others.⁶⁴ While this conclusion is logical given that elections are decentralized and governed by state law, the unprecedented reliance on technology in the electoral process calls for a reevaluation of PRAs and how elections offices should respond to requests for information that can reveal vulnerabilities in the software behind elections.⁶⁵

III. HOW ELECTION TECHNOLOGY DIFFERS FROM OTHER TYPES OF ELECTION MATERIALS

Despite the inconsistent treatment of certain election-related materials across states, the discrepancy has not yet caused any major inter-state conflicts. In fact, since elections are run on the state level, it is sensible for states to govern their electoral process with their own laws and decide what can and cannot be publicly disclosed.⁶⁶ However, there are fundamental differences between election technology- and other election-related materials that justify different treatment when it comes to public record requests. This Part will identify those differences and argue that these significant differences call for a federally imposed rule for election technology, one that requires uniform treatment by all states. For the purposes of this Note and Part, the term “election technology” will include source code, architecture, and other software-related items.

A. Recyclability of Election Technology Materials

Election technology is different from other types of election-related materials because election technology can be recycled.⁶⁷ Unlike ballots or record data, which are discarded and closed at the end of an election, the software and hardware may be used in future

⁶⁴ See, e.g., *Access To and Use of Voter Registration Lists*, *supra* note 11.

⁶⁵ Paul S. Herrnson, *Improving Election Technology and Administration: Toward a Larger Federal Role in Elections?*, 13 STAN. L. & POL'Y REV. 147, 148 (2002) (arguing that state and local governments are not “up to the task” of administering elections and federal leadership is necessary for election reform).

⁶⁶ *Id.*; see also SECURING THE VOTE, *supra* note 16, at 45–46, 115 (reporting that “[s]tates and local jurisdictions carry out the primary functions and processes associated with federal and state elections”).

⁶⁷ Turquoise Baker, Lawrence Norden, Warren Stewart & Megan Maier, *Voting Machines at Risk in 2022*, BRENNAN CTR. FOR JUST. (Mar. 1, 2022), <https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-2022> [<https://perma.cc/JRZ9-EBYW>] (finding that forty-three states relied on voting machines that were “past or near the end of their expected lifespans”).

elections.⁶⁸ Even if updated versions are used every cycle, such updates may be software updates that reuse the foundational source code.⁶⁹ This implies that the vulnerabilities that are exposed by public disclosure of previously used election technology may still be applicable to future elections if they utilize similar technology.⁷⁰ On the other hand, the disclosure of ballots after the close of an election has little impact on future elections since they are not reused.⁷¹ As such, disclosure of election technology materials has arguably more at stake for future elections than the disclosure of non-technology related materials.

B. Use of Election Technology Across State Borders

As noted in *Washington County v. Sippel*, other jurisdictions may utilize the same or similar voting technologies.⁷² Being inconsistent in disclosure policy can lead to inter-state conflict. As *Washington County* argued, disclosing its SQL architecture has the possibility of impacting not only its own elections but any other jurisdiction that utilizes a similar architecture.⁷³ This will increase the workload of election workers, who will have to be aware of what is being disclosed in other states to ensure that they have the appropriate security measures in place if vulnerabilities in their software are exposed. This is not only an extremely challenging task but is unnecessary and avoidable with federal intervention. Although

⁶⁸ *Id.* (reporting that although many states have replaced the most insecure voting systems by 2022, “outdated voting machines . . . remain a problem”).

⁶⁹ *Cf.* SECURING THE VOTE, *supra* note 16, at 87 (arguing that malware can be introduced into a system via software updates).

⁷⁰ *See* Baker, Norden, Stewart & Maier, *supra* note 66. However, the foundational source code may not be available to the public even via PRA because of exceptions for proprietary information and trade secrets. SECURING THE VOTE, *supra* note 14, at 46 n.37 (noting that “the software used to operate voting systems is generally proprietary,” and therefore it is difficult for people outside of the company to “view it to identify flaws or vulnerabilities”); MATTHEW CAULFIELD, ANDREW COOPERSMITH, ARNAV JAGASIA & OLIVIA PODOS, THE PRICE OF VOTING: TODAY’S VOTING MACHINE MARKETPLACE 25 (2021), <https://verifiedvoting.org/wp-content/uploads/2021/03/Price-of-Voting-FINAL2.pdf> [<https://perma.cc/8CMV-SJRJ>] (reporting that a 2018 public records request from the San Francisco Elections Commissioner for a Smartmatic voting system’s source code was denied because it is proprietary).

⁷¹ *Price v. Town of Fairlee*, 26 A.3d 26, 33, ¶ 19 (Vt. 2011) (holding that after the finalization of election results, ballots may be disclosed since there is “no legislative policy . . . furthered by maintaining [their] confidentiality”).

⁷² Pre-Trial Brief, *supra* note 34, at 2.

⁷³ *Id.*

elections are run by the state and most related materials are state-specific, election technology may carry more similarities across jurisdictions and therefore has such a significant effect on other states that it requires uniformity in what is disclosed.

C. Opaqueness of the Election Technology Industry

Another difference when it comes to voting technology and public disclosure exemptions is that voting technology is sourced by certified third parties and governments are entitled to its use through licensing agreements.⁷⁴ As such, it is dissimilar from ballots or voter records on the grounds that the state does not have full control over the technology. Disclosure may be prohibited or limited per the licensing agreement with private third parties. Moreover, these private companies may be reluctant to disclose their source code.⁷⁵ The fact that election technology may be a trade secret is not only a fundamental difference from other election-related material, but it may pose licensing limitations that prohibit public disclosure. Forcing election workers to determine the legal limits on permitted disclosure may be complex and lead to unnecessary legal battles. Having a bright-line approach for public disclosures of materials related to voting technology would provide a simple solution that can be readily administered.

D. Market Concentration within the Election Technology Industry

The top three voting machine companies—ES&S, Dominion, and Hart InterCivic—make up more than 80% of the market.⁷⁶ While public information on these private companies is notoriously limited,

⁷⁴ See generally Ben Wofford, *One Man's Quest to Break Open the Secretive World of American Voting Machines*, POLITICO (June 25, 2021, 4:30 AM), <https://www.politico.com/news/magazine/2021/06/25/voting-machines-costs-election-technology-democracy-matthew-caulfield-483080> [<https://perma.cc/4LE2-YKAN>].

⁷⁵ LORIN HITT, SIMRAN AHLUWALIA, MATTHEW CAULFIELD, LEAH DAVIDSON, MARY MARGARET DIEHL, ALINA ISPAS & MICHAEL WINDLE, *THE BUSINESS OF VOTING: MARKET STRUCTURE AND INNOVATION IN THE ELECTION TECHNOLOGY INDUSTRY* 12 (2016), <https://verifiedvoting.org/wp-content/uploads/2021/05/the-business-of-voting-single-page.pdf> [<https://perma.cc/2F6J-YFFL>] (arguing that the technology sector of voting systems needs to be better understood by the American society).

⁷⁶ CAULFIELD, COOPERSMITH, JAGASIA & PODOS, *supra* note 70, at 6. This figure is current as of 2020. *Id.* at 6, 18–20 (“The ‘big three vendors’ . . . still control 88.8% of the market.”).

the heavy market concentration is an indication of a lack of competition and a lack of pressure to innovate.⁷⁷ Furthermore, since these private companies sell to government entities, it is likely that they are not driven by the potential for bigger profits due to the limited financial constraints of state governments.⁷⁸ Due to these factors, private companies lack the motivation to make new innovations that overhaul previous technologies, making it more likely that they cut costs with less expensive and less labor-intensive software updates. This ties back to the first element of the possibility of software being recycled for future use. Market concentration exacerbates this possibility.

In conclusion, the differences between election technology and non-technology materials are significant. Crucially, inter-state interests may be in conflict if election technology material is disclosed in some states and not in others. The potential for states to harm other jurisdictions' elections, the likelihood of election technology being recycled, the complications of licensing agreements, and the lack of industry growth in voting technology are all compelling factors to reevaluate PRAs. Public disclosure of election technology material needs to be consistent across states in order to mitigate the harm it can have on the US electoral process.

The question then is what should this uniform treatment be? Should election technology materials be broadly excluded from public disclosure? The next Part looks at the fundamental principle behind the Freedom of Information Act—the presumption of openness and improving government transparency—to explain that a broad exclusion will not be a policy favored by the federal government.

IV. TRANSPARENCY IN GOVERNMENTS AND THE ELECTORAL PROCESS

The exploitation of the vulnerabilities in the American election system in recent years has created an urgency to reexamine the

⁷⁷ See SECURING THE VOTE, *supra* note 16, at 110 (“The structure of the current election technology marketplace provides limited incentives for technological innovation.”); see also Thomas Philippon, *The Economics and Politics of Market Concentration*, 4 NAT’L BUREAU ECON. RSCH. 11, 11 (2019), <https://www.nber.org/sites/default/files/2021-12/2019number4.pdf> [<https://perma.cc/5VRM-VKV6>].

⁷⁸ See SECURING THE VOTE, *supra* note 16, at 114 (“There is a lack of dedicated funding for new voting systems.”); see also CHARLES STEWART III, THE COST OF CONDUCTING ELECTIONS 1 (2022), <https://electionlab.mit.edu/sites/default/files/2022-05/TheCostofConductingElections-2022.pdf> [<https://perma.cc/NF8S-9PS6>].

voting system and improve voter confidence.⁷⁹ One approach to improve voter confidence is to increase transparency in the election system, specifically in the technology behind the voting systems. Increasing transparency in elections has been something many states and counties emphasize, although their approaches to achieve it have varied.⁸⁰ For example, El Paso County of Colorado publishes pictures of individual ballots and posts spreadsheets of the entire cast vote records on an online portal accessible to the public.⁸¹ This is pursuant to Colorado law which allows for sharing of ballot images and cast vote records,⁸² and is a system that the county clerk calls a “citizen auditor” tool.⁸³ On the other hand, Colorado’s neighboring state of Utah expressly prohibits the public release of cast vote records and ballots.⁸⁴ States have attempted to increase transparency in a multitude of ways, with counties creating ways for voters to self-audit or preemptively increase access to voting information on their webpage. The following Part will focus on the federally imposed trend of improving government transparency and how a PRA exemption can fit into this movement.

A. History of the FOIA and its Current Exemptions

Before imposing a federal limitation on a broad category of public records requests, it is important to understand the history of the FOIA and the current exemptions and exclusions. This will provide some color as to what standard must be met to impose a federal exemption to public disclosure. While the FOIA only applies to federal-level agencies, for reasons explained below, we will assume the federal government has the ability to impose a nationwide, preemptive exemption from PRAs.

The FOIA traces back to 1952 when a congressman from California began advocating for more government openness during

⁷⁹ See SECURING THE VOTE, *supra* note 16, at xii, 121–22.

⁸⁰ An important caveat to increasing transparency is maintaining anonymous and private ballot casting, which is a factor that cannot be at the expense of increased transparency. See Kreienkamp, *supra* note 45, at 204–05.

⁸¹ 2020 Records and Results, EL PASO CNTY, <https://clerkandrecorder.elpasoco.com/elections/2020-records-and-results/> [<https://perma.cc/5AKY-EAM4>].

⁸² COLO. CODE REGS. § 8-1505-1(17.6.1) (2022) (“The list of voters who cast a provisional ballot and the accept/reject code for the ballot is available for public inspection.”).

⁸³ See Schouten, *supra* note 31.

⁸⁴ UTAH CODE ANN. § 20A-4-202(2)(d) (2022) (“Each election officer shall . . . destroy [provisional ballots cast within the election officer’s jurisdiction] without opening or examining them.”).

a time of high government secrecy amidst the Cold War.⁸⁵ Despite the resistance it faced from federal agencies who were fearful that the inability to keep records a secret would be detrimental to their work, Congress passed the bill in 1966.⁸⁶ President Lyndon B. Johnson “reluctantly” signed the bill later that year.⁸⁷ However, it was not until 1974, after the Watergate scandal, that the FOIA provided enforceable rights to the public.⁸⁸ In 1982, President Ronald Reagan created new rules that made withholding information much easier, only to be reversed by President Bill Clinton in the following decade.⁸⁹ Clinton signed into law the Electronic Freedom of Information Act which acknowledged how new technologies would allow for greater transparency.⁹⁰ After the September 11, 2001, attacks, however, President George W. Bush imposed a number of restrictions on the FOIA, leading to what is regarded as “the most secretive administration in history.”⁹¹ The federal government reversed course again under President Obama, who adopted the “presumption of disclosure” idea, and encouraged transparency and preemptive disclosure by the government.⁹²

⁸⁵ See Patricia M. Wald, *The Freedom of Information Act: A Short Case Study in the Perils and Paybacks of Legislating Democratic Values*, 33 EMORY L.J. 649, 650 (1984) (explaining that people were concerned about “unaccountable bureaucrats” even before the enactment of the Freedom of Information Act).

⁸⁶ History.com Editors, *Freedom of Information Act*, HISTORY.COM, <https://www.history.com/topics/1960s/freedom-of-information-act> [<https://perma.cc/3D7T-RC3H>].

⁸⁷ President Lyndon B. Johnson believed it would limit the ability of government officials to communicate and function effectively. *Id.*

⁸⁸ Fred H. Cate, Annette D. Fields & James K. McBain, *The Right to Privacy and the Public’s Right to Know: The Central Purpose of the Freedom of Information Act*, 46 ADMIN. L. REV. 41, 48 (1944).

⁸⁹ *History of FOIA*, ELEC. FRONTIER FOUND., <https://www.eff.org/issues/transparency/history-of-foia> [<https://perma.cc/B2SZ-55YE>].

⁹⁰ *Id.*

⁹¹ *Id.*; see also David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 631 (2005) (“Facing a post-9/11 national security environment of informational anxiety and terrorist threat, the Administration has designated FOIA a critical liability and narrowed its openness-forcing capacity accordingly.”).

⁹² See Memorandum on Transparency and Open Government, *supra* note 9. But see Margaret Sullivan, *Obama promised Transparency but His Administration is One of the Most Secretive*, WASH. POST (MAY 24, 2016), <https://www.washingtonpost.com/lifestyle/style/obama-promised-transparency-but-his-administration-is-one-of-the-most-secretive/2016/05/24/5a46caba-21c1-11e6-9e7f->

After this long and windy road of the FOIA's development, United States attorneys general in recent years have been consistent in emphasizing improving government transparency. A 2022 memorandum released by Attorney General Garland reemphasized the presumption of openness and declared that a "fair and effective administration of [the] FOIA requires that openness prevail in the face of doubt."⁹³ The memorandum, which encourages proactive disclosure, clearly indicates that the federal government continues to focus on improving government transparency.⁹⁴

The nine exemptions that enable federal agencies to withhold documents include those related to national security, foreign policy, personal privacy, confidential business information, and law enforcement records.⁹⁵ Election technology could arguably be categorized as a national security issue on the grounds that risks to election integrity are a matter of national security. It could also arguably fall into the category of confidential business information on the grounds that election technology is proprietary software and, therefore, the government has the responsibility to maintain such information private.⁹⁶ However, this issue of where and how election technology fits into a FOIA exemption is a policy question reserved for Congress. States do not have the capacity or capability to oversee the broad impacts their PRA exemption could have on other states. Therefore, this issue needs to be left in the hands of Congress. When considering this policy issue, Congress should put significant weight on transparency in order to be in alignment with the goals promoted by Attorney General Garland.

B. Transparency in the Electoral Process

A transparent electoral process is when "each step is open to scrutiny by stakeholders, who are able to independently verify the process is conducted according to procedures and that no irregularities have occurred."⁹⁷ However, "[e]lectronic voting and counting technology pose a challenge [in] ensuring transparency, since visually-verifiable steps . . . are automated inside a machine."⁹⁸

57890b612299_story.html (showing that the Obama administration was also responsible for major acts of secrecy).

⁹³ Garland Memorandum, *supra* note 5, at 2.

⁹⁴ *See id.*

⁹⁵ Freedom of Information Act, 5 U.S.C. § 552(b) (2016).

⁹⁶ SECURING THE VOTE, *supra* note 16, at 46, 46 n.37; CAULFIELD, COOPERSMITH, JAGASIA & PODOS, *supra* note 70, at 25.

⁹⁷ *Transparency*, NAT'L DEMOCRATIC INST., <https://www.ndi.org/e-voting-guide/transparency> [<https://perma.cc/BP76-JXM8>].

⁹⁸ *Id.*

One solution to this problem is to provide transparency in the development of election technology.⁹⁹ While this may be difficult as it takes a certain level of understanding to ensure the development of software and vendors may be reluctant to disclose their source codes, transparency can serve as a way for stakeholders to gain confidence that the machines meet relevant requirements, function properly, and have the necessary security features.¹⁰⁰ As such, transparency can benefit the American electoral process by providing more grounds for voter confidence and ensuring higher standards of accountability.

C. Federal Role in Elections

As established above, elections are administered in a decentralized fashion.¹⁰¹ Nonetheless, the federal government is given constitutional power to play various roles in election administration.¹⁰² Congress has exercised its rights in a range of contexts and federal oversight of election administration and registration provisions have “gradually expanded” since the 1960s in response to issues of national concern.¹⁰³ The federal government now recognizes that while election administration is primarily a state and local responsibility, there are “occasions where the federal government should play a leading role by providing resources that will nudge election administrators in certain directions.”¹⁰⁴ Such an occasion includes the federal government's role in ensuring resilience against cyberattacks and protecting the United States’

⁹⁹ *Id.* (“The procurement, development, testing and certification of voting and counting equipment should be carried out transparently, so stakeholders are confident the machines meet relevant requirements, function properly and have the necessary security features in place.”).

¹⁰⁰ *Id.*; SECURING THE VOTE, *supra* note 16, at 111 (“The transparency provided by the availability of source code increases confidence that the software functions as intended.”). Since not everyone will understand the software, voters must rely on those who do understand these processes. As such, it is essential for stakeholders to have access to this process. *Transparency*, *supra* note 97.

¹⁰¹ SECURING THE VOTE, *supra* note 16, at 115.

¹⁰² *Id.* at 115–16. For example, the Elections Clause specifies that Congress can “make or alter” states’ regulations on congressional elections. U.S. CONST. art. I, § 4, cl. 1, *amended by* U.S. CONST. amend. XVII.

¹⁰³ SECURING THE VOTE, *supra* note 16, at 55.

¹⁰⁴ *Id.* at 116–17. For example, the U.S. Department of Homeland Security designated election infrastructure as a critical infrastructure sector, which prioritized the protection of election systems as a national security issue. *Id.* at 117.

election infrastructure.¹⁰⁵ Providing a federally-enforced rule on how to handle public disclosure of election technology materials falls within this category of protecting election infrastructure. As such, it is likely that it is within the federal government’s power to create such a preemptive rule.

D. Finding the “Right” Balance

Finding the right balance between transparency and security is a difficult task. Congress must consider factors of cost, efficiency, public perception, the burden on election workers, and limits posed by licensing contracts, as well as the effects it might have on transparency and security. It may be that there is no “right” answer. The purpose of this Note is not to propose the exact statutory language, but instead to show that election technology material needs to be treated in the same fashion in every state. To maintain election integrity in a way that does not come into conflict with the federally imposed trend of government transparency, Congress must enact a law that specifies how to treat public records requests for election technology material.

CONCLUSION

Whether it is open-sourced or strictly prohibited from public disclosure, the federal government should enact a law that establishes the standard for election technology related public record acts that fully preempts state and local law.¹⁰⁶ Anything that is inconsistent will only lead to unintended harm.¹⁰⁶ An example of such an unintended consequence is seen in *Washington County v. Sippel*, revealing that Mr. Sippel accidentally gained access to the SQL file when he found it mixed into another public records request fulfillment.¹⁰⁷ This ongoing case exemplifies both the legislative battle between the public disclosure of election tech databases and

¹⁰⁵ *Id.* at 117 (noting that the federal government is vital to “protecting America’s election infrastructure became a national security concern in the wake of Russian cyber efforts to target U.S. voting databases and systems”).

¹⁰⁶ See Herrson, *supra* note 65, at 156 (arguing that the U.S. political system “provides the federal government with a variety of routes for improving elections, ranging from a constitutional amendment to funding studies to generate and disseminate knowledge about elections”); see also SECURING THE VOTE, *supra* note 16, at 115 (“The federal government has . . . a legitimate role to play in election administration.”).

¹⁰⁷ Pre-Trial Brief, *supra* note 34, at 3. Washington County has placed a restraining order to prevent Mr. Sippel from talking about or sharing the file until the court case is over. Tim Sippel’s Trial Brief at 2, *Washington County v. Sippel*, No. 22-07782 (Or. Cir. Sep. 19, 2022).

ensuring election integrity, and the dangers of burdening election workers with overly broad requests. Illegal access to sensitive materials can cause great harm to election integrity. A federal exemption will not only prevent the security concerns discussed in this paper, but it will also help to create a predictable workflow for election workers.

The technological improvements and the greater reliance on election technology require higher standards of care in responding to public records requests. Furthermore, there needs to be a response to the cry for help from election workers who are being overloaded by frivolous public records requests. Imposing a federal exemption that clearly outlines what is and is not permitted for public disclosure can not only alleviate some of the work imposed on election workers but can also enhance security and election integrity. If successful, voter confidence may improve from the fact that election workers can use their time to prepare for upcoming elections instead of responding to frivolous public records requests. Furthermore, the enhancement of security, while not at the expense of transparency, will ensure a trustworthy election system that will hopefully lead to future elections that receive less scrutiny than the 2020 elections.