Drawing a Portrait of Confidence: One Resolution to Legitimate Voter Concerns in the Shadow of Illegitimate Violence

SHANE SANDERSON*

INTRODUCTION

Shortly after being declared the loser of the 2020 Presidential election, Donald Trump submitted a series of challenges to the certification of votes and transition of power.[1] Litigators either representing Trump or closely connected with him alleged that the loss was attributable to election fraud.[2] In support of the fraud narrative, political allies drew in part upon statements by computer science and election security experts that election technology security has been fraught for decades.[3] The legal challenges those claims supported have universally failed and at least some lawyers filing them have begun to face disciplinary proceedings, financial consequences, or both.[4]

* J.D., Georgetown University Law Center (expected May 2023); B.J., University of Missouri (2017).

[1] *See*, *e.g*., Ann Gerhart, *Election Results Under Attack: Here are the Facts*, WASH. POST (updated March 11, 2021), https://www.washingtonpost.com/elections/interactive/2020/election-integrity/. [https://perma.cc/X8BR-D9UW] ("[Former president Donald Trump's] campaign and others went to court in six states, where Biden's total margin was more than 311,000, to challenge certain ballots or the certification of the vote—and lost more than 60 cases, including at the Supreme Court.").

[2] *See*, *e.g*., Jon Swaine & Aaron Schaffer, *Here's What Happened When Rudolph Giuliani Made his First Appearance in Federal Court in Nearly Three Decades*, WASH. POST (Nov. 18, 2020), https://www.washingtonpost.com/politics/giuliani-pennsylvania-court-appearance [https://perma.cc/KY6A-QFGA] ("The president's attorney opened his appearance in court with a broad claim: that the Trump campaign was alleging 'widespread nationwide voter fraud.'"); Aaron C. Davis, Josh Dawsey, Emma Brown & Jon Swaine, *For Trump Advocate Sidney Powell, a Playbook Steeped in Conspiracy Theories,* WASH. POST (Nov. 28, 2020), https://www.washingtonpost.com/investigations/sidney-powell-trump-kraken-lawsuit [https://perma.cc/JLH8-BPCC] (stating that Sidney Powell was not representing Trump "in that Powell had not yet been paid by the campaign" but that "the banishment became not a defeat but a new opportunity").

[3] *See*, *e.g*., Lindell TV, *Mike Lindell Presents: Absolutely 9-0*, https://home.frankspeech.com/video/mike-lindell-presents-absolutely-9-0/ (last accessed April 17, 2022) (quoting University of Michigan Professor J. Alex Halderman who stated: "I know America's voting machines are vulnerable because my colleagues and I have hacked them—repeatedly").

[4] *See, e.g*., Rosalind S. Helderman, *Judge Orders Two Lawyers Who Filed Suit Challenging 2020 Election to Pay Hefty Fees: 'They Need to Take Responsibility'*, WASH. POST (Nov. 23, 2021), https://www.washingtonpost.com/politics/they-need-to-take-responsibility-federal-judge-orders-hefty-fees-assessed-against-two-lawyers-who-filed-suit-challenging-2020-election [https://perma.cc/4SFR-UYNJ] (reporting that a federal judge ordered two attorneys who filed an election lawsuit to pay $187,000 of the defendants' legal fees); Shayna Jacobs, Rosalind S. Helderman, & Devlin Barrett, *Giuliani's N.Y. Law License Suspended in Connection with Efforts to Overturn 2020 Election*, WASH. POST (June 24, 2021), https://www.washingtonpost.com/national-security/rudy-giuliani-law-license-suspended [https://perma.cc/L24G-L78S] (reporting that New

Many of the lawyers involved in the Trump-election litigation presented outright lies, both to the public and to the courts.[5] And it is at least in part because of the bald-faced nature of the lies made in court that they are subject to disciplinary authorities.[6] But attorneys are not always required to be truth-tellers. And in some instances, their ethical obligations may even require them to misrepresent their client's circumstances.[7] In the Trump election cases, however, lawyers' lies undermined confidence in the democratic process and threatened a unique harm to the function of our government.[8] Such harm may not be easily reversed.[9] The virtue in preventing the use of a democratic society's legal system to undermine the function of its own government should be apparent.[10]

In conjunction with the election litigation, Trump and his supporters ran a series of attacks on the electoral process that were fueled by and demonstrative of a lack of faith in the democratic process. As poll workers counted votes in the days following the election, the loser's supporters appeared outside the facilities demanding access and a stop to balloting tabulation.[11] When an election vendor employee was spotted working with a voting machine, Trump's supporters

York suspended the law license of Rudolph W. Giuliani in connection with communicating "demonstrably false and misleading statements . . . in his capacity as lawyer for" Trump).

[5] *See*, *e.g.*, Renee Knake Jefferson, *Lawyer Lies and Political Speech*, 131 YALE L.J. F. 114, 118 (2021) ("Sidney Powell's election lies were so egregious that Dominion Voting Systems sued her for defamation. As a defense, she argued 'no reasonable person' would have believed her.").

[6] *Id.* ("A New York State appellate court suspended [Rudy Giuliani's] New York license pending investigation, ultimately finding 'uncontroverted evidence' that he 'communicated demonstrably false and misleading statements to courts, lawmakers and the public at large in his capacity as lawyer for former President Trump and the Trump campaign in connection with Trump's failed effort at reelection in 2020.'").

[7] *Id.* at 125 ("Professional conduct rules not only permit lawyer lies, but in some instances may require less than candid speech, if not outright lies.").

[8] *Id.* at 115. ("Lawyer lies about the outcome of a valid election, whether told in chambers or in a press conference, risk causing unique, devasting harm to our democratic form of government and should not be tolerated by members of our profession. Indeed, philosopher Jeremy Waldron calls these types of lies 'among the worst kinds of lie to tell. They are libels on democracy.'"); *see also*, *Voter Confidence*, MIT ELECTION DATA + SCIENCE LAB, https://electionlab.mit.edu/research/voter-confidence [https://perma.cc/WUK4-3P8J] (last visited Dec. 12, 2021) (Chart showing that since 2000, voter confidence that their vote was counted as intended has ranged between 60 and 70 percent, and indicating that voters for the losing party have less confidence: in 2000, 59 percent of Democrats were very confident their vote was counted correctly; in 2020, 50 percent of Republicans had such confidence); *but see*, *Voter Confidence, supra*, note 8 (stating there is no evidence that election administration has a "direct effect" on voter confidence).

[9] *See* Rosalind S. Helderman, *'This Is Really Fantastical': Federal Judge in Michigan Presses Trump-Allied Lawyers on 2020 Election Fraud Claims in Sanctions Hearing*, WASH. POST (July 12, 2021) https://www.washingtonpost.com/politics/sidney-powell-disciplinary-hearing [https://perma.cc/Y6YK-5NSA] (The article quotes David Fink, a lawyer for the city of Detroit, regarding plaintiffs' later corrected misstatement of voter turnout: "The suggestion that this is some kind of harmless error because it was ultimately corrected flies in the face of the reality of what actually happened. . .These lies were put out into the world. When they were put out into the world, they were believed.").

[10] But, if it is not, see generally Jefferson, *supra* note 5, arguing that the lawyer should have a duty of candor toward the public in the context of lies about election results.

[11] *See*, *e.g.*, Katie Shepherd & Hannah Knowles, *Driven by Unfounded 'SharpieGate' Rumor, Pro-Trump Protesters Mass Outside Arizona Vote-counting Center*, WASH. POST (Nov. 5, 2020), https://www.washingtonpost.com/nation/2020/11/05/arizona-election-protest-votes/ [https://perma.cc/9U3P-MEWD].

threatened him.[12] Four days after election day, Joe Biden was declared the winner.[13] Trump claimed the election was fraudulent.[14] At least one lawyer with access to President Trump had proposed that the Vice President Mike Pence decline to certify the election.[15] Trump's followers came to Washington, D.C. on the day of the official certification of the electoral vote and stormed the Capitol while legislators met to certify the vote.[16] Only after the building was cleared did Congress conclude its duties and certify the election.[17]

In short, claims of faulty voting technology contributed directly to challenges to the legitimacy of the election, both in the Trump-election litigation and the streets. Those claims—and the legal challenges they inspired—are enmeshed in a lack of confidence in democracy. By issuing a claim that voting technology insecurity undermines the accuracy or legitimacy of election results, the speaker indicates a lack of their own confidence in the function of the democratic process. That claim might then further reduce the broader public's confidence in the process.

Unfortunately, there are several significant problems with extant voting systems that can similarly be used deplete confidence in democracy.[18] Components of election technology are known to be vulnerable to attack by hostile actors.[19] Weaponizing, sensationalizing, overstating, or simply speculating about the

[12] Hannah Allam, Devlin Barrett, Aaron C. Davis, Josh Dawsey, Amy Gardner, Shane Harris, Rosalind S. Helderman, Paul Kane, Dan Lamothe, Carol D. Leonnig, Nick Miroff, Ellen Nakashima, Ashley Parker, Beth Reinhard, Philip Rucker & Craig Timberg, *Red Flags*, WASH. POST (Oct. 31, 2021), https://www.washingtonpost.com/politics/interactive/2021/warnings-jan-6-insurrection/ [https://perma.cc/NFF2-3JCL] [hereinafter *Red Flags*].

[13] Toluse Olorunnipa, Annie Linskey & Philip Rucker, *Joe Biden Triumphs Over Trump, Says It Is 'a Time to Heal' Even as Trump Does Not Concede*, WASH. POST (Nov. 7, 2020), https://www.washingtonpost.com/politics/joe-biden-elected-president/2020/11/07/53ec8726-1f0b-11eb-ba21-f2f001f0554b_story.html [https://perma.cc/FUB5-ULJP].

[14] *Red Flags*, *supra* note 12.

[15] Josh Dawsey, Jacqueline Alemany, Jon Swaine & Emma Brown, *During Jan. 6 Riot, Trump Attorney Told Pence Team The Vice President's Inaction Caused Attack on Capitol*, WASH. POST (Oct. 29, 2021), https://www.washingtonpost.com/investigations/eastman-pence-email-riot-trump [https://perma.cc/7P46-M73S] ("Eastman's memos gave several options for Pence to use the vice president's ceremonial role of counting electoral college votes to halt Trump's defeat. Eastman has argued that the 1887 Electoral Count Act is unconstitutional, and that the vice president has power under the 12th Amendment to decide whether electoral votes are valid.").

[16] *Red Flags*, *supra* note 12.

[17] *Id.*

[18] *See* U.S. Senate, Select Committee on Intelligence, *Russian Active Measures, Campaigns, and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views* (S. Rept. 116-290) Washington, Government Publishing Office, at 3–10 (2020) (stating that our election systems not only can be hacked by foreign actors, but that—in 2016—that is precisely what happened, but that there is no evidence that any of the vote tallying or other substantive functions of those systems were tampered with).

[19] *E.g.*, Matt Blaze, *Election Integrity and Technology: Vulnerabilities and Solutions*, 4 GEO. L. TECH. REV. 505, 516–18 (2020) ("[M]uch of the voting technology used in the United States remains vulnerable not just to hypothetical expert attack in a laboratory environment, but also to practical analysis, manipulation and exploitation by non-specialists with only very modest resources.").

significance of such instances of vulnerability can undermine confidence in the voting process.[20]

There are also potential additional concerns to which the general public is not privy. The existence of these concerns is unclear because of contractual agreements between election jurisdictions and their technology vendors. The aforementioned contracts frequently include provisions preventing disclosure of or access to the computer code used by election technology in use throughout the country.[21] And for many states, these provisions are likely not negotiable.[22] This is to the benefit of technology vendors, who have a financial interest in keeping their intellectual property secured.

In addition, these agreements create an area of ambiguity in the factual landscape, which benefits would-be plaintiffs' attorneys in future election challenges. The adversarial truth-seeking system gives attorneys strong incentive to make the most of factual ambiguity. But it is this set of incentives—when combined with reckless attorneys' arguments, private contractors' election agreements, and problematic technology—that will feed a crisis of confidence in democracy.

Because bad-faith actors are not subject to disciplinary action when they operate in areas of ambiguity, clarifying ambiguity is to the benefit of the democratic process.[23] This Note proposes that Congress create binding requirements tying the certification of election technology to public inspection of that technology's source code. Additionally, it proposes that the legislature use a similar set of requirements to quickly and finally end the use of the most problematic types of voting machines.

Part I outlines the central legislative solution proposed, the reasons for its design, and the extent of disclosure that should be required. Because the proposed solution creates a potential for far-ranging litigation, Part II discusses the desirability of a prohibition in litigation on use of evidence derived from the proposed disclosures. Part III proposes a distinct bright-line rule necessitating entire disclosure of the code run by certain types of disfavored technology with the goal of disincentivizing production and use of those systems. Part IV addresses a series

[20] *See* Nicolas Berlinski, Margaret Doyle, Andrew M. Guess, Gabrielle Levy, Benjamin Lyons, Jacob M. Montgomery, Brendan Nyhan & Jason Reifler, *The Effects of Unsubstantiated Claims of Voter Fraud on Confidence in Elections*, 8 J. EXPERIMENTAL POL. SCI. 1, 3 (2021) ("[A study's] results suggest that unsubstantiated claims of voter fraud undermine the public's confidence in elections, particularly when the claims are politically congenial, and that these effects cannot easily be ameliorated by fact-checks or counter-messaging.").

[21] Candice Hoke, *Judicial Protection of Popular Sovereignty: Redressing Voting Technology* 62 CASE W. RES. L. REV. 997, 1012 (2012) (stating that election vendors' "procurement contracts routinely included clauses barring independent forensic assessments of election databases and the voting equipment").

[22] *See* NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, SECURING THE VOTE: PROTECTING AMERICAN DEMOCRACY 111 (2018) ("The customer base for voting machines is fragmented, and purchasers have widely varying levels of technological and purchasing expertise. Furthermore, buying power is limited for all but the largest customers.").

[23] *Cf.* MODEL RULES OF PROF'L CONDUCT R. 3.1 (2018) [hereinafter MODEL RULES].

of potential issues with the legislative solution proposed in the preceding three parts.

I. LEGAL LINE DRAWING IN THE SOURCE CODE

At its core, this proposal seeks to reduce secrecy surrounding election technology. Specifically, this Note argues that the source code—human-readable instructions upon which computerized voting machines run—should be made public to a degree determined by the legislature in consultation with experts in the field and via a mandatory federal election technology certification process. Successful completion of the certification process would be required before technology could be sold to the states for use in federal elections. Implementation of such a requirement would result in an increase in publicly-available knowledge of election technology processes. In the context of election litigation, this increase in public knowledge would reduce ambiguity available to leverage anti-democratic efforts.

Most categories of election technology would be addressed by application of the line described in this Part, which proposes balancing the public interest in transparency against vendors' profit-motive interest in secrecy. A small category of disfavored technology would be addressed by the line drawn in Part III of this paper, which proposes requiring entire disclosure of source code in disfavored Direct Recording Electronic machines—which produce no paper audit trail to allow independent verification of their results—to disincentivize production of that technology.[24] Additionally, to deescalate political tension and reinforce confidence in the electoral process, Part II discusses a proposed moratorium on litigation seeking to draw upon information derived from the disclosures described in this Part.

Due to issues of profitability, it is not feasible to make all code public under the current contracting model.[25] This means we must determine what portion of code should be public. There are two parties whose intellectual property interests and incentives to stay in the market are relevant: the vendors themselves, and developers of third-party software used on election computers. Although fully open-source elections software is available,[26] jurisdictions' contracts with vendors frequently use confidentiality provisions to keep code secret.[27] Also running on the machines are operating systems with their own intellectual-property protections.[28] Because of the interests involved, it is improbable that either property

[24] *See infra* Part III.

[25] *See, e.g.*, *infra* notes 28–30 and accompanying text.

[26] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *supra* note 22, at 111-14 (stating that although most jurisdictions use commercial systems with closed-source software, New Hampshire has implemented an open-source system in state, federal, and local elections).

[27] *See*, *e.g.*, Hoke, *supra* note 21, at 1012–13.

[28] *See*, *e.g.*, Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin & Dan S. Wallach, *Analysis of an Electronic Voting System*, IEEE COMPUTER SOCIETY PRESS, at 5 (2004) (stating that the software analyzed "was designed to run on a Windows CE device").

owner would remain in the marketplace if they were required to discharge all trade secret protections as a condition of certification. The market for voting machines is simply too small. Microsoft, for instance, would sooner exit the market than discharge trade secrets connected with consumer products that make up a far larger portion of its profitability.[29] Vendors, for their part, are much smaller in size and produce specialized products.[30] Even so, if they could no longer monopolize their technology, they would likely either exit the marketplace immediately and find a new market in which they could keep their trade secrets, or remain in their roles only so long as they were not required to put additional expenditures toward research and development.

The precise structure of the legislation proposed would vary depending on the political process and certain legal questions beyond the scope of this Note.[31] Currently, election technology certification does not include any determinations by the federal government that are binding on the states.[32] The Congress, though, is empowered under the Elections Clause to establish a uniform federal elections plan.[33] The exercise of that power might be used to convert the currently non-binding process of certification into a binding one.

This Note is not the first to consider the issue. A commentator who previously surveyed the area argued in favor of a requirement that the software used in voting machines be available for inspection following contested elections.[34] In 2009, Professor Jennifer Nou acknowledged vendors' intellectual property rights and noted that "successful election administration demands the means for voters or candidates to examine the data and technology that record and count votes."[35] Nou identified four contractual methods of resolving the tension between a public need for transparency and protection of software developers' intellectual property: 1) source code escrow, which involves providing the code to a third party to be released under certain conditions; 2) independent code review, under which

[29] *Compare EAC Commissioners Welcome Deal to Make Available $425 Million in New Help America Vote Act Funds for Elections*, U.S. ELECTION ASSISTANCE COMMISSION, https://www.eac.gov/eac-commissioners-welcome-deal-to-make-available-425-million-in-new-help-america-vote-act-funds-for-elections [https://perma.cc/XH9U-8H4E] (last accessed Dec. 12, 2021) (stating that the Congress appropriated $380 million for HAVA in 2018 and $425 million in 2020), *with* 2020 Annual Report, MICROSOFT https://www.microsoft.com/investor/reports/ar20/index.html [https://perma.cc/MNR5-VED7] (last accessed Dec. 12, 2021) (stating that the computing company recorded $143 billion in revenue and $53 billion in operating income over the year prior).

[30] Penn Wharton Public Policy Initiative, *The Business of Voting: Market Structure and Innovation in the Election Technology Industry* 16 (2017) (stating that the largest of the three firms dominating the American elections market employs about 460 people).

[31] *See generally* Suman Malempati, Note, *The Elections Clause Obligates Congress to Enact a Federal Plan to Secure U.S. Elections Against Foreign Cyberattacks*, 70 EMORY L.J. 417 (2020) for a discussion of the Congress' ability to legislate in the arena of voting technology and an argument in favor of legislative action for national security reasons.

[32] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *supra* note 22, at 80–83.

[33] Malempati, *supra* note 31, at 421.

[34] Jennifer Nou, Note, *Privatizing Democracy: Promoting Election Integrity Through Procurement Contracts*, 118 YALE L.J. 744, 779 (2009) [hereinafter *Privatizing Democracy*].

[35] *Id.* at 783.

state officials may ask a third-party to inspect the code; 3) required disclosure of source code, which allows for its use only for evaluation purposes; and 4) the use of open-source software.[36] Nou noted that—because computer scientists are not capable of writing entirely bug-free software[37]—public disclosure of source code would inform malicious actors of vulnerabilities that might be used to alter election results.[38] Nou did not clearly settle upon one of the "wide range of options . . . on the table" as most preferable for vendors' and governments' use.[39] Instead, she argued that any contract clause adopted to resolve the issue should be aimed at ensuring transparent and accountable vote counting.[40]

At least one large change since Nou published her article counsels in favor of rebalancing the measure of these methods' relative benefits. The knowledge that foreign adversaries are capable of manipulating our election outcomes[41] might mean that the risk of compromising source code by its disclosure is at least somewhat mooted. When considering changes in the voting landscape, it might also be reasonable to consider changes bearing on ancillary benefits to the proposed legislation. In the arena of litigation, a reduction in ambiguity would mean corresponding reduction of bad faith arguments that are beyond account. Public knowledge would also confer benefits beyond the courthouse. Disclosure might help assure the public that *American* government officials (or employees of voting systems vendors[42]) are not tampering with electoral outcomes. It is also worth noting the public shift toward increased skepticism of esoteric expertise and the mass circulation of conspiracy theories.[43] These shifts counsel against gatekept methods of disclosure like source code escrow.[44] After all, if some other party—

[36] *Id.* at 784.

[37] *See*, *e.g.*, Andrew W. Appel & Philip B. Stark, *Evidence-Based Elections: Create a Meaningful Paper Trail, Then Audit*, 4 GEO. L. TECH. REV. 523, 524 n.1 (2020) ("Estimates of software defect rates range from one per thousand lines of code (in high quality commercial products) down to 0.1 per thousand lines of code in extremely high-quality products (this is at the 90th percentile for the software industry).").

[38] *Privatizing Democracy*, *supra* note 34, at 785.

[39] *Id.* at 787.

[40] *Id.* at 779–80.

[41] U.S. Senate, Select Committee on Intelligence, *supra* note 18.

[42] *See*, *e.g.*, Barney Gimbel, *Rage Against the Machine: Diebold Struggles to Bounce Back from the Controversy Surrounding its Voting Machines*, FORTUNE MAGAZINE (Nov. 3, 2006) https://money.cnn.com/magazines/fortune/fortune_archive/2006/11/13/8393084/index.htm [https://perma.cc/R6HQ-L3MK] (last accessed Nov. 25, 2021) (describing a letter by the CEO of a voting company to supporters of presidential candidate George W. Bush stating he would "help Ohio deliver its electoral votes to the President").

[43] *See*, *e.g.*, Sravasti Dasgupta, *QAnon Supporters Gather at JFK Assassination Site in Belief that This Time JFK Jr Will Return from the Dead*, THE INDEPENDENT (Nov. 23, 2021) https://www.independent.co.uk/news/world/americas/us-politics/qanon-supporters-jfk-jr-dallas-b1962575.html [https://perma.cc/8C3F-K3KG] (last accessed Nov. 26, 2021).

[44] *Privatizing Democracy, supra* note 34, came just on the heels of Rivest and Wack's seminal article, *infra* note 89, reorienting the field toward the notion of systems whose results can be verified independent of the software underpinning them. But because Nou's article focuses on the development of market incentives, rather than the technology they might produce, the logic of her argument is just as relevant here, where source-code disclosure is proposed for public belief in the legitimacy of the electoral process as it was there, where the purpose of disclosure focused on providing election results verification *in addition to* public legitimacy in the election system.

but not the public—is sworn to secrecy and provided the code, the cynic or conspiracy theorist will have been provided no benefit of additional transparency. If these factors are sufficient to require disclosure of source code, the question then becomes: What portions of the election system's source code should be made publicly available before it is eligible for federal certification?

In determining the outcome of this inquiry, the legislature will be required to weigh the property interests of software developers against the transparency interests. This balancing act would also be circumscribed by the fact that vendors (and developers of operating systems upon which vendors rely) could exit the market altogether.[45] This risk, however, would be backstopped—albeit marginally—by already available open source replacement software solutions.[46] Because the proposed legislation aims to bolster the electorate's confidence in the vote,[47] the legislature should be cognizant that to the extent information is not made public, withholding may be cast as peculiar or suspicious by disinformation agents, conspiracy theorists, or—depending on the circumstances—reasonable cynics. Therefore, the legislature will need to present a coherent, logical, and well-founded justification for parts deemed necessary to keep closed.

In designing this schema, it could be helpful to look to other areas of law that have dealt with tension between intellectual property rights in software and a public interest in transparency. Drunk driving cases have provided a significant amount of case law demonstrating the challenges of accessing relevant source code belonging to private parties, even where there are strong interests of justice supporting publication of the code.[48] In such prosecutions, courts have generally been reluctant to allow criminal defendants to actually examine source code.[49] In Minnesota, the courts have deemed access to source code essential to a defense.[50] They have done so, though, only where a defendant has been able to make a

[45] *See*, *e.g.*, *supra* note 28–30 and accompanying text.

[46] *See* NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *supra* note 22, at 111–14, for further discussion.

[47] The anticipated bolstering effect could work by way of two methods: either direct public knowledge might create confidence or a reduction of bad-faith litigation might prevent the undermining of confidence. This result, of course, might not adhere if anti-democratic arguments were supported by newly public information.

[48] Steven M. Bellovin, Matt Blaze, Susan Landau & Brian Owsley, *Seeking the Source: Criminal Defendants' Constitutional Right to Source Code*, 17 OHIO ST. TECH. L.J. 1, 8–9 (2021) (stating that because DUI prosecutions rely heavily on third-party computer devices such as breathalyzers, the crime is committed relatively frequently by "people who are not considered criminals in the usual sense of the word," and convictions also have significant consequences, the cases are particularly ripe for discovery challenges).

[49] *Id.* at 14–15 ("Even as we rely on computer software to bear witness, we are simultaneously moving to a criminal justice system in which 'law enforcement privilege' frequently prevents access to the details of investigative techniques and procedures." (internal footnote omitted)).

[50] *Id.* at 57.

threshold showing that the code will be relevant to either a finding of guilt or degree of culpability.[51] Elsewhere, criminal defendants' luck has been worse.[52]

The threshold requirement used in Minnesota's DUI litigation has the benefit of marking a relatively bright line. Because our current inquiry is not in the context of a criminal case, the line would have to be transposed. Rather than requiring a showing pertaining to guilt or culpability (which are less useful concepts in the legislative arena), the line might be drawn to require a showing of danger to the function of an election or the security of the country. This re-drawn line, nevertheless, will only be of partial benefit. A significant portion of the population is already convinced that the electoral process is compromised or illegitimate.[53] That belief—independent of the truth of the claim—is enough to endanger the function of the election.[54] Additionally, the Senate Select Committee on Intelligence found that voting systems used in the 2016 election were indeed compromised by foreign agents.[55] That finding should be sufficient to support opening source code on the basis of security concerns.

The threshold test might also be applied in a modular manner, reflecting the common makeup of voting systems. In doing so, the Congress could look to Microsoft Windows' broad implementation in public and private settings. The legislature might, on the basis of that observation, find that the software's use in the election context poses neither a danger to the function of an election nor the security of the country.[56] In other words, the line should not be drawn to determine *when* disclosure is necessary. Disclosure is necessary now. Instead, the line should determine *what* to disclose and—if the additional inquiry is necessary—*how much* of that material to disclose. Those determinations are best made by parties with political and technical expertise far beyond that of this writer's.

The importance of soliciting expertise from the field of software design is particularly well-illuminated by the legislative path that led to where we are now. The involvement of computer technology in American elections was in large part

[51] *Id.* at 58–59 (arguing that it is "troubling" that such a showing is necessary because the problem of buggy code is "endemic in computer software" and only substantial evidence makes it appropriate to assume that a piece of software functions as it should).

[52] *See id.* at 55–56 (stating that an Arizona appellate court declined to allow a defendant to examine the source code or cross-examine a witness on the code and that a North Carolina appellate court determined a defendant had no legal basis to examine breathalyzer source code).

[53] Jennifer Nou, *Constraining Executive Entrenchment*, 135 HARV. L. REV. F. 20, 21-22 (Nov. 20, 2021) [hereinafter *Constraining Executive Entrenchment*].

[54] *See*, *e.g.*, *id.* at 21 ("These recent events underscore the relationship between perceived election integrity and the felt legitimacy of the incoming administration. To be sure, it cannot be the case that a losing candidate's baseless claims threaten the objective legitimacy of the winner. The observation for now is simply the positive correlation between valid elections that are recognized as such and acceptance of a transition in power—precisely why Trump's meritless claims pose such a democratic threat.").

[55] U.S. Senate, Select Committee on Intelligence, *supra* note 18.

[56] *But see*, *Privatizing Democracy*, *supra* note 34, at 787 (describing a Congressional Research Service finding that the way commercial-off-the-shelf software like Microsoft Windows "is tested and used in [certain voting machines] might itself create vulnerabilities").

facilitated by the Help America Vote Act of 2002, which directly responded to the 2000 Presidential election's highly contested Florida recount.[57] That legislation, which sought to remedy public concern with apparently failed technology, passed by a massive margin.[58] But it also introduced funding that supported and brought to market the voting system companies and components that subsequently contributed to the undermining of public confidence in the vote.[59] We must ensure that we do not once again move from the frying pan to the fire. Engaging involvement of subject-matter experts is essential if democracy is to be strengthened rather than undermined.

II. A PROBLEM WITH REMEDIES AND AN EVIDENTIARY PROHIBITION

Concurrent with the publications of voting systems' source code, the legislature should prohibit use of evidence in litigation revealed by this legislation[60] to make this solution politically palatable. Such necessity is derived from the current landscape of election technology and voter cynicism: despite the significant need for more secure election technology[61] and public distrust of the electoral process,[62] underfunded local governments are generally responsible for the administration and maintenance of election equipment.[63] Given that: a) voting technology is known to be deeply flawed;[64] b) the precise function of the technology is unknown to most of the election officials using it;[65] and c) there is ongoing

[57] *See* H.R. REP. NO. 107-329, at 32 ("The disadvantages of punch card voting systems were highlighted during the recount that took place in Florida following the November 2000 election. Large portions of the American public have lost confidence in them.").

[58] *See H.R. 3295 - Help America Vote Act of 2002* https://www.congress.gov/bill/107th-congress/house-bill/3295/actions?q=%7B%22search%22%3A%5B%22help+america+vote+act%22%5D%7D&resultIndex=1 (stating the final version of the legislation passed the House 357 – 48 and the Senate 92 – 2) (last accessed April 15, 2022).

[59] *See supra* Introduction.

[60] The exact method by which this moratorium should be implemented is beyond the scope of this Note. However, the solution proposed here is inspired by the federal rule of evidence prohibiting the introduction into evidence proof of measures that would have made an earlier injury or harm less likely to occur. *Cf.* FED. R. EVID. 407.

[61] *See* Blaze, *supra* note 19.

[62] *See e.g.*, *Constraining Executive Entrenchment*, *supra* note 53, at 21 ("Trump's 'big lie' continued to find significant support among Republican voters. One March 2021 poll, for example, found that fifty-five percent of Republicans believed that Trump's electoral defeat 'resulted from illegal voting.' That same month, another poll claimed that sixty-six percent of Republicans either completely or mostly agreed that 'the 2020 election was stolen from Donald Trump.' Whether these respondents actually believed their answers (versus just expressed their partisan loyalty) is an open question. But to those that did believe the claim, the Biden Administration represented an illegitimate power grab.").

[63] Blaze, *supra* note 19, at 506; *see generally* G. Michael Parsons, *The Price of Free Elections*, 74 VAND. L. REV. EN BANC 335, 341 (2021) (discussing economic pressures bearing on the electoral process).

[64] *Blaze*, *supra* note 19, at 510 ("Many of the software and hardware technologies that support US elections today have been shown to suffer from serious and easily exploitable security vulnerabilities that could be used by an adversary—insider or outsider—to alter vote tallies or cast doubt on the integrity of election results.").

[65] *See* Hoke, *supra* note 21, at 1013 (stating that election equipment contracts routinely include clauses barring the independent examination of voting equipment used *inter alia* "to eliminate the risk that evidence will be generated that can contradict the marketing assurances that the systems function accurately in real elections").

distrust of the election system and a corresponding appetite for election outcomes litigation,[66] it follows that opening the black box that is voting technology would almost certainly result in massive litigation efforts. These efforts, whether predicated on anti-democratic ideals or on a legitimate problem with an historic election, might aim more toward public perception than judicial remedies.

After all, remedies may not be administrable. If, for instance, the newly revealed source code was used to support a claim that the 2016 election was improperly tampered with, it seems unlikely that a reasonable judiciary could craft a judgment that would compensate the loss.[67] The questions a judiciary might face would be endless. For instance: It would need to determine whether a court should re-balance the vote and declare a "new" winner. It would need to decide whether to unwind every executive action undertaken in the preceding years. It would need to resolve whether private citizens impacted by executive actions could claim money damages. It would need to answer the same question for politicians whose fortunes had changed as a result of the law. It would need to decide if the new winner would be entitled to serve the term already served by the old "winner." If so, it would need to decide if it should suspend the democratic process for an election cycle. Or, alternatively, if elections should run on a four-year delay. It would need to decide if the 2020 election—resulting from votes case in political conditions created by an invalid government—should be deemed improperly tainted and overturned. Given the broad scope of these questions, it seems reasonable to think the judiciary would decline to enforce remedies for an improperly counted Presidential election that was not discovered before the improperly elected official had left office.[68]

Because perception is central to public confidence—and to help build consensus in this part of the democratic process—Congress should prohibit the use of information drawn from the newly-opened source code in support of any litigation seeking to challenge elections conducted prior to passage of the law. This solution is inspired in part by Federal Rule of Evidence 407 (Rule), which prohibits demonstrating liability with evidence of remedial measures implemented after occurrence of the harm at issue.[69] Among the policy supports for the Rule is a

[66] *See* discussion *supra* Introduction.

[67] *Cf.* Sarah Milkovich, Note, *Electoral Due Process*, 68 DUKE L.J. 595, 604 (2018) ("A greatly delayed revelation of mistaken election results would undermine the legitimacy of governance. Voters and legal systems would have to reckon with relics of the invalid exercise of public office: the prosecutorial choices of improperly elected district attorneys, the swing votes of improperly elected legislators, and the common law making of improperly elected state supreme court judges. A state's interest in the timely resolution of any doubts as to the integrity of an election is clear."). *But see generally*, *id.* (arguing that election security threats are so great that a new remedial framework should be implemented, with federal courts exercising stricter oversight of legal procedures to challenge election outcomes in state courts so that plaintiff can "more easily discover the extent of election failures and []prove their impact on election outcomes").

[68] *Cf.* Baker v. Carr, 369 U.S. 186, 210 (1962) ("In determining whether a question falls within (the political question) category, the appropriateness under our system of government of attributing finality to the action of the political departments and also the lack of satisfactory criteria for a judicial determination are dominant considerations." (quoting Coleman v. Miller, 307 U.S. 433, 454–455 (1939) (alteration in original)).

[69] FED. R. EVID. 407.

goal of encouraging parties to take actions that will make the world safer.[70] According to this reasoning, if remediation could be used against them, defendants might choose to leave the circumstances in their original unimproved state. In the same way, by opening public inspection technology that has historically been of questionable quality, we might encourage its creators to build safer and more secure machines, regardless of the—at least somewhat publicly unknown—extent of the current problem.

Public shaming has previously been effective in modifying election vendors' practices and market positions, even when those modifications were born of non-legislative processes. To provide one example: a writer in 2003 found Diebold voting machines' source code online.[71] She provided this code to a computer scientist.[72] His team's analysis found "significant and wide-reaching security vulnerabilities."[73] The report describing those vulnerabilities was released only days after the state of Maryland announced that it had purchased 11,000 of the company's machines.[74] Maryland then corroborated the report with its own third-party examination.[75] Further examination of the machines discovered a number of additional security flaws.[76] Following these findings, the state of California decertified some of the company's machines.[77] Diebold paid California $2.6 million as part of a settlement agreement.[78] Further changes followed. The company removed its name from the front of its voting equipment, at the time stating only that: "It was a strategic decision on the part of the corporation."[79] Ultimately, the voting systems company changed its name and was absorbed by a competitor.[80]

[70] FED. R. EVID. 407 Advisory Committee's note.

[71] Gimbel, *supra* note 42.

[72] *Id.*

[73] Kohno, *supra* note 28, at 4.

[74] Gimbel, *supra* note 42.

[75] Kohno, *supra* note 28, at 5.

[76] Center for Information Technology Policy, *Security Analysis of the Diebold AccuVote-TS Voting Machine: Executive Summary*, PRINCETON UNIV. https://citp.princeton.edu/our-work/voting/ [https://perma.cc/6LLK-BRR7] (last accessed April 14, 2022) ("The famous paper by Kohno, Stubblefield, Rubin, and Wallach studied a leaked version of the source code for parts of the Diebold AccuVote-TS software and found many design errors and vulnerabilities, which are generally confirmed by our study. Our study extends theirs by including the machine's hardware and operational details, by finding and describing several new and serious vulnerabilities, and by building working demonstrations of several security attacks.").

[77] Gimbel, *supra* note 42.

[78] *Id.*

[79] *Id.*

[80] *Justice Department Requires Key Divestiture in Election Systems* & Software/Premier Election Solutions Merger, U.S. DEPT. OF JUSTICE (March 8, 2010), https://www.justice.gov/opa/pr/justice-department-requires-key-divestiture-election-systems-softwarepremier-election [https://perma.cc/B5M6-LQ8R] (last accessed Dec. 12, 2021); *see also*, Verified Voting, *Premier Election Solutions (Diebold)* https://verifiedvoting.org/election-system/premier-diebold-dominion-accuvote-tsx/ [https://perma.cc/XN76-JXWS] (last accessed April 14, 2022) (stating that Dominion Voting Systems ultimately purchased the Diebold voting property following Department of Justice antitrust action).

The state of Maryland still does not use any voting machines created by Diebold's successor, though California does.[81]

Requiring that vendors open at least portions of equipment source code to the public as a condition of use in federal elections would serve a number of ancillary benefits that might make this proposal more politically palatable. It would prevent a maelstrom of ultimately useless litigation.[82] It would help to ensure that software is functional and secure.[83] And it would also help to reduce public suspicion by allowing individual voters to directly inspect code function.[84] Above all, it would reduce the amount of ambiguity available for use by either highly zealous advocates or dishonest and bad faith actors not captured by the attorney disciplinary process.[85]

III. A DIFFERENT LINE, DRAWN FOR A DIFFERENT PURPOSE

The issue of economic incentives that make the line discussed in Part II difficult to draw can be leveraged to quickly remove disfavored technology from the marketplace. The worst of that technology is the Direct Recording-Electronic (DRE) voting machine.[86] Such machines were initially attractive to election administrators because their design provides certain accessibility solutions to voters with disabilities.[87] Along with the accessibility advantages, however, they introduced a number of technical vulnerabilities exploitable by malicious actors,[88] as well as a significant problem of election outcome verification.[89] By centering the voting mechanism in software processes, DRE machines ensured that ballots are cast without a paper trail.[90] Ergo, voting on a DRE machine does not create a physical artifact directly memorializing the voter's intent. Because the machine creates no physical record of the voter's intent, the software and the election results are irrevocably intertwined.[91] There is no way to separate the software from the election results, which makes it impossible to independently verify

[81] *See Verified Voting*, THE VERIFIER, https://verifiedvoting.org/verifier/#mode/search/year/2022/state/24/make/Dominion%20Voting%20Systems [https://perma.cc/85TJ-NJH8] (last accessed April 14, 2022) (stating that Maryland does not use Dominion machines).

[82] *See supra* note 66–68 and accompanying text.

[83] *Cf. infra* Part III.

[84] *See, e.g.*, *supra* note 40–43.

[85] *Cf. supra* note 23.

[86] Blaze, *supra* note 19, at 513 ("From a security perspective, by far the most problematic and risky class of electronic voting systems are those that employ Direct Recording-Electronic (DRE) machines.").

[87] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *supra* note 22, at 78.

[88] *See*, *e.g.*, Blaze, *supra* note 19, at 514 ("The design of DREs makes them inherently difficult to secure and also makes it especially imperative that they *be* secure.").

[89] Ronald L. Rivest and John Wack, *On the Notion of "Software Independence" in Voting Systems*, PHIL. TRANSACTIONS ROYAL SOC'Y 3759, at 3760 (2008) ("A pure DRE voting system produces only electronic cast ballot records, which are not directly observable or verifiable by the voter. Consequently, no meaningful audit of the DRE's electronic records to determine their accuracy is possible.").

[90] *Id.*

[91] *See generally id.* for an argument that voting systems should be "software independent" to resolve this issue.

election tallies presented by these machines. And, although technological solutions have attempted to resolve the problem, in practice they are unreliable.[92] The National Academies of Sciences, Engineering, and Medicine have declared the machines "subject to technological obsolescence."[93]

Despite this, it is not clear when such machines will be fully discharged from service. States began banning certain models of the machines about fifteen years ago, roughly when security issues made them subject to public attention.[94] But vendors continue to provide them. And they still have takers. For instance, the Hart InterCivic Verity Touch—a DRE machine which is not even compatible with the flawed attempts to ameliorate concerns with the technology—is still in use in forty-five Texas counties. And in forty-one of those, *all* voters must use the machine.[95] In order to speed such machines' removal from service, the federal legislature could declare that all DRE machines brought to market must open the entirety of their source code to the public. Such a result might—depending on the stringency of the legislature's mandate and the composition of the code—result in varying outcomes. All could be expected, however, to hasten removal of the machines from the market and therefore increase the general trustworthiness of machines in service.[96]

The precise impact of such legislation would depend on a particular vendor's product offerings. For instance, if a voting machine vendor currently has both DRE and non-DRE machines on the market with significantly overlapping code bases, the vendor might determine it is preferable to simply remove the DRE machine from the market to keep the code secret. Alternatively, however, where such an arrangement is not in place, a vendor might continue to market and sell its DRE machine but decline to invest in research and development. In such an instance, election officials might discard the machines if vulnerabilities were disclosed.

Any vendor could also be expected to pay additional attention to any legal exposure emanating from use of the machine. If the legislature declined to extend the moratorium on litigation—discussed in Part II—to DRE machines, a vendor

[92] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *supra* note 22, at 78-79; *see also*, Appel, *supra* note 37, at 527 ("VVPAT is not an adequate solution: in practice, the vast majority of voters do not verify the paper printout—it is 'voter verifiable' but not 'voter verified'; and the few who do inspect the VVPAT cannot safeguard the votes of their fellow voters who do not.").

[93] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *supra* note 22, at 78.

[94] Philip J. Peisch, Note, *Procurement and the Polls: How Sharing Responsibility for Acquiring Voting Machines Can Improve and Restore Confidence in American Voting Systems*, 97 Geo. L.J. 877, 890–91, 893–94, 913 n.244 (2009) (stating that Maryland in 2007 enacted legislation to replace a statewide DRE system, Florida passed similar legislation the same year, and California's Secretary of State decertified certain DRE machines; stating also that an argument for decentralized voting contracting is reinforced by "public uproar about security of DRE machines").

[95] *See Verified Voting*, *supra* note 81.

[96] *See also Privatizing Democracy, supra* note 34, at 754 ("When voting technology in one jurisdiction—say Miami-Dade County, Florida—fails to register votes or lacks the processes by which to verify them, the validity of other jurisdictions' election results are similarly thrown into question.").

might well decide it not worthwhile to continue selling the machine. In jurisdictions where the vendor leases rather than sells its products outright,[97] the vendor might similarly desire to call in its leases as soon as possible. Ultimately, we should expect that a product with disclosed code not supported by its vendor will quickly cycle out of service, whether for reason of fragility or legal liability.

Additionally, some of the political challenges discussed in Part I might be avoided here. Because the drawing would be made as to machine types—rather than portions of source code—the line would be necessarily clean and comprehensive. Legislators would have little difficulty explaining the reason for inclusion or exclusion of machines in the disfavored group. And because the machines have been disfavored for some time, it seems unlikely that their removal would create political backlash in comparison with any given policy decision. The removal of DRE machines from the market, then, appears to be achievable in a straightforward manner by implementation of the proposed legislative tool.

Even if the use of these machines is already so rare as to have marginal—or non-existent—potential impact on professional election watchers' confidence in the final tally, their removal should be a priority. After all, this paper argues for reforms targeting the dangers of exploitable ambiguity in our election processes. Where machines are in use with the extensive security issues detailed above, removal of those machines from service should take with them a corresponding argument against the validity of elections.

IV. PERCEIVED INADEQUACIES OF THE SOLUTION PROPOSED

A series of potential issues with the legislative plan discussed in this paper have already been noted and—to varying extents—addressed. The line-drawing issues presented to the legislature will be difficult and require significant input from experts in the field. The security risk connected with opening source code presented by Professor Nou is well-taken, but—in the current political climate—should not be overemphasized to undermine amelioration of other risks.[98] Three additional potential challenges to implementation of this solution should also be noted.

First, this Note proposes to make the source code to election equipment more broadly available in part because of foreign governments' apparent unauthorized access to that same equipment. It does seem odd to suggest that a problem of undue access should be solved by way of additional disclosure. However, keeping the source code to this technology closed has clearly been ineffective. If nothing

[97] *See, e.g.*, *id.*, at 767 (stating that in 2009, "[m]any counties in Rhode Island, Maryland, and a few other states" had leased election equipment from vendors).

[98] But even true open-source systems are not necessarily more secure. *See*, *e.g.*, Lucas Laursen, *What Open Source Technology Can and Can't Do to Fix Elections* IEEE SPECTRUM (27 April 2020) https://spectrum.ieee.org/what-open-source-technology-can-cant-do-fix-elections [https://perma.cc/2YCP-39Y6] ("Opening the source may enable some oversight, but it won't assure it on its own.").

else, opening the source code might make it slightly more likely the courts will be able to sift the wheat from the chaff in future election challenges.

Second, a reader may contemplate the public/private partnership discussed above and decide voting technology is a hopeless mess. They might instead propose that this could be an excellent area for the United States government to act more directly. After all, if the government can create an atomic bomb, build the Lincoln Tunnel, and put a man on the moon, it should be capable of building a secure, accurate and trustworthy voting machine. But a restoration of popular faith in the electoral process should not wait until government design and implementation of a secure voting infrastructure can become a political reality. And, if that day ever arrives, the courts will still likely be faced with litigants looking to make the most of the facts available to them.

Third, a reader might think that attorney's ethical rules are the most appropriate vehicle for resolving fallout from the Trump-election litigation as well as future litigious challenges to election results. Under this reasoning, it is best to let sleeping dogs lie. And this may be so. But there are some types of legal arguments that could undermine democratic ideals but that are not captured by the *Model Rules of Professional Conduct*.

This is because attorneys' ethical responsibilities are directed, on the one hand, to their clients,[99] and on the other hand, to the country's legal system.[100] The *Model Rules* require that attorneys practice diligent representation and note that such representation does not "preclude the treating of all persons involved in the legal process with courtesy and respect."[101] But the attorney must ultimately make their own decisions as they balance the interest of diligence against the interest of democracy. Meanwhile, a client seeking to undercut democracy through the courts can shop for attorneys, disregarding those whose ethical scruples are too great. Those retained might eventually become the recipients of disciplinary action. Yet the savvier bad-faith client—and their attorney—can revel in the ambiguity created by a national electoral system built upon private contracts and protected from public disclosure.

[99] *E.g.*, MODEL RULES R. 1.3 cmt. 1 ("A lawyer should pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to the lawyer, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor. A lawyer must also act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client's behalf.")

[100] Jefferson, *supra* note 5, at 131–32 ("False statements intended to foment a loss of confidence in our elections and resulting loss of confidence in government generally damage the proper functioning of a free society. When those false statements are made by an attorney, it also erodes the public's confidence in the integrity of attorneys admitted to our bar and damages the profession's role as a crucial source of reliable information. It tarnishes the reputation of the entire legal profession and its mandate to act as a trusted and essential part of the machinery of justice." (quoting *In re Giuliani*, 146 N.Y.S.3d 266, 283 (N.Y. App. Div. 2021))).

[101] MODEL RULES R. 1.3 cmt. 1.

CONCLUSION

The fallout of the 2020 election has further clarified the extent of the many dangers presented by our country's continued use of untrustworthy voting technology. By allowing the use of such machines—and by making private the full extent of *most machines'* shortcomings—we continue to court the loss of popular faith in the electoral process. With this loss of faith comes a corresponding loss of the security promised by a democracy that provides peaceful resolution to political disagreements. We should not think little of the risk we undertake.

By opening the source code of voting machines to the public, we might have opportunity to slowly rebuild faith in the electoral process and restore our strained democracy. To do so would require grappling with a new set of challenges and risks. The legislature should seriously consider those risks, but always in light of the dangers likely to be exacerbated by inaction. If Congress moves forward with the solution proposed, it should implement the corresponding moratorium on backward-facing litigation, which is foundational to ensuring that the proposed solution serves as an aid, rather than an impediment, to the restoration of trust in the democratic process. Congress should then weigh seriously the practical implications of its line-drawing decision.

Whatever path Congress decides to take, it must resolve the ongoing crisis of democracy. The tension between candidates' (and their litigators') interests on the one hand and that of the voting public on the other must not be ignored. Four years ago, the National Academies of Sciences, Engineering, and Medicine provided a warning: "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."[102] The consequences of failure to secure such confidence should by now be overwhelmingly apparent. It will not do to enter yet another national election cycle without having addressed the importance and immediacy of voters' legitimate interests in transparency.

[102] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *supra* note 22, at 124 (emphasis added).