SMU Law Review Forum

Volume 76 Article 6

10-2023

Redefining "No Evidence of a Breach" in Election Security

Yunsieg P. Kim
University of Missouri School of Law

Author(s) ORCID Identifier:

https://orcid.org/0000-0001-6748-8838

SMU Law Review Forum

Volume 76 2023 130-149

REDEFINING "NO EVIDENCE OF A BREACH" IN ELECTION SECURITY

Yunsieg P. Kim[*]

ABSTRACT

For legal purposes, we rightly understand the lack of evidence to mean a lack of existence. For example, many candidates in the 2022 elections baselessly claimed that the 2020 presidential election was stolen. But, absent evidence of systemic fraud, the law correctly determines that President Biden was duly elected. If the law entertained any outlandish assertion regardless of evidentiary support, accusers could peddle whatever claims they please, forcing the accused to disprove them. Similar to the legal understanding of "no evidence," many appear to believe that no evidence of a security breach in our voting equipment indicates no breach. For example, in the run-up to the 2022 elections, Georgia's Secretary of State Brad Raffensperger "spent months voicing skepticism that . . . a security breach ever occurred" in Coffee County's voting machines, arguing that "[t]here's no evidence of any of that" and therefore that "[i]t didn't happen."

A lack of evidence is rightly equivalent to a lack of existence, for legal purposes. But, for security purposes, no evidence of a breach does not necessarily mean no breach because security breaches can occur without the target's knowledge. Indeed, the more competent the infiltrators are, the more likely they are to commit breaches undetected. The Allies taught the world this lesson in World War II, when they infiltrated the encrypted communications of the Axis powers without being exposed. To this day, it remains an axiomatic rule of cyber security practice that one should never interpret the lack of

DOI: https://doi.org/10.25172/slrf.76.1.6

[*] Visiting Assistant Professor of Law, University of Missouri School of Law; Judicial Law Clerk, United States Court of Appeals for the Ninth Circuit (2021–22); J.D., Yale Law School; Ph.D. in Political Science, University of Michigan; M.S. in Cyber Security, New York University Tandon School of Engineering. I thank Jacob Eisler and Sandra Sperino for their advice and guidance.

evidence of a security breach to mean no breach. Shortly after Raffensperger claimed that a breach did not happen because there was no evidence, it was revealed that voting machines in Coffee County had been breached.

This Article calls for a bifurcated understanding of "no evidence of a breach" in the context of elections. For election fraud claims, we should continue to take no evidence to mean no fraud. But for evaluating the security of our election infrastructure, officials and legal scholars must understand that a breach can still occur despite the lack of evidence of a breach. I argue that the widespread conflation of no evidence of a breach and no breach is a frequently overlooked obstacle to election security reform. If one interprets no evidence of a breach as no breach, both the public and the politicians who represent them can rationalize not spending money on updating voting equipment as long as there is no definitive evidence that it was breached. Persuading the public of the fact that security breaches can occur despite the lack of evidence, while also showing why no evidence must still be interpreted as no existence for legal purposes, is a critical challenge that scholars must meet in order to effect meaningful election security reform.

INTRODUCTION

As any reasonable lawyer knows, the lack of evidence is legally equivalent to the lack of existence. For example, an unreasonable lawyer might claim without evidence that "illegal ballots [for President Biden] were being surreptitiously retrieved from suitcases hidden under a table" and counted in the 2020 presidential election.[1] In the 2022 elections, many candidates for offices that would oversee elections, such as governor or secretary of state, endorsed similar unfounded claims about President Biden's election in 2020.[2] But, absent any evidence of systemic fraud, the law correctly determines that President Biden was duly elected.[3] If the law entertained any outlandish assertion regardless of evidentiary support, accusers could peddle whatever claims they please, forcing the accused to disprove them. If the accused bore the burden to disprove, election officials would be dragged to court every day to try to affirmatively disprove every allegation of voter fraud imaginable—something that they are effectively being forced to do in the court of public opinion.[4]

Perhaps unsurprisingly, both the federal and state governments have applied this legal understanding of "lack of evidence" beyond election fraud claims to

1. *In re* Giuliani, 197 A.D.3d 1, 18 (N.Y. App. Div. 2021) (per curiam).

2. *See* Miles Parks, *Election Deniers Performed Especially Poorly in Races to Oversee Voting in Key States*, NPR (Nov. 19, 2022, 5:01 AM), https://www.npr.org/2022/11/19/1137129319/secretary-of-state-election-denialism-underperformed [https://perma.cc/8ZLE-52CL].

3. *In re Giuliani*, 197 A.D.3d at 15 n.9 ("[N]o evidence of widespread fraud was discovered" in three audits of Georgia's election results).

4. *See, e.g.*, Adam Edelman, *Beleaguered Wisconsin Elections Officials Seek New Office to Fight Misinformation*, NBC NEWS (Sept. 1, 2022, 5:19 PM), https://www.nbcnews.com/politics/beleaguered-wisconsin-elections-officials-seek-new-office-fight-misinf-rcna45950 [https://perma.cc/6VZ7-XBHW].

election security practices. For example, in response to known security flaws in voting machines, officials have reassured the public that "[t]here is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised."[5] Many scholars and other commentators appear to take such statements to mean that voting machines and other equipment were, in fact, not compromised.[6] As a matter of both law and common sense, that interpretation is understandable, especially given the need to counter people who act in bad faith seeking to profit from deceiving the public.[7]

However, as a matter of security practice, no evidence of a breach is not the same thing as no breach. In fact, best practices strongly advise against interpreting no evidence of a breach to mean no breach. A perennial occurrence in software development is the zero-day vulnerability, which is a security weakness that malicious actors learn of before anyone else does, including the developer.[8] The oblivious software developer might tell consumers in good faith that it has no evidence of a vulnerability in its product, and consumers would likely believe the developer. After all, many commentators appear to conflate no evidence of a breach and no breach,[9] and the developer has a strong incentive to ensure that its own product is secure. But, unbeknownst to the developer, malicious actors may well have already exploited the vulnerability. This is what happened with the Stuxnet computer worm, which existed "as early as

5. Press Release, Cybersecurity & Infrastructure Security Agency, Joint Statement from Elections Infrastructure Government Coordinating Council & The Election Infrastructure Sector Coordinating Executive Committees (Nov. 12, 2020) [hereinafter CISA Statement], https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election [https://perma.cc/K8VU-RLJB]; *see also Vulnerabilities Affecting Dominion Voting Systems ImageCast X*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (June 3, 2022) [hereinafter *CISA Advisory*], https://www.cisa.gov/uscert/ics/advisories/icsa-22-154-01 [https://perma.cc/UU8A-VS2S] ("CISA has no evidence that these vulnerabilities [in voting machines] have been exploited in any elections."); *2022 Texas Election Security Update*, TEX. SEC'Y STATE (last visited Apr. 3, 2023, 7:52 PM), https://www.sos.state.tx.us/elections/conducting/security-update.shtml [https://perma.cc/L2TR-QCF5] ("There is no evidence that any voting or voter registration systems in Texas were compromised before the 2016 Election or in any subsequent elections.").

6. *See, e.g.*, Scott J. Shackelford et al., *Making Democracy Harder to Hack*, 50 U. MICH. J.L. REFORM 629, 642 (2017) ("[T]here is no evidence that any voting machines have been hacked during a U.S. election . . . [V]oting machines have not yet been the subject of malicious activity . . . ."); Ellen Chang, *Local Voting Locations Spared From Hackers*, THESTREET (Nov. 7, 2022, 11:16 AM), https://www.thestreet.com/technology/local-voting-locations-spared-from-hackers [https://perma.cc/G7UQ-7FTK] (interpreting no evidence of a breach to mean that voting machines were "[s]pared").

7. *See, e.g.*, Aaron Blake, *Sidney Powell's Tucker Carlson-esque Defense: 'Reasonable People' Wouldn't Take Her Wild Voter-Fraud Claims as Fact*, WASH. POST (Mar. 23, 2021, 11:06 AM), https://www.washingtonpost.com/politics/2021/03/23/sidney-powells-tucker-carlson-esque-defense/ [https://perma.cc/T7DR-UZ4C] (a former attorney for ex-President Trump alleging an "international conspiracy involving Venezuela, Hugo Chavéz and other foreign counties" to steal the 2020 presidential election, and arguing in court that "'reasonable people' would not take her claims about widespread election fraud as fact.").

8. *See* Sushil Jajodia & Massimiliano Albanese, *An Integrated Framework for Cyber Situation Awareness*, *in* THEORY AND MODELS FOR CYBER SITUATION AWARENESS 29, 39 (Peng Liu et al. eds., 2017).

9. *See* Shackelford, *supra* note 6 and accompanying text.

November 2005"[10] and is thought to have compromised more than a thousand nuclear facilities[11] before being fixed by Microsoft in 2010.[12]

Consequently, it is a cornerstone of security practice to not dismiss the possibility of a breach even when there is no evidence. For example, in 2018, when a bug caused Twitter users' passwords to be stored in the company's own servers unencrypted, "Twitter advised all 330 million of its users to update their passwords," even though it "found no evidence of a breach or misuse of these passwords."[13] The fact that one should not understand no evidence of a breach to mean no breach is a lesson that the United States and its allies once taught their adversaries more than half a century ago. During World War II, U.S. intelligence decrypted the Japanese imperial military cipher "Purple"[14] and acquired "valuable, and often decisive" intelligence from listening in on Japanese communications. But, "[t]he Japanese never grasped what was happening"[15] because the United States understood the importance of "keep[ing] the enemy from realizing [that] his cipher is broken."[16] Nazi Germany was also "invincibly confident" that its military encryption technology "could never be broken," but "all through the war . . . the British were reading their messages."[17]

Yet, in the present day, the U.S. government erroneously applies the legal understanding of no evidence of a breach (as no breach) to election security. As detailed in Part I, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) urged a federal court to block a planned public disclosure of an expert witness's report demonstrating vulnerabilities in Georgia's voting machines.[18] This was because the report, according to CISA, "even in redacted form, could, in the event any vulnerabilities ultimately are identified, assist malicious actors and thereby undermine election security."[19] The court agreed that releasing even a redacted report "into the public domain just 89 days before the 2022 General Election could invite hacking and intrusion efforts."[20]

10. MARILYN WOLF, HIGH-PERFORMANCE EMBEDDED COMPUTING 408 (Todd Green & Nate McFadden eds., 2d ed. 2014).

11. *See* CHARLES H. ANDERTON & JOHN R. CARTER, PRINCIPLES OF CONFLICT ECONOMICS: THE POLITICAL ECONOMY OF WAR, TERRORISM, GENOCIDE, AND PEACE 416 (2d ed. 2019).

12. *See* Makkuva Shyam Vinay & Manoj Balakrishnan, *A Comparison of Three Sophisticated Cyber Weapons*, *in* MANAGING TRUST IN CYBERSPACE 389 (Sabu M. Thampi et al. eds., 2013).

13. ABBAS MOALLEM, UNDERSTANDING CYBERSECURITY TECHNOLOGIES: A GUIDE TO SELECTING THE RIGHT CYBERSECURITY TOOLS 14 (2022).

14. Michael Kernan, *Enigma Under Glass*, WASH. POST (Mar. 19, 1981), https://www.washingtonpost.com/archive/lifestyle/1981/03/19/enigma-under-glass/0e807109-6379-4fb2-acf2-88ec38170704/ [https://perma.cc/4NKK-R35S].

15. RONALD LEWIN, THE AMERICAN MAGIC: CODES, CIPHERS, AND THE DEFEAT OF JAPAN 153 (1982).

16. Kernan, *supra* note 14.

17. *Id.*

18. Notice at 5, Curling v. Raffensperger, No. 1:17-CV-2989-AT, 2020 WL 6065087 (N.D. Ga. filed Feb. 10, 2022), ECF No. 1314.

19. *Id.* at 1.

20. Order on Motion to Lift the Stay at 16 n.6, *Curling*, No. 1:17-CV-2989-AT, 2020 WL 6065087, ECF No. 1453.

The implied hope that malicious actors will not learn of these vulnerabilities in voting machines if we hide them neglects the possibility that malicious actors already know of them but are "keep[ing] the[ir] enemy from realizing"[21] that our systems are already breached. Tech firms are usually not so naïve as to hide security vulnerabilities in the hopes that no one finds out. Instead, "Google, Facebook, and Microsoft—operate bug bounty programs," which award "researchers that discover flaws" in those companies' security systems.[22] "Facebook paid $880,000 in 2017 and Google paid out almost $3M" in bug bounties.[23] Yet, far from "leveraging the power of . . . crowdsourced security" through bug bounties,[24] the Department of Justice announced only in May 2022 that "good-faith security research" including research for the "correction of a security flaw or vulnerability," should not be prosecuted under the Computer Fraud and Abuse Act (CFAA).[25] Plainly, this policy is far from a guarantee and can easily be overturned by a future administration.

This Article calls for a bifurcated understanding of what "no evidence of a breach" means in the context of elections. For election fraud claims, we should continue to take no evidence to mean no fraud. But for evaluating the security of our election infrastructure, government officials and legal scholars must stop conflating "no evidence of a breach" and "no breach." I argue that interpreting "no evidence" to mean "no breach" in the context of election security undermines efforts to enhance election security in two ways. First, it removes what meager sense of political urgency there is to update our aging election infrastructure. Second, telling voters to interpret "no evidence of a breach" as "no breach" undermines the public's already low confidence in elections.

First, the view that "no evidence of a breach" means "no breach" gives officials an excuse not to address security vulnerabilities in our election infrastructure under the rationale that there is no need to fix anything if nothing was breached. In the run-up to the 2022 elections, Georgia's Secretary of State Brad Raffensperger "spent months voicing skepticism that . . . a security breach ever occurred" in Coffee County's voting machines, arguing that "[t]here's no evidence of any of that" and thus that "[i]t didn't happen."[26] While this reasoning is sound in a strictly legal sense, it is not from a security perspective: the fact

21. Kernan, *supra* note 14.

22. Ryan Ellis et al., *Fixing a Hole: The Labor Market for Bugs*, *in* NEW SOLUTIONS FOR CYBERSECURITY 129, 132 (Howard Shrobe et al. eds., 2018).

23. Sai Krishna Kothapalli, *The World of Bug Bounties—the Indian Scenario*, *in* CYBER SECURITY IN INDIA: EDUCATION, RESEARCH AND TRAINING 97, 98 (Sandeep Shukla & Manindra Agrawal eds., 2020).

24. *Id.*

25. Press Release, Department of Justice, Department of Justice Announces New Policy for Charging Cases Under the Computer Fraud and Abuse Act (May 19, 2022), https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act [https://perma.cc/C46Z-RQ4M].

26. Amy Gardner et al., *Georgia to Replace Voting Machines in Coffee County After Alleged Security Breach*, WASH. POST (Sept. 23, 2022, 5:00 PM), https://www.washingtonpost.com/investigations/2022/09/23/coffee-county-georgia-election-machines/ [https://perma.cc/4LBE-ZBHU].

that the target is unaware of a breach does not mean that it did not occur. It was revealed six weeks before the 2022 elections that voting machines in Coffee County were indeed breached despite Raffensperger's past claim that it would be "virtually impossible for votes to be manipulated without detection," forcing his office to replace the voting machines.[27] Although late is better than never, late is still after the breach, which may be too late.

Second, understanding "no evidence of a breach" as "no breach" undermines the public's already low confidence in what officials and experts say about election security.[28] While there is indeed no evidence that our election infrastructure was sufficiently breached to compromise any election results, there is plenty of evidence that our election infrastructure is broken. The press has reported for years about appalling incidents of malfunctions, resulting in incidents such as voting machines showing that "a Democrat[] had just 164 votes out of 55,000 ballots" when in fact he got 26,142,[29] or "[m]ore than 80 voting machines in Detroit malfunction[ing] . . . resulting in ballot discrepancies in 59% of precincts."[30] In this environment, saying things like "Louisiana elections [are] secure, but voting machines [are] still vulnerable"[31] is likely to sound oxymoronic to voters. At the very least, the statement does not inspire confidence—akin to telling passengers on a plane that there is nothing to worry about because the captain only *nearly* flew headfirst into a mountain.

It is easy to see why many people take "no evidence of a breach" to mean "no breach" in the context of election security. To legal practitioners, the legal equivalence between "no evidence" and "no existence" probably appears just as self-evident and unchanging as gravity. But we may have neglected that this rule, while axiomatic in law, doesn't work outside the law—just as gravity fades away in outer space. We can pitch reasonable ideas to enhance election security all we want, from buying new voting machines to going back to old-fashioned paper ballots marked with pens.[32] But as long as people understand "no evidence

27. *Id.*

28. *See, e.g.*, Ann Ravel, *A New Kind of Voter Suppression in Modern Elections*, 49 U. MEM. L. REV. 1019, 1024 (2019) ("[T]he failure of some state and federal election authorities to disclose hacking incidents or to respond without taking affirmative steps to assure security of the voting machines has led to distrust in the systems themselves."); Jane R. Bambauer & Derek E. Bambauer, *Information Libertarianism*, 105 CALIF. L. REV. 335, 368 (2017) ("[A] study of the 2008 presidential election found [that] . . . people believed that pollsters misrepresented true attitudes. . . .").

29. Nick Corasaniti, *A Pennsylvania County's Election Day Nightmare Underscores Voting Machine Concerns*, N.Y. TIMES (Nov. 30, 2019), https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html [https://perma.cc/BZ8J-3G5T].

30. Charlotte Alter, *Detroit Voting Machine Failures Were Widespread on Election Day*, TIME (Dec. 13, 2016, 8:33 PM), https://time.com/4599886/detroit-voting-machine-failures-were-widespread-on-election-day/ [https://perma.cc/C4VW-5FDP].

31. Wesley Muller, *Louisiana Elections Secure, but Voting Machines Still Vulnerable*, LA. ILLUMINATOR, (Nov. 11, 2022, 9:03 AM), https://lailluminator.com/2022/11/11/louisiana-elections-secure-but-voting-machines-still-vulnerable/ [https://perma.cc/A2NJ-CAA8].

32. *See id.* (stating that a commission chaired by the Louisiana Secretary of State chose "hand-marked paper ballots" as an option for reforming the state's election system, and that his attempts to buy new voting machines failed).

of breach" to mean "no breach" in the context of election security, a fix will likely not materialize because voters will tell themselves that there is no need to fix anything, since nothing was breached. As many have said, the first step in fixing any problem is to recognize that there is one. I submit that the first step in election security is to recognize that "no evidence of a breach" should not be understood to mean "no breach."

I. BACKGROUND

"Low public confidence in U.S. election predates the tumultuous 2020 season."[33] Since *Bush v. Gore*, "[p]ublic confidence in election administration" is at "embarrassingly low levels" and "[e]lections more frequently result in litigation."[34] Such skepticism is supported by credible reports of failures in election infrastructure. For example, voting machines in a Pennsylvania county incorrectly showed that the Democratic candidate had "164 votes out of 55,000 ballots."[35] He had in fact won 26,142 votes, which was revealed only because the county kept paper backup ballots—prompting the county's Democratic Party chair to ask "if some of the numbers are wrong, how do we know that there aren't mistakes with anything else?"[36] In another Pennsylvania county, voting machines were accessed remotely "multiple times, most notably . . . the night before a federal election."[37] Although it was revealed that "an authorized county contractor working from home" was responsible, the incident appears sufficient to undermine officials' claims that voting machines cannot be remotely hacked because "the systems are not connected to the internet."[38]

More recently, major party candidates for offices overseeing election administration have latched onto such concerns and campaigned on baseless claims of *systemic* electoral fraud. For example, Republican nominees for secretary of state and governor in 2022 in states such as Nevada, Arizona, Pennsylvania, Wisconsin, and Michigan have claimed that "the 2020 election was corrupt or stolen."[39] Democratic candidates running for the same

33. Rebecca Green, *Election Observation Post-2020*, 90 FORDHAM L. REV. 467, 468 n.1 (2021).

34. Richard L. Hasen, *The Untimely Death of* Bush v. Gore, 60 STAN. L. REV. 1, 44 (2007).

35. Corasaniti, *supra* note 29.

36. *Id.*

37. Kim Zetter, *The Myth of the Hacker-Proof Voting Machine*, N.Y. TIMES (Feb. 21, 2018), https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html [https://perma.cc/P8UJ-KHZQ].

38. *Id.*

39. Sarah Smith, *Kari Lake Defeat: Did Democracy Win in US Midterms?*, BBC (Nov. 15, 2022), https://www.bbc.com/news/world-us-canada-63565226 [https://perma.cc/DJ2B-U3K7].

positions,[40] as well as scholars[41] and the press,[42] have argued that these claims of systemic electoral fraud are baseless, an approach which seems to have been vindicated by the fact that every candidate for secretary of state and governor in those states who advanced claims of systemic election fraud lost,[43] while many Republican candidates for secretary of state and governor who rejected such claims "were easily re-elected."[44]

It is only natural that many people take a failure to demonstrate systemic fraud as legally equivalent to no fraud, because parties acting in bad faith should not be able to claim fraud without meeting the due burden of proof. But unlike the legal understanding of "no evidence," no evidence of a breach in the security context should not be taken to mean no breach because hackers have an incentive to commit breaches without being detected. Yet, the officials entrusted with the security of our election system apparently operate under the assumption that no evidence of a breach means no breach—even in response to credible reports of security vulnerabilities from genuine experts.

Officials' erroneous understanding of no evidence of a breach as no breach is particularly well demonstrated by a federal case from Georgia. In 2017, a group of voters and election security advocates sued state officials, including the secretary of state, alleging that security vulnerabilities in voting machines had compromised the special election in Georgia's 6th congressional district held that year between Republican Karen Handel, the winner, and Democrat Jon Ossoff, the runner-up and eventual U.S. Senator.[45] A witness for the plaintiffs was Dr. J. Alex Halderman, a professor of computer science at the University of Michigan who studies election security[46] and has testified before Congress on

40. *Cf.* Karina Elwood, *As Judges Rule Against Dan Cox, Md. Dems Press Him to Accept Results*, WASH. POST (Sept. 29, 2022, 7:17 PM), https://www.washingtonpost.com/dc-md-va/2022/09/29/maryland-democrats-criticize-cox-election/ [https://perma.cc/RWV8-N256] ("Maryland Democrats . . . launched a campaign . . . casting [Republican gubernatorial candidate Dan] Cox's stance as dangerous to democracy, focusing on his denial of the 2020 presidential election results.").

41. *See, e.g.*, Donie O'Sullivan, *A Glitch in Maricopa, a Gift to Election Deniers*, CNN (Nov. 9, 2022, 7:05 PM), https://www.cnn.com/2022/11/09/politics/election-deniers-maricopa-county-arizona-midterms/index.html [https://perma.cc/KGZ5-5UM8] (quoting a report from the University of Washington stating that "honest human errors can be opportunistically exploited to imply intentionality and to support unfounded narratives of . . . fraud, undermining the legitimacy of electoral outcomes" but "as research shows, election fraud is exceedingly rare and such mistakes are unlikely to impact election outcomes.").

42. Cecilia Kang, *5 Unfounded Claims About Voting in the Midterm Elections*, N.Y. TIMES (Nov. 2, 2022), https://www.nytimes.com/2022/11/02/technology/midterm-elections-misinformation.html [https://perma.cc/XBH5-CN3K] (arguing that "voting machines aren't rigged" and that "ballot fraud isn't rampant.").

43. *See* Smith, *supra* note 39.

44. *See id.* ("It appears voters specifically rejected these candidates [advancing claims of systemic fraud] rather than their party. . . . In Georgia, Brian Kemp and Brad Raffensperger—who resisted pressure from Donald Trump to overturn the result in their state—were easily re-elected as governor and secretary of state.").

45. Amended Complaint at 4, *Curling*, No. 1:17-CV-2989-AT, 2020 WL 6065087, ECF No. 15.

46. Brief for J. Alex Halderman at 1–2, *Curling*, No. 1:17-CV-2989-AT, 2020 WL 6065087, ECF No. 260.

the matter.[47] Dr. Halderman was given access to the voting machines at issue[48] and, on July 12, 2021, filed with the federal district court a sealed report identifying various security flaws.[49] The parties released the full, unredacted report to CISA with the court's authorization.[50]

In addition, both parties requested that the court release a redated copy of the report to the public. The plaintiffs requested public disclosure of a redacted report within thirty days of the unredacted report's release to CISA so that "officials can secure the upcoming . . . elections,"[51] whereas "the State would prefer immediate (or as soon as practicable) release."[52] The parties did not explain why releasing the report to the public—as opposed to releasing the report only to the equipment manufacturers and officials who would implement fixes to any vulnerability—would enhance election security. But it is easy to see why public disclosure would help. Because "finding a bug in a large code base can be equivalent to finding a needle in a haystack," many developers "rely on the active participation of users to help . . . test new releases and verify bug corrections."[53]

But eight days after receiving the report, CISA urged the district court to deny the parties' joint request to release it to the public. The report, according to CISA, "even in redacted form, could, in the event any vulnerabilities ultimately are identified, assist malicious actors and thereby undermine election security."[54] The court agreed that releasing even a redacted report "just 89 days before the 2022 General Election could invite hacking and intrusion efforts,"[55] and held that it "would not likely publicly release the report prior to the full completion of the 2022 election cycle."[56] The district court held partly for the plaintiffs, issuing a preliminary injunction that would require officials to make certain changes to Georgia's election administration.[57] However, the Eleventh Circuit vacated the injunction and dismissed the rest of the state's appeal[58] and the Halderman report was not publicly released. Instead, CISA reviewed an unredacted copy of the Halderman report[59] and released a public advisory listing

47. *Election Security: Ensuring the Integrity of U.S. Election Systems: Hearing Before the H. Appropriations Subcomm. on Fin. Serv. and Gen. Gov't*, 116th Cong. (2019) (statement of Dr. J. Alex Halderman, Professor of Computer Science and Engineering, University of Michigan, Director, Michigan Center for Computer Security and Society).

48. Brief for J. Alex Halderman, *supra* note 46, at 3.

49. Order on Motion to Intervene at 1, *Curling*, No. 1:17-CV-2989-AT, 2020 WL 6065087, ECF No. 1453.

50. Order at 1, *Curling*, No. 1:17-CV-2989-AT, 2020 WL 6065087, ECF No. 1406.

51. Notice of Filing at 2, *Curling*, No. 1:17-CV-2989-AT, 2020 WL 6065087, ECF No. 1300.

52. Notice, *supra* note 18, at 3.

53. ALLEN TUCKER ET AL., SOFTWARE DEVELOPMENT: AN OPEN SOURCE APPROACH 130 (Richard LeBlanc ed., 2011).

54. Notice, *supra* note 18, at 1.

55. Order on Motion to Intervene, *supra* note 49, at 16 n.6.

56. *Id.* at 16.

57. Curling v. Raffensperger, 491 F. Supp. 3d 1289 (N.D. Ga. 2020), *vacated*, 50 F.4th 1114 (11th Cir. 2022).

58. Curling v. Raffensperger, 50 F.4th 1114 (11th Cir. 2022).

59. Notice, *supra* note 18, at 1–2.

several security flaws in the voting machines at issue as well as "[m]itigations to reduce the risk of [their] exploitation" that officials could implement.[60]

II. NO EVIDENCE OF A BREACH DOES NOT MEAN NO BREACH

CISA argued, and the district court agreed, that the Halderman report should not be publicly released, because disclosure would "assist malicious actors"[61] or "invite hacking . . . efforts."[62] The implied belief that hiding a security vulnerability will meaningfully reduce the likelihood of a breach assumes that hackers have not already exploited the vulnerability undetected. This is because, if a vulnerability has already been exploited, hiding it would not reduce the chances of a breach. This assumption that an undetected breach has not yet occurred would be impossible if officials already had evidence of a breach. Hence, the belief that hiding a vulnerability would reduce the likelihood of a breach requires understanding no evidence of a breach to mean no breach.

As discussed briefly in the introduction, it is only natural to interpret no evidence to mean that nothing happened, for legal purposes. But for security purposes, understanding no evidence of a breach as no breach is the last thing we should do because the more competent the infiltrators are, the more likely they are to commit breaches undetected. Recall that, during World War II, U.S. intelligence cracked the Japanese military cipher, Purple, without being detected.[63] While the United States obtained a large amount of actionable intelligence from listening in on what the Japanese believed were secure communications, the United States had to tread carefully when acting on that intelligence, for fear that the Japanese might notice that their security was breached:

> In 1943, the United States intercepted and decoded a Japanese message indicating that Admiral Isoroku Yamamoto, commander in chief of the Japanese Navy, would be visiting Japanese bases in the Solomon Islands on April 18, 1943. The message included precise times and locations, as well as the fact that Yamamoto's aircraft would be escorted by six fighters. Admiral Chester W. Nimitz, the U.S. commander in chief in the Pacific, had a tough decision to make. It was highly tempting to try to shoot down Yamamoto's aircraft, but doing so might tip off the Japanese [to the fact] that their codes were being read.[64]

Nimitz did eventually order U.S. forces to shoot down Yamamoto's aircraft, but when Yamamoto was killed, "[t]he Japanese concluded that Yamamoto had been the victim of a routine patrol [by U.S. fighters] and did not change their codes."[65] Clearly, "[t]he United States took a huge chance and got away with it"

60. *CISA Advisory*, *supra* note 5.
61. Notice, *supra* note 18, at 1.
62. Order on Motion to Intervene, *supra* note 49, at 16 n.6.
63. *See supra* notes 14–16 and accompanying text.
64. JAMES M. OLSON, FAIR PLAY: THE MORAL DILEMMAS OF SPYING 189 (2006).
65. *Id.*

by doing something that might have alerted the Japanese to the fact that their security was breached.[66] Just as the United States showed the world that infiltrators have every incentive to operate undetected, our enemies would likely conceal themselves if and when they do infiltrate our election infrastructure. Therefore, the fact that we have no evidence of our election infrastructure being breached should not be understood to mean that it was not actually breached.

But when it comes to election security in the present day, many officials seem to conflate no evidence of a breach and no breach. For example, CISA argued in the *Curling* case, and the court agreed, that the Halderman report should be concealed from the public because releasing it "could invite hacking and intrusion efforts."[67] As discussed, the belief that hiding a vulnerability would reduce the likelihood of a breach assumes that undetected breaches do not occur. Moreover, officials concealing evidence of security flaws undermines voters' *perception* of election security. Generally, hiding things raises suspicion. Hiding something that may indicate incompetence or negligence raises even more suspicion. Granted, such suspicion is not entirely fair in this case. It was the district court that decided to keep the Halderman report sealed, not the state, and the state apparently agreed with the plaintiffs that the report should be released to the public in some form.[68]

But contrary to what the court may have intended, hiding the report apparently exacerbated the "heated climate surrounding voting issues" and "ever heightening concerns about . . . cybersecurity attacks."[69] This is because media reports, even without any ill intent, often focus on the result (the fact that the Halderman report was hidden) at the expense of the reason (the report was sealed to preserve election security). For example, in an article titled "[s]ecret report finds flaw in Georgia voting system, but state in the dark," the *Atlanta Journal-Constitution* reported that the secretary of state "hasn't asked the court to disclose the report" and "[t]here's no sign that state election officials have done anything about the vulnerability."[70] A reasonable voter could take this to mean that officials are concealing evidence of incompetence, especially if the voter is unaware of the details of the litigation. Thus, even without implicating any actual election security issue, keeping the Halderman report sealed has apparently undermined voters' perception of election security.

Voters' perception of election security can be undermined even further when groups that openly spread conspiracy theories get involved. For example, in the run-up to the 2020 elections, Fox News Network and MyPillow spread baseless claims that Dominion, the manufacturer of the voting machines at issue, intentionally designed them to "shave[] off votes from . . . Trump and award[]

66. *Id.*

67. Order on Motion to Intervene, *supra* note 49, at 16 n.6.

68. Notice, *supra* note 18, at 3.

69. Order on Motion to Intervene, *supra* note 49, at 16 n.6.

70. Mark Niesse, *Secret Report Finds Flaw in Georgia Voting System, But State in the Dark*, ATLANTA J. CONST., https://www.ajc.com/politics/secret-report-on-georgia-voting-system-finds-flaws-but-state-shows-no-interest/YKFEET2WE5BBPJ7TYVOYMBTIKQ/ [https://perma.cc/5CVE-LJQ5] (Jan. 26, 2022).

them to Biden"; Dominion sued both for defamation.[71] Both companies moved unsuccessfully to intervene in the *Curling* case to obtain the Halderman report, arguing that it likely contains facts that pertain directly to Dominion's defamation suit against them.[72] The fact that the report remains under wraps would allow conspiracy theorists to claim that it confirms every outlandish claim they have made, and that is why officials are hiding it.[73] Had the court unsealed the report, speculations about what it *might* say could not be used to fuel conspiracy theories about systemic election fraud.

Setting aside the issue of voters' perception, however, some may argue that the decision to keep the Halderman report sealed did not undermine actual election security. The argument may be that, while the public did not get an opportunity, CISA reviewed the full report and published an online advisory describing the vulnerabilities in the voting machines at issue and the mitigation methods.[74] Thus, one might argue that publishing the advisory achieved the same effect in warning the relevant stakeholders about security flaws as releasing the report to the public would have done.

But such an argument misunderstands how security vulnerabilities are found and fixed. There is no reason to doubt that the CISA personnel who reviewed the Halderman report and published the online advisory describing vulnerabilities in Georgia's voting machines are both dedicated and competent. Nevertheless, bug hunting is akin to finding a needle in a haystack,[75] which is one of those tasks where a large crowd of laypeople often outperforms small teams of experts. The history of bug hunting is replete with examples of ordinary consumers exposing critical security flaws that the hardware or software manufacturer failed to find. One especially memorable example involved people breaching the fingerprint reader on the Samsung Galaxy S10 smartphone by using anything from "$3 gel cover screen[s]"[76] and "a clear silicone phone

71. Alison Durkee, *Murdoch Deposed: Here's What Fox Is Accused Of Lying About In Defamation Lawsuit Over 2020 Election*, FORBES, https://www.forbes.com/sites/alisondurkee/2022/12/13/rupert-murdoch-testifying-in-dominions-fox-news-defamation-lawsuit-here-are-the-false-2020-election-statements-featured-in-the-suit/?sh=5866f208228b [https://perma.cc/LAX4-MADM] (Jan. 19, 2023, 9:46 AM).

72. Order on Motion to Intervene, *supra* note 49, at 2, 17.

73. Jose Pagliery, *Judge's Election Nightmare Comes True: The MyPillow Guy Has Entered the Chat*, DAILY BEAST (Mar. 9, 2022, 7:26 PM), https://www.thedailybeast.com/judge-amy-totenberg-election-nightmare-comes-true-the-mypillow-guy-mike-lindell-has-entered-the-chat [https://perma.cc/87PX-RNU6] ("When Judge Totenberg took the rare step of sealing this expert report back in July, she did so out of concern that its release would fuel conspiracy theories. Totenberg refused to entertain ideas about releasing it to the public, saying she was 'at the end of my rope about that.' . . . Cybersecurity experts warned this continued secrecy would only draw more curiosity, an obvious case of the Streisand effect. But Totenberg stuck to her guns last month, keeping even a redacted . . . version of the report secret . . . . Now, [Mike] Lindell [CEO of MyPillow] has adopted this report as part of his conspiracy-riddled crusade.").

74. *See* Notice, *supra* note 18, at 1–2; *CISA Advisory*, *supra* note 5.

75. TUCKER ET AL., *supra* note 53.

76. Zak Doffman, *New Samsung Warning: Galaxy S10 Fingerprint Reader Hit By 'Security Breach'*, FORBES (Oct. 14, 2019, 2:05 AM), https://www.forbes.com/sites/zakdoffman/2019/10/14/serious-samsung-security-warning-for-millions-of-galaxy-s10-owners/?sh=63817688312a [https://perma.cc/2WVE-Z5WF].

case"[77] to even a sweet potato.[78] This is despite the fact that the experts at Samsung have a strong incentive to prevent such vulnerabilities.

Even though people do not exactly carry voting machines around in their pockets like cell phones, the strategy of crowdsourced bug hunting can be applied equally effectively to both. That is, just as smartphone users discovered and reported a vulnerability that Samsung was unaware of, had the Halderman report been released to the public, people may have discovered a vulnerability that Dr. Halderman or CISA failed to catch. Moreover, the likelihood of the public discovering something that was overlooked would have increase if they are given further incentives. Thus, it should come as no surprise that many firms have bug bounty programs, which pay users who report bugs.[79]

The efficacy of bug bounties is not merely theoretical. One firm in particular showcased the power of crowdsourced bug hunting by having a bounty program for only some aspects of the same product, thus leaving that product more vulnerable to malicious actors in some respects than others. One of the various bounties offered to the public by Meta is the bug bounty for security vulnerabilities in their app products. "To be eligible for a bounty, [users] can report a security bug in one or more . . . Meta technologies" including Facebook, Instagram, and WhatsApp.[80] Meta's bug bounty program has "paid out more than $16 million" since 2011 and "awarded more than $2 million" in 2022 for "more than 750 [bug] reports."[81] In December 2022, Meta announced that it would pay up to $300,000 for each report of mobile remote code execution bugs,[82] which are a vulnerability that can affect "the [smartphone app] versions of Facebook . . . and WhatsApp."[83]

In addition to the bug bounty, Meta also offers a data abuse bounty, which "incentiviz[es] anyone to report apps collecting user data and passing it off to malicious parties to be exploited."[84] The data abuse bounty rewards users for reporting anyone "buying, selling, disclosing, transferring, or using Facebook or Instagram user data . . . in any manner prohibited by . . . terms governing the

77. Ron Amadeo, *Anyone Can Fingerprint Unlock a Galaxy S10–Just Grab a Clear Phone Case*, ARS TECHNICA (Oct. 17, 2019, 11:24 AM), https://arstechnica.com/gadgets/2019/10/galaxy-s10-fingerprint-reader-defeated-by-screen-protectors-phone-cases/ [https://perma.cc/2UVX-JP6X].

78. Lim On-yu, *'Unlock with Sweet Potato'. . . Samsung's Fingerprint Recognition Error Took a Big Hit*, ASIA ECON. (Oct. 19, 2019, 8:23), https://cm.asiae.co.kr/article/2019101908234435005 [https://perma.cc/A24X-MRSQ].

79. *See* Ellis et al., *supra* note 22.

80. *Meta Bug Bounty Program Info*, FACEBOOK, https://www.facebook.com/whitehat [https://perma.cc/3RWG-HLLF] (Nov. 21, 2022).

81. Neta Oren, *Looking Back at Our Bug Bounty Program in 2022*, META (Dec. 15, 2022), https://about.fb.com/news/2022/12/metas-bug-bounty-program-2022/ [https://perma.cc/DZL3-ESSC].

82. *Id.*

83. Jai Vijayan, *Meta Ponies Up $300K Bounty for Zero-Click Mobile RCE Bugs in Facebook*, DARK READING (Dec. 15, 2022), https://www.darkreading.com/vulnerabilities-threats/meta-300k-bounty-mobile-rce-vulnerabilities-facebook [https://perma.cc/4GK3-YPZF].

84. *Data Abuse Bounty Program*, FACEBOOK, https://www.facebook.com/data-abuse [https://perma.cc/B6CE-UB8A] (Apr. 9, 2018).

Facebook or Instagram platforms."[85] Whereas the bug bounty rewards reports of defective design features—such as software bugs that permit hackers to commit security breaches—the data bounty rewards reports of "data abuse," which does not have to exploit any security vulnerability. Indeed, Meta's data bounty terms redirect anyone who "believe[s] [to] have found a security vulnerability" to Meta's bug bounty page.[86] An example of data abuse that does not exploit any security flaw is selling data obtained through scraping, which refers to gathering large amounts of data (such as Meta user data) using a computer program.[87] Unlike Meta's bug bounty program, which covers WhatsApp,[88] WhatsApp is "[e]xplicitly out of scope" of its data bounty program.[89]

A recent incident shows that excluding WhatsApp from the data abuse bounty likely made it more vulnerable to data abuse. On November 16, 2022, a user claimed on a hacking community forum to be "selling a 2022 database of 487 million WhatsApp user mobile numbers."[90] The seller sold the "the US dataset for $7,000, the UK – $ 2,500, and Germany – $2,000."[91] The data "went on sale for 4 days," after which it was "distributed freely amongst Dark Web users."[92] The data appeared to be scraped from WhatsApp[93] and, according to analysis by the security firm Check Point Research, contained "360 million phone numbers from 108 countries."[94] Had Meta's data abuse bounty covered WhatsApp, this leak may have been avoided. The data abuse bounty has "no maximum"[95] and would likely have paid a large reward to prevent a leak of hundreds of millions of phone numbers. Thus, had the bounty covered WhatsApp, users who realized that numbers could be scraped might have alerted Meta so they could collect the bounty, thereby allowing Meta to implement fixes to prevent scraping, instead of scraping the data and selling it for only a few thousand dollars.

The lessons from bug bounties can easily be applied to election security. For example, U.S. authorities could disclose reports of vulnerabilities like the Halderman report in full and reward people to point out if the report (or experts

85. *Data Abuse Bounty Terms: Terms and Conditions*, FACEBOOK, https://www.facebook.com/data-abuse/terms/ [https://perma.cc/S2N5-AMHX] (Jan. 27, 2022).

86. *Id.*

87. *See* Rajeev V. Gundur et al., *Using Digital Open Source and Crowdsourced Data in Studies of Deviance and Crime*, *in* RESEARCHING CYBERCRIMES: METHODOLOGIES, ETHICS, AND CRITICAL APPROACHES 145, 150 (Anita Lavorgna & Thomas J. Holt eds., 2021) ("Data scraping . . . involves using an automated program to harvest data that others have collected or posted to form a dataset . . . .").

88. *Meta Bug Bounty Program Info*, *supra* note 80.

89. *Data Abuse Bounty Terms: Terms and Conditions*, *supra* note 85.

90. Jurgita Lapienytė, *WhatsApp Data Leaked - 500 Million User Records for Sale Online*, CYBERNEWS, https://cybernews.com/news/whatsapp-data-leak/ [https://perma.cc/6F4Y-8LJW] (Feb. 24, 2023).

91. *Id.*

92. Check Point Research Team, *Check Point Research Analyzes Files on the Dark Web and Finds Millions of Records Available*, CHECK POINT (Dec. 1, 2022), https://blog.checkpoint.com/2022/12/01/check-point-research-analyzes-files-on-the-dark-web-and-finds-millions-of-records-available/ [https://perma.cc/EV7H-28EV].

93. *See* Lapienytė, *supra* note 90.

94. *See* Check Point Research Team, *supra* note 92.

95. *Data Abuse Bounty Terms: Terms and Conditions*, *supra* note 85.

at agencies like CISA) missed anything. After all, the Department of Homeland Security—CISA's parent agency—offers bug bounties of up to $5,000 "to hackers who help the department identify cybersecurity vulnerabilities" within its own systems.[96] The Brazilian judiciary "[b]efore each election . . . invites researchers and software experts to look for vulnerabilities in the voting system" and even "tr[y] to penetrate the system."[97] CISA and the *Curling* court did the opposite, by keeping the report sealed under the hope that doing so would reduce the likelihood of a security breach. As discussed above, hoping that concealing vulnerabilities will reduce the likelihood of a breach assumes that no unknown breaches have occurred, which in turn assumes that no evidence of a breach means no breach.

I am not arguing that the *Curling* court's decision to keep the Halderman report under wraps was entirely baseless. Such a decision might even seem intuitively appealing: a reasonable person could believe that disclosing the report would cause at least some nefarious actors to learn about vulnerabilities in voting machines, which they would otherwise never have learned.

While concealing the report could reduce the number of nefarious actors who learn about those particular security vulnerabilities in voting machines, the point is not to reduce the total number of people who know of the vulnerabilities. It is to minimize the risk of those vulnerabilities actually being breached. The two things are clearly different because, if a large enough number of people already know of those vulnerabilities or have already breached them, preventing a few more people from learning of the vulnerabilities would not materially reduce the risk of a breach.

There is good reason to think that a critical mass of people already know how to breach voting machines, given that many white-hat hackers have shown how easy it is to do that. At a convention of hackers in 2018, organizers "packed a conference room . . . with voting machines and . . . asked civically-curious hackers to wreak havoc."[98] In just a few hours, "one hacker was essentially able to turn a voting machine into a jukebox, making it play music and display animations."[99] Given how easy it apparently is to breach our voting equipment, it is reasonable to assume that a large number of nefarious actors already know how to breach existing vulnerabilities in voting machines, if they have not done so already. Under these circumstances, keeping reports like the Halderman report hidden from the public would not really do anything to reduce the already high likelihood of a breach. That would merely prevent ourselves from

96. Geneva Sands, *US Government to Offer Up to $5,000 'Bounty' to Hackers to Identify Cyber Vulnerabilities*, CNN, https://www.cnn.com/2021/12/14/politics/dhs-bug-bounty-hackers-cyber-vulnerabilities/index.html [https://perma.cc/QX5R-66GP] (Dec. 14, 2021, 8:09 PM).

97. Juliana Gragnani & Jake Horton, *Brazil Election: Do Voting Machines Lead to Fraud?*, BBC (Oct. 3, 2022), https://www.bbc.com/news/63061930 [https://perma.cc/3CXT-7C9Z].

98. Donie O'Sullivan, *Election Officials' Concerns Turn to Information Warfare as Hackers Gather in Vegas*, CNN (Aug. 12, 2018), https://www.cnn.com/2018/08/11/politics/defcon-election-machine-hacking-vegas/index.html [https://perma.cc/RHL2-2ZTH].

99. *Id.*

exploiting the benefits of public disclosure, one of which is crowdsourced bug hunting in the form of bounties.

III. THE NECESSITY OF A NEW UNDERSTANDING OF "NO EVIDENCE OF A BREACH"

Part II has argued that our election security infrastructure is in dire need of a crowdsourced bug hunting approach, represented most typically by bug bounties. But academics will likely not be the ones to adopt that approach on behalf of the nation, or to finance any bug bounty. Part III presents one thing that academics can do to make this scenario more likely: propagate a new public understanding that no evidence of a breach should not be taken to mean no breach, specifically in the context of election security. I argue that this new public understanding would make the adoption of a crowdsourced bug hunting approach more likely because, as explained in Part II, the justification for hiding reports of security vulnerabilities from the public relies on the assumption that no evidence of a security breach means no breach.

It will likely be a challenge to propagate the understanding that, for security purposes, no evidence of a breach should not be taken to mean no breach. One reason is that many experts are used to the opposite understanding of "no evidence of a breach": as discussed in the introduction, no evidence of a breach means no breach for *legal* purposes. Both scholars and the media often repeat that understanding of no evidence of a breach to the public.[100] Given the public's familiarity with the legal understanding of no evidence of a breach, it may be difficult to convince them that "no evidence of a breach" in the security context means the opposite of the legal meaning. This challenge may be compounded by the public's general unfamiliarity with cyber security issues.[101]

The fact that the public is much more familiar with the legal understanding of no evidence of a breach might not be the only obstacle to propagating a different understanding of no evidence of a breach for the security context. The second challenge may be the fact that government officials and the public have a material incentive to understand no evidence of a breach of election security to mean no breach. That is, if one accepts that our election equipment could have been breached even if we are not aware of it, there is a greater urgency to keep that equipment up to date regardless of whether it is known to be breached. By contrast, if we can tell ourselves that no evidence of a breach means no breach, we can avoid paying for new equipment in perpetuity, as long as we lack definitive evidence that our existing, outdated equipment has been breached.

100. *See supra* notes 5–6 and accompanying text.

101. *See, e.g.*, Kenneth Olmstead & Aaron Smith, *What the Public Knows About Cybersecurity*, PEW RSCH. CTR. (Mar. 22, 2017), https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/ [https://perma.cc/2DU7-5UCY] ("Of the 13 questions [about cybersecurity] in the survey, a substantial majority of online adults were able to correctly answer just two of them."); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L., TECH. & POL'Y 341, 349–50 (2015) ("[T]echnical issues surrounding cybersecurity are not widely understood by the general public.").

Therefore, both the taxpayers and their representatives have a strong financial incentive to stick to the understanding of no evidence of a breach as no breach, not only for legal but also for election security purposes.

This is not merely speculation. In 2018, Michael Chertoff, a former Secretary of Homeland Security, stated that replacing "all paperless voting machines in the United States" would require "about the cost of a single F-22 fighter jet,"[102] which "cost approximately $250 million" at the time.[103] While that expenditure may be affordable for the United States as a whole, even a fraction of that cost may be too expensive for local authorities who directly administer elections. Moreover, keeping voting machines up to date is unlikely to be a one-time expenditure, given that computer equipment must be updated to address newly discovered vulnerabilities.[104] Unsurprisingly, local authorities from counties to states too often resist spending money on updating voting machines.[105]

I argue that the entrenched nature of the legal understanding of no evidence of a breach as no breach is an overlooked reason that experts' calls for election security reform have gone unheeded.[106] Pushing through any reform that spends any amount of money is generally an uphill battle in the American political process, as there will likely be at least some people who are against it and political minorities in the United States have disproportionate power to stop spending proposals.[107] In such an environment, politicians can block a proposal under the rationale that they support the spirit of the reform, but that they oppose the specific proposal because it would cost too much.[108]

102. Michael Chertoff & Grover Norquist, *We Need to Hack-Proof Our Elections. An Old Technology Can Help*, WASH. POST (Feb. 14, 2018, 2:22 PM), https://www.washingtonpost.com/opinions/we-need-to-hack-proof-our-elections-an-old-technology-can-help/2018/02/14/27a805bc-0c4b-11e8-95a5-c396801049ef_story.html [https://perma.cc/SBS4-Y3H3].

103. Kyle Mizokami, *This Chart Explains How Crazy-Expensive Fighter Jets Have Gotten*, POPULAR MECHS. (Mar. 14, 2017), https://www.popularmechanics.com/military/weapons/news/a25678/the-cost-of-new-fighters-keeps-going-up-up-up/ [https://perma.cc/QU3H-5H6S].

104. *Cf.* GURDIP KAUR ET AL., UNDERSTANDING CYBERSECURITY MANAGEMENT IN FINTECH: CHALLENGES, STRATEGIES, AND TRENDS 162 (2021) ("Software updates offer a lot of benefits: [t]hey repair a security loophole, remove a computer bug, and fix vulnerabilit[ies].").

105. *See, e.g.*, Muller, *supra* note 31 ("Since [Louisiana Secretary of State Kyle] Ardoin took office in 2018, he has been trying to purchase new voting machines but continues to run into various obstacles. . . ."); William Westhoven, *Morris County Commissioners Spar Over $5 Million Voting Machine Purchase*, DAILY REC. (Feb. 25, 2022, 3:12 PM), https://www.dailyrecord.com/story/news/2022/02/25/morris-county-commissioners-disagree-postpone-purchase-voting-machines/6921386001/ [https://perma.cc/P8V5-KJJE] (criticism of county officials' decision to delay a scheduled vote to spend $5 million to purchase new voting machines in Morris County, New Jersey).

106. *See, e.g.*, DAVID L. SHRIER, BASIC BLOCKCHAIN: WHAT IT IS AND HOW IT WILL TRANSFORM THE WAY WE WORK AND LIVE 115 (2020) ("Calls for improvement to election security have gone unheeded or . . . deliberately ignored.").

107. *Cf.* Catherine Fisk & Erwin Chemerinsky, *The Filibuster*, 49 STAN. L. REV. 181, 230 (1997) ("The filibuster allows the minority to block legislation . . . and tremendously increase the minority's power and bargaining strength.").

108. *Cf.* Rachel Treisman & Quil Lawrence, *The Senate Passed a Bill to Help Sick Veterans. Then 25 Republicans Reversed Course*, NPR, https://www.npr.org/2022/07/29/1114417097/veterans-burn-pit-bill-republican-senators

What makes election security reform even harder is the existence of a stronger rationale to block it: one can use the legal understanding of "no evidence of a breach" to claim that election security reform is not only expensive, but also wholly unnecessary. If one understands no evidence of a breach to mean no breach, and there is no evidence that any voting machines were breached, one can argue that we should not spend any money to fix or replace them. This is a much stronger rationale for opposing spending than, say, arguing that one supports paying for health care for 9/11 first responders in principle but that the specific proposal on the table costs too much.[109] Thus, I argue that displacing the understanding of no evidence of a breach as no breach is just as important to enhancing election security as making specific reform proposals is. Yet, scholars are apparently focusing on promoting reform proposals[110] without discussing a significant problem that enables voters and politicians to argue that those reform proposals would be a waste of taxpayer money.

Thus, to improve the chances of election security reform, academics and other experts must establish a coherent narrative that reconciles two different understandings of what no evidence of a breach means. As discussed, the understanding of no evidence of a breach as no breach must be retained for legal purposes. Alongside that understanding, we must also establish an understanding that no evidence of a breach can still mean a breach in the context of election security. The public must be persuaded that malicious actors can breach elections without our knowledge, and thus keeping our voting equipment up to date (or doing something else to minimize the risk of a breach, such as using paper ballots)[111] would not be a waste of money—just as having a military that is strong enough to deter invasions is not a waste of money even if no invasion actually occurs.

Although establishing a new paradigm is likely to be challenging, the idea that a problem can occur without our knowledge and that preempting that problem may be well worth the cost is not new. The 17th-century mathematician-philosopher Blaise Pascal presented that idea in what is now called Pascal's wager.[112] According to Pascal's presentation, God may or may not exist.[113] A person may choose to believe in God or not.[114] If God does not

[https://perma.cc/C5QU-68JB] (Jul. 29, 2022, 2:58 PM) (Republicans filibustering a bill that would provide health care for 9/11 first responders and the Senate Republican leader stating that "he supports the substance of the bill, but not the 'accounting gimmick.'").

109. *See id.*

110. *See, e.g.*, Michael A. Carrier, *Vote Counting, Technology, and Unintended Consequences*, 79 ST. JOHN'S L. REV. 645, 647 (2005) ("I propose for electronic voting machines a voter-verified paper trail, random audits, open source software, more robust certification . . . ."); Annie Barouh, *A New Old Solution: Why the United States Should Vote by Mail-in Ballot*, 18 SEATTLE J. FOR SOC. JUST. 243, 262 (2020) ("Paper ballots are not subject to the same chip replacement and security problems as the voting machines. Paper does not have to be calibrated.").

111. *See* Barouh, *supra* note 110.

112. *See* JEFF JORDAN, PASCAL'S WAGER: PRAGMATIC ARGUMENTS AND BELIEF IN GOD 28–30 (2006).

113. *Id.* at 30.

114. *Id.*

exist, people who lived their lives believing in God would have made only a finite loss, such as the time and money spent in going to church and donating to the church.[115] If God does exist, the same people would make an infinite gain by being rewarded with eternity in Heaven; by contrast, people who spent their lives not believing in God would suffer an infinite loss, in the form of eternity in Hell.[116] Thus, Pascal argued, rational people should live their lives assuming that God exists, regardless of the truth.[117]

Applying Pascal's wager to election security, whether God exists is equivalent to whether hackers may breach our elections undetected—in other words, a grave problem that can occur without our knowledge. If malicious actors would not breach our voting infrastructure undetected, spending money to secure that system would only lead to a finite loss. But if malicious actors *can* breach our voting infrastructure undetected, securing that system would lead to an infinite gain (protecting American democracy) and preventing an infinite loss (hostile forces tampering with our elections). In other words, Pascal's wager is a testament to an intuitive idea. If a problem would have catastrophic consequences if it were to occur, spending a relatively small amount of money to prevent it will be worthwhile, even if the chances of that problem actually occurring are low.

IV. CONCLUSION

An unwanted consequence of arguing that our election infrastructure may be vulnerable is that the argument can be misconstrued as questioning the legitimacy of duly contested elections. Dr. Halderman's research indicating that voting machines can be easily hacked has been co-opted by conspiracy theorists who claim, among other things, that "the 2020 [presidential] election was somehow fraudulent."[118] Dr. Halderman himself has repudiated such attempts as "people co-opt[ing his] work to lie to people."[119] Just as Dr. Halderman's research lends absolutely no support to the notion that the 2020 election was fraudulent, nothing said in this Article should be taken as questioning the legitimacy of any election. I cannot emphasize the following statement enough: President Biden was duly elected in 2020 because there is no evidence of systemic fraud in the 2020 election, meaning that there was no systemic fraud in the 2020 election as a matter of law.

What this Article does question is the extension of what should strictly remain a legal understanding—no evidence means no existence—to the realm of security. A good lawyer should believe that no evidence of fraud means no fraud.

115. *Id.*
116. *Id.*
117. *Id.*
118. The Political Science Podcast, *The Vulnerabilities of Our Voting Machines, and How to Secure Them*, NEW YORKER, at 5:28 (Oct. 24, 2022), https://www.newyorker.com/podcast/politics-and-more/the-vulnerabilities-of-our-voting-machines-and-how-to-secure-them [https://perma.cc/K9N8-EK55].
119. *Id.*

But any security professional who believes that no evidence of a breach means no breach should be fired. Security breaches can occur undetected despite our best efforts, and they are more likely to occur undetected the more competent the perpetrators are. To a good security expert, "no evidence of a security breach" merely means "no lawsuits from our customers—for now." This is why I am arguing that, for security purposes, we must understand that no evidence of a security breach does not necessarily mean no breach.

A simple comparison illustrates the importance of the public understanding of no evidence of a breach to enhancing election security. Throughout this Article, I have compared the possibility of our voting machines being compromised to U.S. intelligence deciphering Japanese military code during World War II, to illustrate that both kinds of breaches can occur undetected. I have also established that the American public, as well as many experts, apparently conflate no evidence of a breach and no breach, and that such an understanding can rationalize not spending money on election security because there is no need to fix anything if one believes that nothing was breached.

Would we accept this same rationale to cut funding for counterintelligence operations? Take the recent proposed ban on the Chinese social networking service TikTok. As of when this Article was written, U.S. officials appear to have a strong suspicion, but not definitive evidence, that hostile agents may use the app to collect "sensitive data about the location, personal habits and interests of Americans."[120] Do politicians act as if they can get more votes by telling the public that there is nothing to worry about, because we should understand no evidence of a breach to mean no breach? The answer seems to be a no. In fact, officials are moving to *increase* security measures against TikTok by banning the app from all U.S. government devices[121] and with a pending bipartisan bill in Congress that "would ban the app for everyone in the United States."[122]

Clearly, the idea of relaxing security measures because there is no definitive evidence of espionage by hostile forces appears unacceptable to politicians and, by extension, their constituents. This Article has shown that it would be just as reckless to block spending for election security on the assumption that no evidence of a breach of voting equipment indicates no breach. I submit that we have an obligation to convince the public and, if officials' response to apps like TikTok is any indication, convincing the public would not be as difficult as it may seem at first sight.

120. Sapna Maheshwari et al., *Bans on TikTok Gain Momentum in Washington and States*, N.Y. TIMES (Dec. 20, 2022), https://www.nytimes.com/2022/12/20/technology/tiktok-ban-government-issued-devices.html [https://perma.cc/KXZ4-G9BY] ("TikTok has long denied that it shares data with Chinese government officials . . . .").

121. Moira Warburton, *U.S. House Administration Arm Bans TikTok on Official Devices*, REUTERS (Dec. 27, 2022, 4:07 PM), https://www.reuters.com/technology/us-house-administration-arm-bans-tiktok-official-devices-2022-12-27/ [https://perma.cc/J632-J576] ("TikTok has been banned from all U.S. House of Representatives-managed devices, according to the House's administration arm, mimicking a law soon to go into effect banning the app from U.S. government devices.").

122. *See* Maheshwari et al., *supra* note 120.