Recommended Resource List:

Survey and Scrutiny of Election Security

by Douglas Lucas

DouglasLucas.com; DAL@RISEUP.NET

Hackers on Planet Earth conference (HOPE XV)

July 12, 2024 in New York City

Last updated July 11, 2024

BOOKS AND PAPERS

* *Code Red: Computerized Election Theft and the New American Century* by Jonathan D. Simon. He periodically updates the book to analyze new election cycles, most recently Election Day 2020. The book's website prominently includes analysis of Election 2020 and the current situation. Simon used to work as a polling analyst during the Carter administration, then left the field for law school — but his experience and connections as an analyst later proved helpful when, starting in earnest with Election 2004, he began using exit polls as a way to try to pry into the black-box portions of our elections.

* *The Hidden History of the War on Voting: Who Stole Your Vote and How to Get It Back* by Thom Hartmann. Published in 2020. A good overview of various elections-related issues such as D.C. statehood and the Electoral College, but also cybersecurity vulnerabilities of the country's private vendor voting computers.

* *Black Box Voting: Ballot Tampering in the 21st Century* by Bev Harris with David Allen. Written in 2003. On the Black Box Voting website, the entire book is available for free. *Vanity Fair* reviewed the book and so did Salon.

* In September 2006, three computer science professors at Princeton University published a security analysis of the Diebold AccuVote-TS voting machine. They stated: "Analysis of the machine, in light of real election procedures, shows that it is vulnerable to extremely serious attacks." Here's the executive summary.

* Project EVEREST — which stands for Evaluation and Validation of Election Related Equipment, Standards and Testing — was commissioned by the Ohio Secretary of State and conducted by academics and consultants. Their final report housed by the federal Election Assistance Commission (EAC) is 334 pages, dated Dec. 14, 2007, and definitely worth a read. EVEREST is a risk assessment of (then-)Ohio voting computers based on red team penetration testing, inspecting source code, and more. The evaluated systems included those designed and developed by Election Systems and Software (ES&S), Hart InterCivic (Hart) and Premier Election Solutions (Premier, formerly Diebold). Here's the EVEREST executive summary and a news article about the report from 2008 by a local newspaper in Pennsylvania, where some of the EVEREST findings applied (in addition to Ohio).

* NYU's Brennan Center for Justice has been covering this issue for a long time. Their website has an election security section. See especially their 162-page report *The Machinery of Democracy: Protecting Elections in an Electronic World*, which they spent more than a year putting together in 2005 and 2006. The report comes with three pages of endorsements. The authors describe in great detail precisely how software patches, ballot definition files, and memory cards can be manipulated to enable rigging. The report found "All three voting systems have significant security and reliability vulnerabilities, which pose a real danger to the integrity of national, state, and local elections." (The three voting systems were DREs, DREs with paper trail, and opscans, all of which are still in use today in some jurisdictions.)

* Professor Philip B. Stark, a math and statistics professor at UC-Berkeley, and Mark Lindeman, Policy & Strategy Director at Verified Voting, co-authored the 2012 paper "A Gentle Introduction to Risk-limiting Audits" with a companion set of tools to perform computations. Risk Limiting Audits (RLAs), developed by Stark, involve manually examining a subset of the audit trail, preferably handmarked paper ballots, and running a statistical analysis for irregularities. If an RLA finds the subset(s) to exceed the amount of irregularity expected, it'll flag the election to indicate a full recount is needed. RLAs successfully flag problematic elections with a 95% success rate. In 2020, the Georgetown Law Technology Review published a related paper by Stark and Princeton computer science professor Andrew Appel, "Evidence Based Elections: Create a Meaningful Paper Trail, Then Audit."

* Founded in 2004 by David L. Dill, Ph.D. — currently a computer science professor at Stanford University — VerifiedVoting.org provides great resources on this topic, such as the voting equipment database, and the verifier for exploring voting equipment use and post-election audit requirements across the U.S. However, the aforementioned Professor Stark, and Georgia Institute of Technology computer science professor Rich DeMillo, both resigned from Verified Voting because Verified Voting promoted RLAs for elections using Ballot Marking Devices (BMDs) without meaningful paper trails. Resigning, Stark said Verified Voting "will teach you to sprinkle magic RLA dust [...] on your untrustworthy election. All will be fine; you can use our authority and reputation to silence your critics." This is unfortunate, especially as Verified Voting's voting equipment database and verifier are great tools.

* E-book published by *WhoWhatWhy.org* in 2020 by investigative journalists Celeste Katz Marston and Gabriella Novello titled *Is This Any Way To Vote? Vulnerable Voting Machines and the Mysterious Industry Behind Them* with an addendum: *Is Mail-In Voting the Answer? WhoWhatWhy* hosts the e-book in full here. There's a six-minute promo video for the e-book on Youtube. See also *WhoWhatWhy*'s elections tag for many worthy articles on the subject of election security.

* Collection of articles, videos, podcasts, and more by independent researcher/journalist Jennifer Cohn. She writes about election security and related topics via her twitter account as well.

* *Was the 2004 Presidential Election Stolen? Election Fraud, and the Official Count* To be clear, I've yet to read this book, but it came highly recommended to me a while back from folks at *WhoWhatWhy*. It was published in 2006 and co-authored by journalist Joel Bleifuss — his work is often included on Project Censored — and Steven F. Freeman, a professor of research methods who at the time was at the University of Pennsylvania.

* *Loser Takes All: Election Fraud and The Subversion of Democracy, 2000-2008* was published in 2008 and edited by Mark Crispin Miller, a NYU professor of media studies. The book collects numerous short pieces on election security by authors such as journalist Brad Friedman, statistical forensics analyst Jonathan Simon, and others. To be clear, I've only read some of the pieces in this book so far, but the ones I have read have been really great.

* The late Roy G. Saltman was a computer security specialist known for his work on computerized voting at the National Institute of Standards and Technology (NIST). He wrote a tome published in 2006 titled *The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence*. I haven't read this one yet either, but it comes highly recommended to me by Ion Sancho, a Florida county election supervisor with about three decades of experience. Sancho is known for leading the 2000 presidential election hand count in Florida's Miami-Dade county — until the U.S. Supreme Court stopped just as it began — and for participating in election security activism (and documentaries) from his perspective as an actual election supervisor. Besides the Saltman book, Sancho thinks there's an important story waiting to be told someday about the history and development of election administrators, the professionalization of a countrywide cadre of nonpartisan election workers.

* The Election Assistance Commission (EAC), a federal executive agency, houses a lot of PDFs ranging from big reports like the EVEREST one or this lengthy glossary of election terminology to small small docs like this 6-page overview of recommended election security practices. Similarly, the Congressional Research Service (CRS), a federal legislative agency, performs research for members of Congress and their staff. CRS reports are sometimes public, sometimes confidential, but the restricted ones often make their way onto leak sites. A good way to begin trying to get a bird's eye view of any particular election security issue is to search the EAC and the CRS, perhaps with a Google site:filter (set google to search "Web" instead of the default "All") or using the search fields within the EAC and CRS websites.

* Eight prominent right-wing lawyers, former U.S. senators, and retired federal judges put together a report in July 2022 titled *Lost, Not Stolen: The Conservative Case that Trump Lost and Biden Won the 2020 Presidential Election.* They assess that the Trumpers did not provide meaningful evidence in court regarding Election 2020, and hint that the point of the Stop the Steal lawsuits was to leverage them to fuel sound bites. I'll add, to obtain donations as well.

DOCUMENTARIES

* PBS Frontline and ProPublica released their 54-minute documentary *Plot to Overturn the Election* (2022) free for watching online. It's a great crash course in the current Stop the Steal movement. Frontline describes the documentary as follows: "In a new investigative collaboration, FRONTLINE and ProPublica trace the hidden sources of misinformation about the 2020 election, demonstrating how a handful of people have had an outsized impact on the current U.S. crisis of democratic legitimacy." The film provides national-level context while also examining in detail specific voting jurisdictions.

* *Hacking Democracy* (2006). This 82-minute HBO documentary follows Bev Harris of Black Box Voting and others and is one of the better-known election security documentaries. Also, cybersecurity expert Harri Hursti is shown demonstrating what can surreptitiously be done to voting computers.

* *Kill Chain: The Cyber-War on America's Elections.* This 90-minute HBO documentary from 2020 is something of a follow-up to 2006's *Hacking Democracy*, again featuring cybersecurity expert Harri Hursti. Sleek HBO production again, too.

* *Murder, Spies & Voting Lies (the Clint Curtis story).* This 68-minute documentary follows journalist Brad Friedman's investigation of the murder in south Georgia of civil investigator Raymond Lemme, who refused his superiors' demands that he stop following up on the computerized election fraud claims of Clint Curtis, whose previous whistleblowing had resulted in the conviction of a Chinese spy, meaning Curtis was taken quite seriously by the authorities — but pursuing Curtis's whistleblowing about a government contractor asking him to make a prototype for real-world vote rigging was apparently a step too far in the eyes of some of Curtis and Lemme's opponents. (While the overt authoritarianism of governments such as the Kremlin or the Chinese Communist Party is certainly far worse than the milder domestic evils here in the U.S., this is one of those many stories reminding you that governance, even here, is ultimately not really determined by apple pie, say-the-pledge, *I Voted* sticker feel-goods.)

REALITY WINNER AND KREMLIN CYBERATTACKS ON 2016 ELECTIONS

* In 2017, whistleblower Reality Winner leaked top-secret evidence of Kremlin hackers targeting the 2016 elections — the second stage of these Russian military intelligence cyberattacks occurred just days before Election Day 2016. The Intercept published five leaked pages, and wrote an accompanying article. The pages are from a National Security Agency analysis that quotes raw data such as email addresses and hash values, despite one prominent journo I refuse to platform claiming there was no substantial evidence in it whatsoever because, according to him, Russiagate is all a big hoax or whatever. The Intercept failed to protect their source in so poor a way that she and others accuse The Intercept of being a shell tha attracts leaks away from outlets who might actually protect sources and thus prevent more 793(e) espionage cases. Winner says The Intercept has never taken public responsibility for the prosecutions of Terry Albury and Daniel Hale, who is still in prison to this day, and that reporter for The Intercept Matthew Cole is an inside source for U.S. spy agencies. She also says The Intercept hasn't meaningfully reformed themselves since her case, believing they did nothing wrong, and that giving up sources and then covering the "martyrs" they make is their basic modus operandi.

* This is my Aug. 24, 2018 article from Reality Winner's sentencing, published at an alt-weekly in Buffalo NY called *The Public*. Winner received the longest sentence — five years, three months — ever imposed on a civilian defendant for unauthorized disclosure of national defense information to the media. Note the website doesn't have HTTPS.

* This is my Mar. 30, 2023 article at the *Texas Observer* titled "The Voting Vendor in Reality Winner's Leak is Coming to Texas." This article provides the most comprehensive in-a-single-URL look at what Winner's leak revealed. For instance, it's not well understood that her leak was strengthened by several corroborations that emerged after its publication, nor that a governor said Florida election official(s) actually fell for the Kremlin's spearphishing trickery, nor that Bob Woodward wrote that the Kremlin planted malware on Florida election systems, and so on. Winner

herself said, frustrated, that "the scandal of who Reality Winner is, and how weird her name is" became the focus instead. My article links out to many more resources about Winner and the Kremlin cyberattacks. The article is supposed to be first in a series, but the *Texas Observer* has been busy with financial and other restructuring...

BMD VULNERABILITIES, COFFEE COUNTY, GEORGIA ELECTIONS OFFICE BREACH, AND ONGOING STATEWIDE VOTING SOFTWARE COMPROMISE

* It's important to understand three legal cases going on in Georgia right now that relate to the Coffee County elections office breach, since these cases are where much of the information is emanating from. The first is *Curling v. Raffensperger*, filed seven years ago, and currently waiting for senior judge Amy Totenberg in the federal Northern District of Georgia to issue her final ruling(s). The plaintiffs, such as Coalition for Good Governance (CGG), have been seeking to force the battleground state of Georgia to abandon mandatory electronic ballots and in most circumstances use hand-marked paper ones.

* In the course of *Curling*'s seven years, Coalition for Good Governance discovered the Coffee County elections office breach at the hands of top Trumpers, with MAGA lawyer Sidney Powell paying for much of it. The intrusion resulted in the operatives making exact copies of voting computers' software: Dominion Democracy Suite Version 5.5-A. Because all 159 counties in Georgia use the same voting vendor, and because the top Trumpers have spread around this pilfered source code to their allies (presumably that proliferation is ongoing), the elections office breach — which began just 24 hours after Jan. 6 — is still compromising Georgia's election system today, on an ongoing basis.

* Fulton County district attorney Fani Willis, in the Atlanta area, charged Trump and his 18 co-defendants with a RICO indictment including several different charges. Though Trump was not, some of his co-defendants were charged for their doings related to the Coffee County elections office breach.

* Finally, two years ago, some of the *Curling* plaintiffs issued a pair of subpoenas to the Coffee County Board of Elections and Registration for breach-related records. Such records would help specify additional information about the breach, its planning, and its cover-up, such as to possibly result in, say, additional indictments. But the elections board refused to obey those subpoenas, probably at the behest of the County Commissioners and the county's de facto diarchy, county manager Wesley Vickers and senior county lawyer Tony Rowell. So last year, in the federal Southern District of Georgia, the plaintiffs sued the Coffee County board of elections in a discovery action, demanding production of said breach-related records. Just as *Curling v. Raffensperger* is awaiting Judge Totenberg's ruling in the Northern District of Georgia, so the discovery action awaits Judge Cheesbro's decisions in the Southern District. Meanwhile the Fani Willis Fulton County RICO prosecution has been delayed. This all fits the pattern of other criminal trials for Trump or his top associates, around the country, being neutered or delayed as Election Day 2024 approaches.

* Nonprofits Coalition for Good Governance and Free Speech For People compiled this 4-page list of major media pieces on the Coffee County elections office breach and ongoing statewide election software compromise. It begins with the May 13, 2022 Washington Post article that broke the breach story and concludes with the Apr. 24, 2023 MSNBC "Deadline White House" 20-minute

segment on Coffee County and related matters. To my knowledge, no one has collected subsequent news items (there have been a lot!) — would make a good volunteer project for someone out there.

* On Aug. 15, 2023, *Lawfare* published journalist Anna Bower's very comprehensive article *What the Heck Happened in Coffee County, Georgia?* Two days later Bower was on a *Lawfare* podcast discussing the same. The article has since become the standard, all-in-one, published-in-a-fancy-pants place longread on the Coffee County elections office breach and ongoing statewide voting software compromise.

* On Jun. 14, 2023, Judge Totenberg in the Northern District of Georgia unsealed University of Michigan computer-science professor Alex J. Halderman's report examining the vulnerabilities of Georgia (and Dominon's) voting computers, ballot marking devices (BMDs). The unsealed report is a text with slight corrections made since the sealed version and some redactions from the sealed version remaining. This report should be of great hacker interest and the vulns may very well become national news in some ugly way just a few months from now. The report was originally filed under seal on Jul. 1, 2021 and remained confidential until Jun 14, 2023.

* In 2022, Judge Totenberg allowed Halderman's team to share their then-sealed report with the Cybersecurity and Infrastructure Security Agency (CISA), an arm of Homeland Security responsible for election infrastructure. CISA released a security advisory in June 2022 confirming the vulnerabilities Halderman and his team had found, and Dominion subsequently created updated software (Democracy Suite Version 5.17) in response to the problems. Yet, though Georgia Secretary of State Brad Raffensperger has been aware of the findings for nearly two years, his office astonishingly continues to insist Georgia will not install Dominion's security update until after the 2024 Presidential election, giving would-be adversaries months and months to develop and execute attacks that exploit the known-vulnerable machines.

* The accompany the unsealing of his report, Halderman wrote a lengthy same-day blog post providing a great overview that should be of special interest to those wanting hacker-y details. For example, he writes, the "The most critical vulnerability we found is a software flaw that would allow an attacker to spread malware from a county’s central election management system (EMS) computer to every ICX in the jurisdiction. Before an election, workers use the EMS to prepare an election definition—data files that describe what’s on the ballot—and they copy this data from the central computer to every ICX using USB sticks. We discovered a vulnerability in the ICX software that loads the election definitions. By modifying the election definition file in a precise way, an attacker can exploit the vulnerability to install arbitrary malicious code that executes with root privilege when the ICX loads the election definition. The underlying problem is a classic 'Zip Slip' vulnerability (in which a modified .zip file can overwrite arbitrary filesystem paths when it is decompressed), coupled with a badly designed system-level service that facilitates privilege escalation. This attack is especially dangerous because it is scalable—a single intrusion to the EMS computer in a county office could affect equipment in polling places over a very wide area. Attackers do not need access to each individual machine."

* On Jun. 21, 2023, *The BRAD BLOG* published my in-depth Coffee County investigation titled "A secret meeting within a secret meeting: Unspooling the Coffee County, Georgia voting system breach and continuing cover-up." In short, we knew top Trumpers have been directing a multistate scheme with Trump's knowledge, including in the battleground state of Georgia, to breach county elections offices and make off with copies of the voting systems software, presumably for hacks, rigs, and/or for sprinkling into their disinfo campaigns for enhanced pseudo-plausibility. Unfortunately for the conspirators, Georgia open meetings law mandates that Coffee County officials must provide transparency about a secretive February 2021 post-breach gathering of two county boards supposedly revolving around the resignation of the then-election supervisor and not

the intrusions, which were then still a secret, having concluded not a month prior... I also discussed this article of mine the same day it was released on the nationally syndicated AM/FM radio show *The BradCast* (Apple Podcasts; .MP3 file direct download).

* On Jul. 5, 2023, *The BRAD BLOG* published another Georgia investigation of mine, this one titled "Exclusive: Georgia Secretary of State has failed to certify urgent, CISA-recommended voting software update; critics charge state laws block him from doing so, even if he wanted to." In short, Brad Raffensperger's office has not contracted with a certification agent to get the requisite state-level examination done for Dominion Democracy Suite 5.17. Other evidence corroborates that, without a state certifying agent and possibly even with one, Raffensperger legally cannot move forward on upgrading to this latest version. According to J. Alex Halderman — same University of Michigan computer science professor whose report on the matter was unsealed by a federal judge in June 2023 — version 5.17 claims to address the flaws he'd uncovered in earlier version 5.5-A. That older 5.5-A version is presumably what we'd find in place if we booted up the voting computers presently stored in Georgia warehouses and closets. It's the same defective version currently set for use on Election Day 2024, since Raffensperger's office says he won't update the version till at least 2025.

* On Dec. 19, 2023, *The Daily Dot* published my investigative article about Coffee County titled "Exclusive: A missing laptop could be key to prosecuting Trump. This rural Georgia county only recently admitted that it exists" with the standfirst "The device may contain evidence about the infamous breach of Coffee County's election system." The silver laptop used by Misty Hampton, the Coffee County election supervisor during the breach — and one of Trump's 18 co-defendants in the Fani Willis Fulton County RICO case — presumably contains many breach-related records on it. Finding this laptop could impact not just the criminal trial of Trump and his co-defendants, but also *Curling v. Raffensperger*. To accompany the article, I self-published a blog post with four Coffee County surveillance images published for the first time along with important extra material about senior Coffee lawyer Tony Rowell meeting in the elections office with soon-to-be-breachers just days in advance of the initial intrusion.

* On Jan. 4, 2024, I wrote a four-page letter to officials, lawyers, and activists of Coffee County, Georgia highlighting some of the most important findings from my *Daily Dot* article. I also self-published an accompanying little blog post. Note the letter has quite a few typos as I had to write it hurriedly in hopes of affecting then-imminent county meetings. No time for spell-check! In response, I heard from the county — crickets. Maybe it was the typos.

* On Jan. 9, 2024, I snailmailed a one-page letter motion to Judge Cheesbro in the Southern District of Georgia. I pointed out the elections board attorney speculated in court that the silver laptop might be Georgia Secretary of State property, but my simple records request, which I carried out and provided, shows it was *not* Georgia Secretary of State property. I pointed out that counsel for the elections board told Judge Cheesbro in court that Charles Dial, head of the county's longtime IT firm, declined to fill out a sworn declaration as to his knowledge of the silver laptop — except my phone call to him regarding same showed that Dial didn't even know what a sworn declaration was, what I was even talking about. On Jan. 24, 2024 his judicial assistant Kim Mixon told me "The hardcopy and electronic copies of your letter have been received and have been forwarded to Judge Cheesbro for consideration." I heard later that the judge showed the letter to both sides of the case and asked parties if they wanted to respond, but nothing ever came of it and my letter motion was never officially docketed. I followed up. I heard crickets. I'm now planning to resubmit it, this time with notarization and obedience to the local rules of the Southern District of Georgia regarding margins, font, and suchlike. Maybe it was the incorrect font.

* Near the end of the as-yet-still-unconcluded *Curling v. Raffensperger* case, in January 2024, there was a three-week trial in Atlanta. Transcripts from that trial are listed on my website's files page, with each item specifying which witnesses took the stand that day. The slides from the plaintiffs' opening arguments, plaintiffs' closing arguments, and Halderman's Jan. 18, 2024 direct examination (as well as Video Segment 1 and Video Segment 2) are insightful, including listing specific voting computer CVEs widely affecting Georgia voting computers (CVEs are widely used classifications of security vulnerability bug reports).

ELECTION ACTIVISM

* The usual GOTV ("Get Out the Vote") efforts, such as voter registration drives or combatting disinformation concerned voting rights, are not included here, as GOTV falls under *voting* security, whereas my talk and this recommended reading list address *election* security. The difference is the agent: voting rights or voting security issues address what voters do; election security addresses the election system, usually seen from the point of view of election supervisors (aka election administrators, aka election directors). However, if you want a pair of good September 2022 *ProPublica* stories/videos about voting rights in rural Coffee County, see those linked about Olivia Coley-Pearson fighting against weaponized poverty and illiteracy suppressing the vote there. They brought tears to my eyes. Voter disenfranchisement, voter suppression on the one hand, and election security with its newfangled high-tech cyber-everything, are all ultimately part of the same big picture.

* Scrutineers. Founded by director Emily Levy in January 2020, the organization's website says they're currently seeking nonprofit status. The idea is to build a well-trained, countrywide core of volunteer election observers/monitors/pollwatchers/scrutineers. Their mission is to "educate, train, and mobilize nonpartisan election scrutineers to ensure all voters can vote and all votes are counted accurately, in order to increase voter confidence and achieve and sustain a thriving democracy in the United States." Levy was inspired by the fact that there were likely millions of people in the United States "who were concerned about the security of our elections yet had no idea that there were actions they could take to help create transparent elections we all can trust." Scrutineers is the place where, for example, if you're curious about the extent to which the transport teams moving votecount storage media from precincts to the county central tabulating facility are or aren't transparent — are the chain-of-custody forms and the bipartisan nature of the teams sufficient, or should the interiors of the vehicles be filmed? — somebody at Scrutineers is going to enjoy nerding out with you about that and finding readings and media to determine if such a situation needs improvement and if so, how to get started improving it.

* League of Women Voters. In a lot of voting jurisdictions, most election monitors/observers are there on behalf of a political party. They're partisans working for their party. But you can observe elections as a nonpartisan. In some cases, such as King County (Seattle) where I live, if you want to be a nonpartisan observer, you must first take a training from the King County elections department. Signing up for that, in King County anyway, is handled through the League of Women Voters, who require a small annual membership fee. Pay-to-play democracy, amirite? Anyway, I'll be attending my first training to become a nonpartisan observer later this month and I expect it'll really help me lay eyes on these various election system components and interlocking parts, as well as how they're actually used in practice. The League of Women Voters was founded in the 1920s by women suffragettes and has since expanded to include men and others. Outsiders have said that they're center-left, but the League does strive to be nonpartisan and make available factual information, resources, etc. to help everyone vote. It's one of the first-stop places when you're trying to figure something out about your local election security scene. They're the organization that has been around forever, whereas Scrutineers is more of a scrappy technohip upstart. By the same token,

your local elections department might be more helpful and talkative than you might imagine, so you can try giving them a call or email if you have a random question about something like "are undervoted ballots treated differently than fully voted ballots, and if so how?" Here are the websites of King County Elections, the NYC Board of Elections, and Coffee County, Georgia's as examples. You might know the saying, the public attends school board meetings, because that's part of the government that they can get their hands on (and understand more directly, more personally, if they have a kid in school). It seems county election boards are becoming the next big thing after school boards.

* The National Popular Vote Interstate Compact (NPVIC). The idea here is to keep the Electoral College— not abolish it— since abolition would be too difficult to achieve constitutionally. Instead, states pass laws agreeing that, if enough other states also agree so that the Compact has real teeth (*i.e.*, enough states join for the Compact to wield a total of 270 electoral votes), then each Compact member's electors will automatically vote for the presidential candidate who receives the most popular votes in all 50 states and D.C.. That would guarantee that the Electoral College always elects the winner of the country's popular vote. Trump and Bush II, for instance, won the White House without winning the popular vote, thanks to the Electoral College.

Originally the Electoral College (which isn't a place or a group with a membership list; rather, it's a process) was instituted by aristocratic founders to keep the ignorant plebs from falling for demagogues. Which is happening now; the Electoral College isn't stopping it. Further, a *Politico* article argues for routing around the Electoral College in this Compact way on national security grounds. In cybersecurity terms, routing around the Electoral College should reduce attack surface. In plain language, dramatically simplifying the Electoral College according to the Compact and yoking electors to the popular vote reduces the number of things that can go wrong in an already overcomplicated election system in a gigantic country with 162 million-something presidential voters.

Finally, note that linked to the Coffee County, Georgia wrongdoings were "fake electors" who for Election Day 2020 were impersonating legitimate Electoral College electors and trying to vote in Trump. Some of them, and other fake electors in Nevada as well, have been indicted for this impersonation, but I don't think most people have realized the dwindling of U.S. democracy (so called) is reaching the point where we have Electoral College imposters running around trying to fake the vote. It's yet another thing that can go wrong. Yet more states are joining the National Popular Vote Interstate Compact all the time. There's an enormous book on the topic by people behind the Compact called *Every Vote Equal* (fourth edition 2013). I've only skimmed my copy so far, sadly. They do have branches in different states trying to advocate for these different states to join the Compact, so if you read up on it thoroughly and decide you like what they're doing, there are probably plenty of related activism opportunities.

* Ranked Choice Voting (RCV) or similar is also called Instant Runoff Voting (ICV) elsewhere, such as in Canada. The current election system in the United States is organized under the principle "first past the post." Imagine racecars. The first racecar that wheels past the post wins, no matter what's going on with the racecars behind. So if there are two racecars understood to have a shot at winning the race, the Demonrat and the Repulsican, those who vote on the clunker way in the back, which may not even make it to the finish line, are accused of wasting their vote by giving it to such a so-called "spoiler" candidate: the lovable but fatally slow clunker car, or Ralph Nader (speaking of cars), or whoever. This "spoiler" problem is why people vote for evil — lesser evil to be sure, but evil nonetheless.

So why not change the first past the post paradigm? Ranked Choice Voting says, here's a list of all the candidates, rank them in order of your preference. Your first preference is the good honest

clunker, but if the good honest clunker isn't going to make it, then who do you want instead? Vote on what kind of pizza you want — and if they don't have vegan glutenfree with extra broccoli, what's your second choice? Same idea. If the clunker loses, give that vote to the lesser evil Demonrat to stop the greater evil Repulsican from getting in (or vice versa depending on political preferences). Sounds great, but on closer inspection, there are multiple ways, multiple algorithms potentially governing how such didn't-win votes may be redistributed to other candidates. What if the Demonrat left the race after you completed your RCV ballot, then Ayn Rand and KRS-One both entered, and now the ballgame has changed dramatically? As one redditor put it, "The only thing we know is the first preference" and not how that preference changes in light of additional changes the come into existence subsequent to filling out the ballot. Of course, algorithms can be prepared in advance for various situations, but they're not always clear to voters, election workers, or candidates.

Advocacy organizations such as Fair Vote certainly aren't putting front and center the hotly debated algorithm and ballot design confusions; instead, they're just touting that nearly 50 U.S. jurisdictions have passed RCV, including all federal elections in both Maine and Alaska. That's impressive, enough to mean these issues matter viscerally to people and have teeth, but if you look at the experience of Seattle, where I live, some people are really confused about the reforms that were passed there and will be first implemented in an August 2027 primary. One December 2022 article in Seattle's *The Stranger* was titled and subtitled "Ranked-Choice Voting Won in Seattle. Now What? Just Gotta Design a New Ballot That Doesn't Suck, Make It Idiot-Proof, Update the Tabulation System, Figure Out How to Report the Results, and Make Sure Everyone Knows What the Hell's Going On."

The issues aren't unsolvable, and my Canadian friends understand their longstanding Instant Runoff Voting and don't understand why the United States doesn't use it or something similar. So ultimately, I think ranked-choice voting or something like it can be a big help, but with a large asterisk next to it, the proviso that there's still a lot of competing confusion, problems needing sorting out and education, etc. before they just usher in some trojan horses, such as an RCV that isn't really what people intuitively understand as RCV. There are even competing ideas such as approval voting, and to just illustrate the confusion, King County Elections (Seattle) describes what the Seattle electorate voted for in November 2022 as ranked-choice voting, whereas the Center for Election Science describes it as approval voting. Feel free to explore the topic more; it's something I'm still struggling to fully grasp.

* University of Iowa computer science professor Douglas W. Jones maintains a website with an excellent brief illustrated history of U.S. voting equipment. The Help America Vote Act (HAVA) of 2002 greatly accelerated the computerization of voting in the United States. Since then, one of the biggest battles has been fighting for what at first was simply termed "paper ballots." Meaning, hey, it's a piece of paper, you mark it and you're good to go. It's associated with the idea of a Voter-Verified Paper Audit Trail (VVPAT) which is like it sounds, a paper receipt the voter can use to compare ther intent against what the computer is saying it's storing. But then over time, the Powers That Be corrupted the term "paper trail" to mean, among other things, a touchscreen that spits out a piece of paper with an unreadable QR code on it. Hence, activists wisely rebranded "paper ballot" as "handmarked paper ballot" to differentiate the human-marked, human-readable paper trail from the unreadable QR codes. Think of the VVPAT is a far more official version of a random piece of paper you bring in with you to scribble down your choices as a memory guide for yourself. It's not magic on its own.

Australia and multiple other countries use handmarked paper ballots counted observably in public, sometimes counted manually. A great book on this is *Code Red*, the Jonathan Simon book referenced above. Some voting activists believe that as long as strong Risk-Limiting Audits (RLA)

are in place, the legit Prof. Philip Stark-style spot-checks based on a real voter-verified paper audit trail, then it's okay to feed the handmarked paper ballots into the digital scanners for tabulation purposes. That would be faster and perhaps more accurate than taking several weeks to hand-count, which would require massive societal change, such as making Election Day and other days beyond federal holidays to recruit counters — and teaching the public at large not to expect immediate overnight results from presidential elections any longer. Of course, centuries ago, such elections took a long time to hand-count, so it wouldn't be something inherently new. I don't necessarily have a strong position on any of these different avenues of reform, and am just offering them and the ideas as springboards for audiences to jump off from, pursue their own curiosity and activism.

* If you're going to use voting computers (as opposed to handmarked paper ballots counted observably, whether by humans or by scanners spot-checked by humans), then the voting computers shouldn't be corporate-owned devices with proprietary closed-source software. For instance, here in New York City, Queens County uses the corporate voting vendor ES&S. Queens County voters vote on a Ballot Marking Device ES&S calls the AutoMARK and those votes are tabulated by an ES&S hand-fed scanner, model DS200. Neither of those are going to be running on free software, but rather proprietary closed-source software. Secretaries of State staff and other election workers do sometimes verify software hashes and the like, but it's not a process that's designed from the ground up to be a transparent, public-facing thing. So if you want public verification of hash numbers for voting computer files, then typically the answer is, good luck with that — maybe go ask ES&S in person, they're located in Omaha on 11208 John Galt Boulevard. Instead of this propertarian nonsense, the voting computers should be publicly owned (as in Brazil) and they should use free software (as in FLOSS). Some companies, such as Clear Ballot in Boston (used in King County!) have made stabs at this with varying degrees of success and failure, but it's something that publicly-minded volunteers could hack together if they really put their minds to it and had a sympathetic elections board and election supervisor in a state such as Texas where each county can choose its own voting vendor (rather than, say, Georgia where each county uses the same voting vendor).

* Statistical forensics and free information/better data. The best book about statistical forensics is Jonathan Simon's *Code Red*, referenced above. Exit polls, perhaps better termed "exit samples," ask a portion of voters leaving the voting booths who they voted for. Such exit polls are used by the United States, among others, to gauge the legitimacy of elections in other countries. But domestically, sometimes our exit polls show wide discrepancies between what the exit polls say, and what the final votecounts say. It's something of an axiom of illogical propaganda that when these domestic disparities occur, they're never because of rigging or other foul play— heavens no, that can't happen here — but always because there was some sort of error in the exit poll process, such as *oversampling Democratic voters* or *reluctant Republican voters* (supposedly reluctant to speak with exit pollsters) or what have you. There's a 2017 text called "A Guide to Election Forensics" by USAID (yes I know) that helpfully explains the math, the processes, and so on, behind election forensics, kind of a primer. *Code Red* has some very good examples of disparities between exit polls and final votecounts, sometimes to the benefit of Dems, sometimes to the benefit of Repubs, in races across the United States going back years and years.

Simon has suggested two activist ideas, one a "scanner party" where activists link arms around a scanner and refuse to leave until the ballots therein are counted transparently, rather than by the corporate, closed-source computer scanner, and the other the idea of a political candidate who, upon winning, halts his own inauguration and says in front of the press, Wait, let's have a transparent, hand-recount in public to make sure I really won, thus normalizing 100% fully transparent elections, save for the secret ballot of course.

Generally speaking, improving access to data and other information about elections is another worthy activist goal. There are 3000-something voting jurisdictions in the United States, 50 states,

D.C., and other places of voting, and all of them make information available to different degrees and in different ways. Scrutineers (referenced above) is especially interested in getting photographs and videos of poll tapes, sometimes called results tapes — they typically look like cash register receipts. Poll workers often tape them to precinct windows to show the vote totals for that precinct as election night comes to a close. Sometimes they're required by law to do this, sometimes not. But other data is interesting too, showing how different counties voted for example, so you can compare this against demographic changes, or cyberattack reports, or types of voting equipment used. It's a lot of nerdy work and you can reach out to me or Jonathan Simon or others if you want pointers on getting started. Mostly it's just being a curious detective, making phone calls and sending emails, while doing some statistical work and other logical reasoning.

GENERAL DEEP POLITICS AND ACTIVISM

* Before Trump's ad hoc use of the terms "deep politics" and "deep state" cast them into disrepute, the terms were associated with, among other things, academic political science and international relations. They were, and are, terms used by scholars and the like to refer to unelected powerful people, such as CIA directors or other spies, who stay in power for a long time regardless of which party or person holds the White House, making decisions more impactful than commonly understood. Their covert doings, such as assassinations, kidnappings, torture, and propaganda, domestic or abroad, were and are the stuff of deep politics: the work of building hierarchy-maximalist states that persist across centuries and attempt to gain and maintain as much power as possible. Learning this depressing stuff helps you grow out of the "How a bill becomes a law" view of history.

Two long books I've found invaluable in understanding how deep politics works in the United States are investigative journalist and *WhoWhatWhy* founder Russ Baker's *Family of Secrets: The Bush Dynasty, America's Invisible Government, and the Hidden History of the Last Fifty Years* (2008) and Catholic theologian James W. Douglass's *JFK and the Unspeakable: Why He Died and Why It Matters* (2008). Baker spent more than half a decade writing his and Douglass spent twelve years on his. Those who insist *it can't happen here* might behoove themselves to check out the extensive bibliographies of both these books and then give them a careful read. To me they were both very depressing, because they force you to realize the vast extent to which authoritarianism is no fleeting foe, but — in its latest incarnations — something planned and organized for centuries. Not taking your opponent seriously will only result in getting your ass handed to you. So read this stuff helps better map the layout of the real world, including but not limited to election security. This of course raises the question of whether statist voting does any good, which I grudgingly think it can as a hold-your-nose tactic, but I address that more fully in the talk.

* By the same token — learning about deep politics — read a few hundred of the quarter-million State Department diplomatic cables leaked by Chelsea Manning. Not articles about the associated hacker heroes and their hairdos, but read the actual cables, in full, slowly. Why not one a day for a year? Other good resources for primary source deep state docs are George Washington University's National Security Archive and the Federation of American Scientists. My articles and media appearances on the five million-plus emails liberated from the Austin-based spy firm Stratfor by hacktivist Jeremy Hammond are helpful too to show it isn't just states, but private industry as well — corporations and their hired anti-activist guard dogs such as Stratfor. Again, this sort of knowledge applies to any and all activism, not just election security. It's important that (often subsidized) talk of government transparency, government wrongdoing, does not overshadow the wrongdoing and complete lack of transparency from their corporate overlords.

* In 1977, investigative journalist Carl Bernstein — of the Woodward and Bernstein Watergate duo — published a 25,000-word piece in *Rolling Stone* titled and subtitled: "The CIA and the Media: How America's most powerful news media worked hand in glove with the Central Intelligence Agency and why the Church Committee covered it up." It's one of those textbook reads on then-subtler spy agency pressure on or infiltration of domestic media, something becoming evermore overt. But by no means should it be assumed, either, that every local newspaper is staffed by waffling weaklings; that very often isn't the case at all.

* The above three bullet points feel somewhat historical — JFK's assassination and whatnot — but this next resource looks at deep politics in the present day. *Spooky Connections* is a project of writer/journalist Heather Marsh. The website states: "*Spooky Connections* is an independent international open source investigation to probe transnational organized crime. We operate using open source information from established news outlets and primary sourced documents to graph, map, and document a clear understanding of organised criminal networks and activities." The front page is illustrated with the faces of (at the time of this writing) nineteen repulsive VIPs, much like a deck of cards spread out for inspection. Clicking on any one of them takes you to a webpage dedicated to exposing that single individual, using reputable sources such as investigative journalism reports and court filings. VIPredators making an appearance include Donald Trump, the late Jean-Luc Brunel who founded MC2 Model Management with financing from Jeffrey Epstein, etc. Remember, blackmail makes the world go round, including in terms of election security.

Think, for instance, of Barack Obama commanding Hillary Clinton to prematurely cede the 2016 election. Not saying there's proof, but Obama's purported motive of "let's all get along is more important than challenging elections" is so idiotic, especially in light of today's extreme not-getting-along polarization and the pure and proper legality of challenging elections (if it's so awful for a candidate to do, why's it a longstanding legal option?), that I think it's fair, in an *inference to the best explanation* way, to ask if there's maybe something more, such as blackmail or anything else untoward, influencing these Democratic decisions to self-sabotage than simple kindly concern for the well-being of the plebs. It's not particularly scientific to *a priori* rule out such possible explanations as blackmail, especially now that we've all read stories about Jeffrey Epstein or even more mundane pressures on candidates.

* The same Heather Marsh behind *Spooky Connections* is also a software developer and philosopher. In my talk, I referenced some of the ideas in her *Binding Chaos* series of philosophy books. Okay, I was a *summa cum laude* philosophy major, and I still read the stuff in primary source decades later. And I can say her books are as interesting or more so than any of the historical ones you've heard of, and with dozens of pages of bibliographies spanning millenia. She'll write of the PreSocratics one second, then from-the-latest-headlines human rights reports the next. It's dizzying in a good way. If you're depriving yourself of her books — three have been published of an anticipated 13 — you're missing out.

She's also the founder of the *GetGee* project, which is a real global data commons, a universal graph database project. The GetGee website also includes a promo video, talks at software development conferences about it, etc. Research, journalism, activism into election security or anything else is hampered until we have this. She describes *GetGee* as follows: "Our greatest need is for a collaborative information commons, for open journalism, for open science, and just for fun. We need a place where the data is not personal data but it is not corporate data either. We need a place where the application software is decoupled from the data but the data is all still linked. While secure communication and ownership of personal data is important, mass communication and mass collaboration are required to change the world. People risk their lives to tweet because they want to be heard. More, they want their stories to be a part of the permanent record, not lost in a stream of transient white noise. If we have a data commons, we can have the participatory governance,

research and global collaboration so many of us dreamed of, free of corporate ownership or interference."

DOUGLAS LUCAS

* My website since 2004 is DouglasLucas.com. The front page has a bio, bullet points of my recent articles, etc. There's a list of all my journalism: DouglasLucas.com/journalism. There's a list of all my media and other appearances: DouglasLucas.com/media. There's a collection of all the PDFs and other files I've ever obtained, mostly via open records requests: DouglasLucas.com/files. There's my blog which has hundreds of posts stretching back two decades or so: DouglasLucas.com/blog. Best of all, there's a donate page: DouglasLucas.com/donate.

* My email address is DAL@RISEUP.NET. Ask me, or the keyservers, if you want encryption.

* Snailmail (United States Postal Service only): Douglas Lucas / PO Box 75656 / Seattle WA 98175 / United States

Snailmail (Private carriers such as UPS, Fedex, DHL, Amazon): Douglas Lucas / 11036 8th Ave NE #75656 / Seattle WA 98125 / United States

Note the single-character change in ZIP codes, between the address for USPS (98175) and the address for private carriers (98125), is not a typo.

* My social media:

Twitter.
Bluesky.
Instagram.