

The Truly Disenfranchised Voter

The Disenfranchised voter has nothing to do with skin color, as many try to claim in an effort to alter election processes, rules and laws. No, there is a much larger group that includes all races, creeds, backgrounds, genders alike, those who have legitimate concerns of exchanging their personal data for a vote. In today's environment, Citizen's data has been compromised in many forms, Citizens have become a commodity by nation-states but even more disappointing is their own government's failure to protect their citizens. The Indiana Election Commission with the partnership of VSTOP is no exception. It is noted that the small, selected group at VSTOP has had the influence to alter Indiana Legislation and Election Laws in the past 15 plus years.

The Electronic Election systems have created a wide variety of ways to interfere and rob American Citizens of their vote but worse, their privacy. However, the most concerning with the digital age of Elections, is the theft of personal data. This puts Citizens at risk to both physical harm and financial harm. Citizens are increasingly aware that they are being made to choose between their private information being stolen or casting their ballot for the candidate that best represents them, perhaps even worse- both are stolen with the use of online technology. In 2020 the Electronic PollBook put over 4.7 Million Hoosiers at risk.

The Indiana Election Commission, VSTOP, Secretary of State, Clerks and many more officials who are involved with the Indiana elections have all claimed that the Election systems do not connect to the internet. Not only is this disingenuous it is purposely deceitful.

Quote: "It's also important to know that no piece of Indiana's voting equipment is online. The machines and tabulators are not connected to the internet."

While this controversy has been proven both to be false and true across the country utilizing the very same systems and equipment created by the very few companies in the industry. **One fact does remain, the key system which does indeed connect to the internet is the Electronic Poll Books.**

The Electronic Poll Books are utilized to transmit BMV data of every registered voter who participates in elections over the internet to communicate cross-county and cross-state. This data includes photo, name, address, date of birth and even whether the individual is an organ donor. Contrary to any individual making a statement otherwise, this data is easily grabbed by a number of nefarious actors to be sold on the dark web. And in some cases, the data is grabbed and sold by an insider, be it a "rogue" employee or a high level executive. It is confirmed that Clerk's Office, Secretary of State's Office,

The Election Poll Book Vendor, all have real-time access to the Electronic Poll Book. It is also confirmed that all of these entities also have the ability to assess who has voted also in real-time. Naturally, the potential for hackers to capture the personal data of voter's information from their Driver's License information is also in Real-Time. Political parties have access to this information as well, their campaigns may call individuals on Election day if they see that individual has not yet cast their ballot.

Prior to the Electronic Poll Book (EPB) Indiana utilized a printed Poll Book for each precinct, the information on the Paper Poll Book was kept physically secure with the Poll Worker throughout the duration of Election Day. And while it had basic information like name, address and previous signature on file, a voter simply showed his or her Drivers License or State Issued ID Card to the Poll Worker. The Poll worker in the presence of the voter, searched in the printed Poll Book for the individuals name, confirms the address information and the voter physically signed the Paper Poll Book in the presence of the poll worker. In turn the ID was handed back to the voter. There was no personal data such as organ donation participation, being sent or received over the internet. The Paper Poll Book remained secured with a poll worker in the presence of others and returned to the Clerk's Office to remain secured. Furthermore, after the legal retention time period the Poll Book could be recycled saving the environment from harmful devices.

If an individual did not have their ID at the Polling location, they were offered a Provisional Ballot in which the Poll Worker marked the ballot with a non-identifying number to be provided between the poll worker and the voter with the expectation that the voter would go to the Clerks office within 7-10 days, to provide their Driver's License and/or State Issued ID as confirmation that they were eligible to vote. The Clerk's Office then pulls the provisional ballot stack to find the matching written number on the ballot provided to the voter with the number the voter presented to the Clerk. The provisional ballot was then moved into the eligible ballot stack to be included in ballot counts. At no time during this process did the voter feel concerned about their private information being captured over the internet without their knowledge.

Within the State of Indiana, all government agencies utilize Cyber Security companies as a "layer of protection". In preparation to the 2020 election, Secretary of State Connie Lawson endorsed the cyber company Fire Eye with a signed a 40 month contract and further made a public statement in November 2019. Quote:

"We selected FireEye because of its reputation – in election security, threat intelligence, and in incident response. FireEye has helped us address both detection and prevention with the context needed to act quickly as needed. This partnership also helps further collaboration between the Secretary of State's office, Indiana counties, FireEye, and the

U.S. Department of Homeland Security (DHS)," said Connie Lawson, Indiana Secretary of State and Chief Elections Officer. "This statewide access to voter registration systems by requiring a multifactor authentication protocol for county election offices, implementing risk limiting audits, and working with the DHS to perform regular cyber vulnerability scanning on the statewide voter registration system."

"Election security is a growing priority, and the Indiana Secretary of State is leading the nation with the infrastructure it has put in place," said Tom Guarente, VP, External Affairs & Alliances for U.S. Public Sector at FireEye. "States like Indiana are tackling this challenge holistically and collaboratively by extending beyond just technologies to also focus on emergency management and preparedness. We applaud Secretary Lawson for her leading role in shoring up the State's election defenses and believe other states will take to Indiana's leading approach as well."

"Through this partnership, FireEye will provide Indiana counties with internet traffic monitoring to protect against threats and state data intrusions. This includes implementing FireEye technologies at the county level, and FireEye Managed Defense service for active monitoring and hunting of bad actors within their environments to detect and block threats, backstopping their security officials should action need to be taken. This initial 40-month contract will carry the Indiana Secretary of State's office and counties through the 2022 U.S. election."

While FireEye was not transparent when they first discovered their systems were infiltrated, nor were they transparent on how long they were aware of the infiltration into their Customers' Security Services. However, it was only 33 days after the 2020 Election FireEye was forced to file a report with the SEC. To date FireEye nor the Government has updated the situation other than some media reports stating that the hack had occurred months before the 2020 Election.

Quote:

On December 8, 2020, concurrently with the filing of this Current Report on Form 8-K, FireEye, Inc. ("FireEye", "we", "our" or "us") is announcing on our corporate blog that FireEye recently was attacked by a highly sophisticated cyber threat actor, one whose discipline, operational security, and techniques lead us to believe it was a state-sponsored attack. Based on his 25 years in cyber security and responding to incidents, Kevin Mandia, our Chief Executive Officer, concluded we are witnessing an attack by a nation with top-tier offensive capabilities. This attack is different from the tens of thousands of incidents we have responded to throughout the years. The attackers tailored their world-class capabilities specifically to target and attack FireEye. They are highly trained in operational security and executed with discipline and focus. They

operated clandestinely, using methods that counter security tools and forensic examination. They used a novel combination of techniques not witnessed by us or our partners in the past. We are actively investigating in coordination with the Federal Bureau of Investigation and other key partners, including Microsoft. Their initial analysis supports our conclusion that this was the work of a highly sophisticated state-sponsored attacker utilizing novel techniques.

We have witnessed the Indiana government entities experiencing intrusions, for example during a February 2021 County Council Meeting on Zoom, someone was able to infiltrate with Pornographic video/images causing the Elected Officials to stop the meeting and restart.

During a County Commissioner Meeting, a resident questioned the Commissioner on the vulnerability of the systems to hacks, the entire board of elected officials nodded and stated, quote “EVERY GOVERNMENT ENTITY IS HACKABLE”.

Particularly curious is the fact that in July 2021, town councils, county councils and other government entities were made aware by their Insurance Brokers, the standard liability insurance cost would remain the same, however, the insurance for Cyber Security was to increase immediately by a whopping 100%. This raises the question, what are the chances that the Election Data is NOT manipulated by cyber intrusions at any level of government? It is more likely than not given the vast number of cyber intrusions throughout the nation.

On August 17, 2021 Cyber Security Companies, Indiana Department of Health and the Indiana Office of Technology failed over 700k Hoosiers when it was discovered that in July 2, 2021 personal information of individuals was also compromised through the use of the Digital Contact Tracing. Similar to the FireEye SEC Filing, this knowledge was not disclosed to the public for over 45 days. Providing Hoosiers with one year of Credit Monitoring does not address the issue that digitizing, sending and storing personal data including name, address, email, gender, ethnicity, race and Covid testing information being handled in a questionable manner. Just because the Social Security number was not collected does not stop bad actors from causing physical, financial or social harm to a Citizen.

Quote:

“We believe the risk to Hoosiers whose information was accessed is low. We do not collect Social Security information as a part of our contact tracing program, and no medical information was obtained,” said State Health Commissioner Kris Box, M.D., FACOG. “We will provide appropriate protections for anyone impacted.”

The state Department of Health will send letters to affected Hoosiers to notify them that the state will provide one year of free credit monitoring and is partnering with Experian to open a call center to answer questions from those impacted. In addition, the Indiana Office of Technology will continue its regular scans to ensure information was not transferred to another party.

Billions of tax-payer funds were poured into electronic election equipment and systems which have caused controversy in one way or another during every election since inception. Billions of dollars invested into Environmentally harmful, non-recyclable equipment causing more harm to the Earth with disposal of electrical equipment and batteries laying in a landfill for the past two decades. This goes against the philosophy of "Saving Planet Earth". The idea of CO2 being a catastrophe is miniscule compared to the pollution that remains and spreads throughout the nation. The fact is, True Environmentalism favors recyclable and biodegradable materials, such as paper, which has been perfected by the recycling industry. Furthermore, because of VSTOP's outside partnerships, some legislators in Indiana have been incorrectly convinced that having a paper trail is not necessary for the public to accept election results.

Between 1964 and 1996, prior to electronic voting systems the average participation in elections through the paper ballot and paper poll book was **73% of Registered Voters Participated**. Indicating the confidence in the election system was substantially higher than it is today with only 58% participation in 2016 and 65% in 2020, while the **Absentee Ballots went from an average of 7% 1964-2004** to a substantial increase in 2008 to 24% Absentee Ballots, in 2020 a whopping 61% were Absentee ballots, even with the increase in population, percentages tell the real story.

In less than 20 years of the Elections, confidence fell in the Indiana Electronic Election Systems as **Participation declined by an average of 15%** each election, however the **Absentee Votes have increased by 90.6%**.

A severe distrust with the government, elected officials, election system companies, outside groups and lobbyist has decimated confidence in the Indiana and National Elections. The electronic systems fail to provide the necessary information for Audits, as even today there are still 76 counties in Indiana without Paper Trails. The Election Division, Secretary of State and Legislators have been made aware of the voting machines vulnerability to security issues. The Indiana University Public Policy Institute reported in October 2020 the following, Quote:

"Indiana is one of only eight states to still use DRE Machines without a verified voting paper audit trail. In fact, 57% of all voting equipment used in Indiana does not have a

paper record. Only 16 of Indiana's 92 counties (17%) use hand-marked paper ballots with BMD's."

That is 76 counties of millions of dollars in electronic equipment sitting in a landfill over the years. Whereas paper ballots and paper Poll Books ensure a Paper Trail for audits and are recyclable after 5 years. While both saving confidence in the election and truly saving the environment. Another aspect of electronic election systems is the disenfranchisement of the blind. These individuals should have the ability to vote on a ballot with braille and not be required to assume that what they heard, through the use of headphones, and the timing of their choice will be their own. The blind and deaf have participated in elections for decades using their own talents of reading braille or having a trusted friend join them to assist. Today this group has lost faith in the electronic election systems because it truly does not suit their needs and allows for unknown individuals to assist in their private choice to vote.

Recovery remains critical as reported by Public Citizen, Quote:

"The election security advocacy community has been focused on critical tools for recovery in case of a hack- paper ballots, audits to check the paper against the machine count and recovery systems, should the voter rolls be hacked. Recovery systems are critical because no system is perfectly secure. Although audits of paper ballots would expose any mismatch between machine tallies and the votes on paper, allowing election administrators to find both computer errors and hacks, only a handful of states conduct rigorous post-election audits."

Indiana is unable to perform such rigorous audits due to the 76 counties that do not utilize paper ballots.

Americans have discovered that the Electronic Election has created a billion-dollar cottage industry with a few people making changes in the United States Republic, which have had far reaching implications that continue to be ignored. Through this cottage industry, every Citizen has been transformed into a commodity for the highest bidder. Security and the Respect of Privacy for the US Citizen has been cast aside while these election systems transmit, over the open internet, Photos, Names, Birth Dates, Addresses, Organ Donation and whether or not they have participated in their Civic Duty. Furthermore, the Electronic Poll Book's connectivity to the internet have shown to be an entryway into the election systems via the Clerks Office, Indiana Secretary of States Office or a simple hack into the online state-wide county servers.

It is no secret that foreign and unknown adversaries wish to collect this personal data for nefarious activities, the fear of violence through release of personal data has

increased as we witnessed extremist spend a better part of 2017 and 2018 “doxing” innocent individuals for their political beliefs, only to have those individuals physically attacked or fired from their job through the manipulation of truth. Identity theft, through the use of cyber technologies, coupled with the constant failures of cyber security firms chosen by the State of Indiana have created a new money-making industry of Cyber Insurance for government entities, however still do not protect the Citizen. Why would Cyber Insurance Rates increase for government entities by 100% in July 2021 unless they have already calculated that Cyber Security firms have failed time and time again to protect Government entities, Corporate Entities of every industry and more importantly the American Citizen’s data.

As reported by Public Citizen, Quote:

“The hacks of Yahoo, LinkedIn and Experian- which sometimes went undetected for years- illustrate that corporate entities with enormous security budgets remain vulnerable. Local governments running elections have far fewer resources available to protect voter data and voting systems”

Indiana Election Commission, VSTOP, the Secretary of States Office have all been aware for a number of years that the electronic election system companies have been dishonest time and time again over the course of the past 20 years. However, the Indiana Election Commission and the Secretary of State has refused to hold them accountable under the guidance of VSTOP. Through the guidance of VSTOP, Indiana has changed legislation to accommodate the cottage industry, not the Citizen.

In fact, of all the reported years, only one year did Indiana Election Commission and Secretary of State publish a “Cost Per Vote” for each county. This average “Cost Per Vote” in 1996 was \$2.86. The state has chosen not to hold itself accountable, nor provide the Cost Per Vote to the public with the insurmountable costs it is imposing on the Indiana taxpayer to pay millions to just three private election companies involved.

In 2020, both political parties sent out Unsolicited Absentee Applications to thousands of Hoosiers. This not only caused confusion, it poses the question how do they gain private information of the voter without their knowledge? The Application for Absentee Ballot is supposed to a private affair requested by the voter, however the Indiana Election Division and the Secretary of State’s response to this action was simply, “well, it isn’t illegal”.

What a majority of Citizens do not know is that regardless of Party arguing for or against Voter ID, the fact is Absentee Ballots do NOT REQUIRE VOTER ID. This was mentioned in the 2007 Ruling Crawford v. Marion County Election Board and Indiana

Democratic Party v. Rokita (as Secretary of State). While the complaint derives from a "Talking Point", never is the question asked; Why did in 2008 the absentee votes begin skyrocket and subsequently become out of control beast? We have heard from different Election Boards that they want electronic Tabulators because of the "burden" of hand counting, and yet another question must become front and center, how does the public know that Absentee Mail In Ballots were truly verified at all given the massive amount in 2020?

Additionally, there were 10 Indiana counties which had over 100% of the Voting Population as being registered. This further demonstrates that the Registration Voter Rolls are not maintained properly. This information became public by Judicial Watch in October 2020. As someone who must confirm before sharing information, we investigated and found that 2020 was not the only time more than 100% of voting age population was registered to vote in Clark County. In fact, this circumstance has occurred in the two previous elections, particularly when the substantial increases in Absentee Ballots occurred. Ignoring Citizens who were incarcerated at the time, moved, were not eligible to vote (non-Citizen), away at out of state universities and even passed away individuals.

In summary, Hoosiers have far less confidence in elections due to the electronic systems. Hoosiers have far greater concerns for their safety and security due to the technological systems and failures of Cyber Security firms to protect their client data. Hoosiers have lower participation in their Civic Duty because of their distrust of all involved. This great distrust of all involved with Indiana elections lead to a vast number of Truly Disenfranchised Voters that remain to be seen in future elections. The trend is continuing to discourage Citizens to participate in their Civic Duty. It is past time to return to real election security as described with Paper Ballots and Paper Poll Books which has proven for centuries to provide Citizens with private, secure, fiscally responsible, environmentally friendly, free and fair elections.

My expectation is that you have read carefully and will consider the dangers that has been thrust upon Hoosiers in which there is only one solution. The attached file further demonstrates how the current system and any foregoing systems that this Commission is considering through its partnerships has altered Elections and has cost the Hoosier Taxpayer in unsurmountable ways that must be corrected. While the attached file may seem large it provides the sources you may require for consideration.

Attachments and Citations

1. Indiana Election Statistics and Clark County Election Statistics Cited by www.state.in.us/sos/election/iec, <http://clerkweb.house.gov/elections/elections.htm> , in some cases utilizing the Way Back Machine as the current Secretary of State's website fails to provide all data today.
2. Indiana Secretary of State Connie Lawson and Fire Eye Partner In Preparation for 2020 US Election, November 19, 2019, Press Release by Fire Eye.
3. Fire Eye Cyber Security Services Agreement
4. United States Securities and Exchange Commission FireEye, Inc. December 8, 2020,
5. State Notifying Hoosiers About Improper Access of Contact Tracing Information, Indiana Department of Health Press Release, August 17, 2021 www.in.gov
5. Indiana Elections Commission Voter Portal Statement
6. VSTOP 2019 EPB Investigation
7. Election Systems Software (ES&S) Conflict of Interest
9. Judicial Watch Study October 2020
10. Indiana University Public Policy Institute October 2020
11. Public Citizen Calls on Largest Voting Machine Vendor to Stop Selling Machines That Connect to the Internet, Increase Costs to Taxpayers, July 2018

Thank you kindly for your consideration, I look forward to the Commission's response to these very important topics of protecting Hoosiers safety, security and vote.

Respectfully,

Concerned Citizen and Tax Paying Voter