BOMBSHELL EXCLUSIVE: NATIONWIDE CELLULAR NETWORK CONNECTS ELECTION EQUIPMENT AND GIVES FEDERAL GOVERNMENT ACCESS TO ELECTION SYSTEMS AT THE PRECINCT LEVEL

August 14, 2023 by Joe Hoft



BOMBSHELL: NATIONWIDE CELLULAR NETWORK CONNECTS ELECTION EQUIPMENT AND GIVES FEDERAL GOVERNMENT ACCESS TO ELECTION SYSTEMS AT THE PRECINCT LEVEL

Guest post by David and Erin Clements

A growing majority of Americans know the 2020 election was fraudulent. Many analysts who have been studying election integrity have concluded that there had to be a two-way connection between local election electronics (electronic poll pads, tabulators, election management systems, voter databases, etc.) and a centralized data collection system responsible for monitoring and manipulating the election. Fingers have rightly been pointed at all-inclusive election management software, the Albert Sensor system, Scytl and Edison, and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC).

This incestuous collaboration between the Department of Homeland Security, the Election Assistance Commission, leftist/globalist funding, foreign companies, and their private partners, allowed for the real-time monitoring of all election data, and more importantly, the ability to change the results.

While experts could understand the functional capabilities of how these programs manipulate elections at the county and state levels, one area of mystery remained. Experts could not fully explain how systems within individual precincts which are supposedly "air-gapped" were adding votes in real-time – such as KnowInk poll pads in Texas that added

hundreds of votes to the 2022 midterm election after the polls had closed. To accomplish election fraud at individual polling places, it is necessary to have an air-interface with the supposedly "air-gapped" equipment networked at the polling place.

A year-long research project led by an election integrity investigator from Utah, Sophie Anderson, and communications engineer, Dr. Charles Bernardin, has uncovered the mechanism that is being used to connect our election equipment at polling places across the nation. Anderson and Bernardin met while working together in several overlapping election integrity efforts. After submitting a countless number of public documents requests from multiple federal, state, and local governments, and working with other grassroots researchers, **the team realized that the federal government has indeed created a nationwide network that is capable of collecting and changing real-time voting data at polling places across the country from a central location. The private network tool is called FirstNet, and like so many things that have proven detrimental to American liberty – it was sold as a tool to ensure public safety.**

WHAT IS FIRSTNET?

The idea of a national cellular network dedicated to public safety was hatched in the wake of 9/11 when congested cell networks proved to be a bottleneck for first responders. In 2012, Congress created the First Responder Network Authority under the Department of Commerce to oversee the build-out of "FirstNet." The original intent provided by its sponsors was that FirstNet would serve police, fire, and EMT services. However, the scope was soon expanded to include all "critical infrastructure" – which included water, energy, and transportation infrastructure. (https://www.digi.com/solutions/by-technology/firstnet)

Curiously, just days before Barack Obama left office, his administration's Department of Homeland Security used the specter of "Russian interference" in the 2016 election as an excuse to declare election systems to be a part of that critical infrastructure. As a result, the stage was set to roll election systems into FirstNet.

The original plan to build FirstNet was to create a separate network with nationwide coverage that used a dedicated cellular band portion known as Band 14. Years and billions of dollars later, AT&T had built out the FirstNet Band 14 network with the coverage shown in the map below.



AT&T's FirstNet Band 14 Coverage

The obvious problem was that separate Band 14 coverage was proving to be too slow and expensive to build, as only pockets of the country had the service available – with some states left completely without service. If Barack Obama's vision of using FirstNet to connect to all election equipment was going to be realized before the 2020 election, the developers would need to speed things up.

In 2017, AT&T offered the First Responder Network Authority "preemption services" on its entire cellular network. "Preemption" would give FirstNet customers priority on AT&T's network, ensuring they would always have service on the AT&T network. Verizon, T-Mobile, and Sprint soon followed suit in offering preemption services, instantly expanding FirstNet service wherever cellular service was available. These other providers gave their preemption services names like "Frontline" and "Connecting Heroes," but for the purposes of simplicity for this article we will refer to the preemption service on all the providers as "FirstNet."

Almost instantly, FirstNet's coverage increased from pockets of the country to cover most of the population and its voting locations as shown in the map below. This coverage assures electronic poll pads, election management systems, and tabulators with internet connection capabilities could be connected as "critical infrastructure" to the FirstNet network and given priority service, regardless of the presence or quality of local wired internet service.



Areas where FirstNet has ability to preempt existing cellular networks (source (https://www.nperf.com/en/map/5g))

THE PUSH TO CONNECT ELECTION SYSTEMS TO FIRSTNET

Just because the FirstNet cellular network was now available to be used for election systems, didn't mean all local jurisdictions would connect. Some of them would need to be pushed. Coincidentally, public discussion of using the Election Assistance Commission's (EAC) influence to push election jurisdictions nationwide to connect to FirstNet took place at a two-day Election Assistance Commission (EAC) Board of Advisers meeting in April 2019. The full transcript of the meeting is here.

The Board of Advisors supposedly exists to assist the EAC in setting standards and guidelines to help states comply with the Help America Vote Act (HAVA) through their certification program. Oddly enough, almost two years prior to this meeting, the accreditations for both election equipment testing labs, Pro V&V and SLI Compliance, had lapsed. This lapse in accreditation effectively shut down the ability of all states to legally certify their election systems as required by HAVA. No vendors, anyone in the EAC, or anyone on their Board of Advisors appeared to have noticed this indefensible oversight. As a result, most of the country's election systems were not legally "certified" for the 2020 election.

While a lapse of this magnitude defies reason, the Board of Advisors had an inexplicable and prescient impulse to meet before the manufactured Covid crisis of 2020. To do what exactly? In April 2019, the Board met to discuss "disaster management and recovery when elections are disrupted by natural or manmade disasters." And they weren't talking about dealing with a small, local disaster during an election, but a national disaster that had the ability to affect the presidential election itself.

Board member David Beirne said, “But you also look at it in terms of the Presidential elections is you have one shot at it. And I think that’s the real discussion that needs to occur in terms of your continuity of operations, your response plan, and the scalability impact that if you have a shelter in place or on a Presidential election, what does that really look like…for the State’ electoral votes?”

The Board’s expectation of the need to deal with unprecedented national shelter in place orders during a presidential election amounts to an unbelievable prophetic foresight of what would occur leading up to, and during the 2020 election. A similarly dark prophetic exercise called **Event 201** was held by the Johns Hopkins Center for Health and Security in partnership with the World Economic Forum and the Gates Foundation where bureaucrats practiced controlling narratives during a “hypothetical” worldwide pandemic that would soon take over the planet in reality.

While the EAC Board of Advisors discussed being prepared for a national disaster during a presidential election, a board member named Daniel Ivey-Soto chimed in to advocate that FirstNet be used as the internet connection at polling places across the country. (Ivey-Soto is a state senator from New Mexico who has become well-known for his ethical conflicts, his leadership role in the corruption of the election franchise in that state, and accusations of sexual misconduct.)

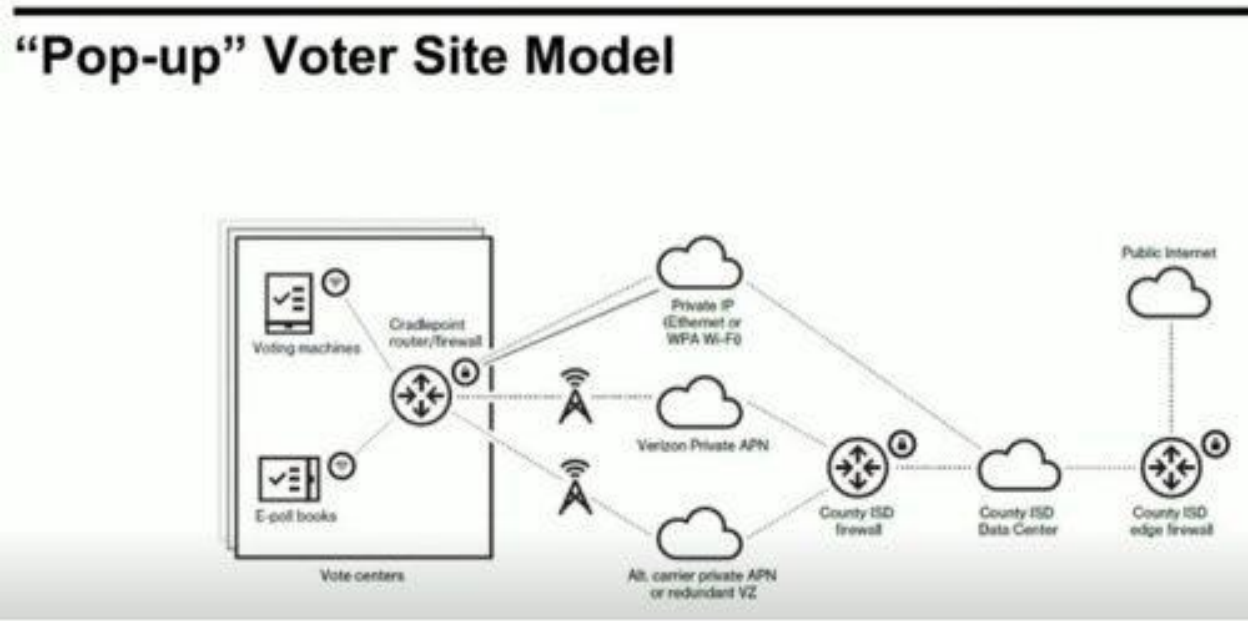
Ivey-Soto wanted the electronic poll pads (which have full access to the voter registration database and voter turnout) and the systems that transmit the election results to be connected to the FirstNet network. Fellow board member, Gema Howell, immediately latched on to Ivey-Soto’s idea of using preemption privileges to connect election equipment to the internet. The board lamented their lack of authority to force jurisdictions to connect to FirstNet. But they decided to use their leverage and connections in the federal government to push the use of the FirstNet cellular network for election systems.

EVIDENCE LOCAL JURISDICTIONS ARE CONNECTED TO FIRSTNET

There is a lot of hard evidence that the EAC Board of Advisors successfully carried out Daniel Ivey-Soto’s vision to connect the nation’s polling places to the FirstNet cellular network.

DALLAS COUNTY

For example, there is the official network diagram for election sites in Dallas County, Texas (shown below). The diagram shows both the electronic pollbooks and the tabulators connected to a cellular network with a ***two-way*** connection between the router at the polling place and the cellular network itself, which is connected to a central county data center.



Network diagram from Dallas County public presentation showing tabulators and pollbooks connected to a cellular network

The priority cellular services provided by Verizon to the Dallas County elections office was the subject of a May 2020 discussion hosted by Hans Olsen, former Department of Homeland Security employee. The goal of the talk was to explain how they "securely" connected election equipment to the cellular network during the March 2020 Primary election. They also heavily advertised Cradlepoint modems which are used prolifically by public safety and critical infrastructure customers to connect to FirstNet.



Slide from Dallas County public presentation on using Cradlepoint modems to connect polling sites to cellular networks

Lester Lewis, a Dallas County IT professional stated, “We were able to use remote tools…to look and to see the signal strength from the carriers… I was able to define the issue right then [from the County Data Center], call Verizon and **they were able to make some changes there**… on voting night.” Then Gregory Brown, Solution Architect Manager at Verizon stated, “Dallas County upgraded their modems [to Cradlepoint] so that they could have that **real-time voter count and voting results** sent back to the data centers.” (emphasis added)

The researchers believe the priority cellular network referenced in this talk is actually FirstNet. According to Dr. Bernardin, “The environment for the Government’s intrusion is partially determined by the IT people when they configure the router at the voter center… the IT manager sets up the private network with Wi-Fi protected access and a firewall. The router can be set to randomize the MAC address to keep the network from being identified, but the randomization can be shared with trusted people. The router provides a private, two-way connection between the election equipment and the FirstNet cellular network. Once this two-way connection is established, FirstNet can monitor real-time data that is passing through the election equipment – including who is turning out and how they are voting. This data can be remotely changed by a man-in-the-middle operating on the FirstNet network. In fact, the election results can be entirely fabricated with this clandestine configuration, and nobody would know.”

FLORIDA

Citizen researchers in St. Johns County, Florida coordinated with each other to document the Wi-Fi networks that were active at fifteen of the polling locations across their county. They discovered that a single cellular network that had been named “LetTheDogOut!” was serving all 15 voting locations in St. Johns County during the 2022 midterms.



Screenshot of Cellular Wi-Fi Network serving St. Johns County, Florida

This evidence indicates that St. Johns County was using a similar priority network setup as Dallas County, Texas, and that service was part of the nationwide "public safety" network.

CENSORSHIP ABOUT FIRSTNET

As Americans have learned since 2020, looking at what information is being censored and ridiculed is often a strong clue to discovering truth that is inconvenient for the globalist narrative. Elon Musk's "Twitter Files" and recent congressional hearings have proven that the government has gotten into an Orwellian habit of violating American's first amendment rights to suppress what they call "malinformation."

Malinformation is information which is true but will undermine the agenda the government is trying to accomplish.

It appears that actors who have popped up to support the government narrative about the 2016 and 2020 elections wanted to suppress discoveries of county-wide, cellular networks being used to support election equipment:

Prior to the 2022 midterms, True the Vote put out a call to action to their national audience asking citizens to take screenshot documentation of the Wi-Fi networks that were active at their polling places and report anything that seemed suspicious.

This led the leftist coalition called Election Integrity Partnership (EIP) to monitor how this call to action spread on social media and they also likely helped censor it on Twitter. At the conclusion of their "study," they released a barrage of tweets intimating that there is nothing wrong with internet connections at polling sites and shaming election integrity activists for looking into it. (https://twitter.com/EI_Partnership)

Suspiciously, the EIP (Election Integrity Partnership) was formed a mere 100 days before the 2020 election to monitor "attempts to delegitimize election results" – an activity that prior to 2020 was reserved for prominent democrats and three letter agencies which was never taken seriously by most Americans. The EIP's work culminated in the publication of a report called "The Long Fuse" that was published in the Spring of 2021 and dismissed all claims of election fraud in the 2020 election as baseless conspiracy theories – a conclusion that a cursory review of video evidence proves to be false.

A prominent member of the EIP is a former CIA employee and anti-Trumper named Rene DiResta who was a primary proponent of the "Russian interference" narrative that the FBI and Hillary Clinton campaign tried to pin to the 2016 election to derail the Trump presidency. The narrative has since been completely debunked by the investigation led by special counsel, John Durham.

The EIP was also tied to the elaborate censorship scheme to silence dissent over the 2020 election and the COVID response exposed by the House Oversight Committee in March 2023.

Since publishing their report in Spring of 2021 condemning everyone who questioned the 2020 election, the EIP was largely silent on the hundreds of efforts that were ongoing across the country to expose insecure and fraudulent elections, until True the Vote asked people to document Wi-Fi networks at polling places. **Just the fact that EIP was seeking to suppress citizens looking into Wi-Fi connections at polling places suggests researchers looking into FirstNet were on the right track.**

SECRECY AND VULNERABILITY

It is difficult to obtain information on FirstNet because, while it is taxpayer funded and supposedly for public safety, it is the result of one of the many public-private partnerships involved in our elections which are immune to public records requests.

Shockingly, according to Senator Ron Wyden, FirstNet is also exempt from congressional oversight. In a letter published in April 2023, Wyden stated concerns about the security of the FirstNet network and the likelihood that it could be hacked by bad actors:

"...Cybersecurity experts have long warned that phone networks are vulnerable to surveillance by hackers and foreign spies...[who] can exploit flaws...to track mobile users, intercept calls and tests, and even steal sensitive information available on devices...all U.S. carriers are vulnerable to these exploits, resulting in risks to national security..."

Wyden went on to state that AT&T had apparently conducted cybersecurity audits of the FirstNet system, but that they were unavailable to anyone in the federal government, including Congress, because of a non-disclosure provision in the contract the Department of Commerce had negotiated with AT&T. Therefore, no one knows what was investigated in the audits, what the results were, or whether any identified deficiencies were fixed.

INFRASTRUCTURE TO STEAL ELECTIONS

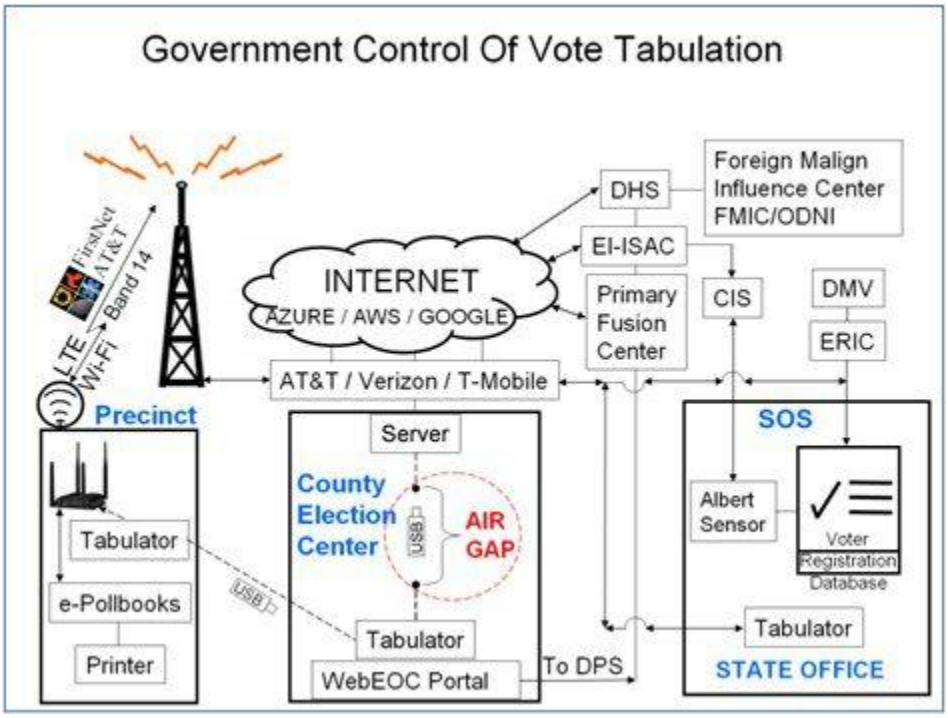
The fact that the federal government has interfered in foreign elections is an undisputed fact accepted by the left, the right, and even fact checkers. (https://www.globalresearch.ca/us-interfered-in-elections-of-at-least-85-countries-worldwide-since-1945/5601481) Even the fact that AT&T has worked closely with the federal government for spying operations isn't much of a secret. Multiple pieces of evidence were provided in this article that AT&T has had a cozy relationship with the federal government to carry out both international and domestic spying operations going back decades. In 1976, President Gerald Ford blocked a subpoena from a congressional

subcommittee because he said AT&T "was and is an agent of the United States acting under contract with the Executive Branch."

Revelations from the Snowden documents suggest that AT&T's relationship with the federal government continues with the installing of surveillance equipment for the NSA in at least 59 domestic sites. Shortly after the corrupt election system failed to deliver the presidency to Hillary Clinton in 2016, even the Brennan Center for Justice expressed concern that the NSA was too cozy with our domestic communications infrastructure – a topic they are silent on now.

Does infrastructure exist that could change election results electronically in real-time without noticeable delay? Yes – such a thing could be facilitated at the national level by the FirstNet cellular network. All the players surrounding the deployment of FirstNet into elections are already on the suspect list of bad actors of every election integrity researcher as well being part of the group of people who were caught illegally censoring Americans who know 2020 was not a legitimate election.

Dr. Bernardin describes in the following network diagram how the FirstNet network could be misused to connect precincts to county and state election offices in such a way that all election data passes through a single network where it could be intercepted and changed by the other programs the DHS has set up to supposedly protect and monitor our election infrastructure:



Network diagram showing how FirstNet could be misused to interfere with election infrastructure

The idea that our own government would betray its people in such a way was almost impossible to accept in the immediate aftermath of the 2020 election. But after the discovery of massive illegal censorship by the government over discussion of the 2020 election, federal agents planted to agitate the crowd on January 6th, eternal gaslighting from the establishment, and the weaponization of law enforcement to create a two-tiered standard of justice against those claiming fraud occurred – the conclusion that our own government was to blame for the coup that occurred on November 3, 2020, seems obvious.

One last piece of evidence that supports Anderson and Bernardin's theory that FirstNet is a critical piece of the election-stealing machine is the still unexplained explosion that destroyed an AT&T's data center in downtown Nashville on Christmas Day, 2020. Very few details ever came out about the perpetrator of the explosion, and no one ever tried to explain why he did it. Early articles did admit that "911 call centers, hospitals, the Nashville airport, government offices" were affected "from Georgia to Kentucky." Police departments in multiple states were unable to use their FirstNet phones and had to communicate through radio or temporary burner phones. It's possible FirstNet was the target and it's possible that evidence of election interference carried out using FirstNet needed to be destroyed.