IT IS FINISHED! The EC’s Data Security Is in a Complete Meltdown, A Messy Train Wreck, Putting the Personal Data of 19 million Ghanaian Voters at Risk.

By Alolga Akata-Pore – Ex Soldier and Cybersecurity Researcher

Introduction

It is Finished! Ghanaians have spoken. They have FINISHED their part by participating in the elections and inauguration of their new president, but the work of fixing the Electoral Commission is not FINISHED. DAAAABI, ƐN SAAAA YƐ! EBI AKA!

On December 10, 2024, after stumbling over the reading of the election results; initially misstating the winning candidate’s votes in the thousands rather than millions, the Chairperson of the Electoral Commission (EC) of Ghana declared with finality: *“It Is Finished!”*.

With those words, she signalled the official conclusion of Ghana’s highly contested 2024 general elections. But while the people of Ghana may have finished their task of electing a new government in a historic landslide victory, what remains far from finished is the EC’s troubling track record of IT failures, data security lapses, unnecessary institutional outreach, its refusal to take responsibility for mishaps and its negligence of duty to Ghanaians.

Even worse, the Commission appears to mistake its constitutional independence as a license to operate with impunity, ignoring the accountability and transparency principles that are fundamental to democratic governance. Whether through negligence or incompetence, the EC’s persistent failure to secure Ghana’s electoral data poses a systemic risk to national security and the integrity of our democracy.

This article highlights the most alarming IT failures within the EC, their far-reaching implications for Ghana’s democracy, and the urgent reforms needed to prevent a future electoral crisis.

Unaddressed Data Breach and Unauthorized Access to Voter Information

One of the most alarming concerns arose in May 2024, during the Limited Voter Registration exercise. Shortly after registering, I received an unsolicited campaign text message from a presidential candidate containing specific details that could only have originated from the EC’s voter database. This strongly indicated that voter data had either been leaked, misused, or compromised due to severe lapses in the EC’s data security protocols.

Readers are advised not to mistake the information contained in this SMS as something that could have been obtained from a commercial data broker. While data brokers may be able to confirm voter registration status, the specificity of the information in the message, including an intimate knowledge of the exact time I registered as a voter, strongly suggests that the source of the data was the EC itself, either directly or indirectly. A data broker would not have access to such near-real-time registration details, reinforcing the likelihood of unauthorized access or insider involvement within the EC’s systems.

Realizing the gravity of the situation, I formally wrote to the EC in August 2024, raising concerns about a potential data breach. Despite multiple follow-ups, the EC failed to

acknowledge or respond. Determined to ensure accountability, I escalated my concerns to the following institutions:

- **The Data Protection Commission (DPC)**
- **National Security**
- **The Office of the President**

Recognizing the seriousness of the issue, the President himself intervened, forwarding my concerns to the EC for action. Yet, in a shocking display of disregard, even this high-level intervention failed to elicit a response from the Commission. The EC's outright refusal to engage on a matter as critical as a potential breach of voter data is a gross dereliction of duty and raises serious questions about its commitment to protecting voter privacy and upholding democratic integrity.

Despite repeated warnings, the EC has neither publicly acknowledged the potential data breach nor taken steps to inform affected voters about the possible unauthorized access to their personal information. This lack of transparency and accountability is deeply troubling and stands in stark contrast to how any responsible public institution should handle such a serious security lapse.

The IDOR Vulnerability in the EC's SMS Voter Verification System:

While awaiting the EC's response, I discovered another critical vulnerability in the EC's SMS-based Voter Verification System, which allowed anyone with a valid voter registration number to retrieve another voter's details. This flaw, known as Insecure Direct Object Reference (IDOR), is one of the most basic cybersecurity vulnerabilities; something that should never exist in a secure national electoral system.

This meant that anyone, using their phone, could access the registration details of any Ghanaian voter without their consent; by simply entering a valid voter ID number. The vulnerability remained active until November 2024, when the EC's SMS system was taken offline *not* because of a security fix, but because the *USSD rental had expired*.

A More Alarming Development: IDOR Vulnerability in EC's Website-Based Voter Verification System:

After the elections, on December 8, 2024, the EC deployed a web-based Voter Verification App on its website – https://ec.gov.gh. This system, which should not have been necessary post-elections, contained an even more alarming version of the same IDOR vulnerability and raised additional concerns:

- **It exposed more personal data than the SMS system, including full names, dates of birth, polling stations, and even voter photographs.**
- **It required no authentication - anyone with an internet connection could anonymously retrieve voter data. No PIN or any form of identification was required.**

  This is akin to a bank or telecom provider launching an app that allows transactions without requiring a PIN or password. In any other industry, such negligence would result in mass lawsuits, regulatory fines, and a collapse of public trust.

- **Unlike Ghana's controlled-access voter exhibition process, which restricts access to accredited political party agents and voters, this web-based app provided unrestricted and anonymous access to sensitive voter data.**

- **The EC even provided a difficult-to-ignore button in the app that allowed users to retrieve additional voter data effortlessly, further demonstrating a fundamental lack of security awareness.**

- **A Curious Timing: Why Was the App Deployed After the Elections?**

  It remains a curious and troubling decision that the EC chose to deploy this web-based voter verification system *not before* the elections, when it would have served a legitimate purpose, but only *after* the elections had concluded, at a time when its necessity had become completely moot.

  Ordinarily, a voter verification system is most useful in the lead-up to an election, allowing voters to confirm their registration details and polling stations to prevent confusion on election day. However, the EC's decision to launch this system on December 8, 2024, a full day after the elections raises serious questions about its intended purpose and necessity. If the goal was to assist voters in verifying their registration details, this system should have been deployed before the elections, not after. A simple one-way SMS notification to all registered voters, confirming their registration status, would have been a far more effective and secure approach. This would have ensured broad accessibility while safeguarding voter data from unnecessary exposure. This bizarre and illogical deployment further underscores the institutional incompetence and cybersecurity negligence within the EC. Or was there an operational or political motivation behind its post-election release?

  At best, this reflects sheer mismanagement and a fundamental misunderstanding of digital security principles. At worst, it suggests an unsettling level of carelessness with sensitive voter data that demands immediate accountability.

The EC's Troubling Pattern of IT Negligence:

The EC's IT failures are not limited to data breaches and IDOR vulnerabilities. Additional serious operational and governance concerns include:

- **Missing or Lost Biometric Verification Devices (BVDs): Reports indicate that BVDs have either gone missing or were improperly disposed of, with at least one device allegedly found in a private individual's possession in Nsawam.**

- **Delayed acknowledgments of missing Biometric Verification Devices (BVDs) suggest that the EC may not have implemented an effective geotagging system for tracking its critical election hardware. The fact that some BVDs were unaccounted for long after the registration exercise, and others were only discovered in the possession of unauthorized individuals, indicates possible gaps in the EC's ability to monitor the location of these devices in real time. A properly implemented geotagging system would have enabled prompt identification of missing equipment, reducing the risk of loss, theft, or unauthorized use.**

- **Unnecessary Use of Thumbprints in Voting:**

    - **Thumbprint voting is not used in established democracies such as the US, UK, Canada, Australia, all EU countries or New Zealand.**
    - **Even in Uganda, India, and Brazil, where biometric authentication is employed, thumbprints are only used for authentication; not for marking ballots.**
    - **Ghana's use of thumbprints compromises ballot secrecy, as it makes it easier to track voter choices.**

<u>Oversight Institutions Are Also Failing the EC and the Public:</u>

Despite these alarming failures, institutions responsible for oversight have been largely ineffective:

- **The Data Protection Commission (DPC): Despite assurances of action, the DPC failed to hold the EC accountable, effectively emboldening its negligence.**
- **National Security: Has failed to intervene meaningfully, despite the clear national security risks posed by these vulnerabilities.**
- **The Audit Service of Ghana: The EC should be subject to performance and compliance audits, yet there is no public record of any such audit taking place.**
- **Parliamentary Select Committees responsible for Communications and Electoral Affairs: These committees have seemed powerless in their quest to ensure IT security in public institutions, allowing the EC's failures to persist unchecked.**

<u>A Call to Action:</u>

The EC's failures demand immediate and decisive action. The Ghanaian public must insist on accountability for the EC's reckless handling of voter data and demand that it operates with transparency and integrity.

Key Actions That Must Be Taken Immediately

1. **Immediate Removal of the Web-Based Voter Verification System**
    - **The system must be taken offline immediately to prevent further unauthorized access.**
    - **The EC must publicly acknowledge the data exposure and issue an unreserved apology to all affected voters.**
2. **Comprehensive Audit of the EC's IT Systems**
    - **The Audit Service of Ghana must conduct a full performance and compliance audit of the EC's IT systems.**
    - **This should include investigations into missing BVDs, IT procurement processes, and cybersecurity protocols.**
3. **Parliamentary Inquiry into EC's Cybersecurity and IT Failures**
    - **The Parliamentary Select Committees on Communications and Electoral Affairs must launch a public inquiry into the EC's cybersecurity failures.**

- The inquiry should include testimony from EC officials, IT contractors, and data protection experts to determine the extent of the failures and necessary reforms.

4. **Legal and Regulatory Enforcement**

    - The DPC must take legal action against the EC for failing to protect voter data, as required under Ghana's Data Protection Act, 2012 (Act 843).
    - The EC must be compelled to adopt international cybersecurity best practices to prevent future breaches.

Conclusion:

On December 10, 2024, after declaring the final presidential election results, the Chairperson of the Electoral Commission boldly proclaimed: "It is Finished!" These words, meant to signify the conclusion of Ghana's electoral process, have since become emblematic of the EC's approach; one that appears to prioritize moving forward at all costs, on a wing and a prayer rather than ensuring that the systems it deploys are fair, secure, and transparent.

But for millions of Ghanaians, particularly those whose personal data remains exposed due to the EC's cybersecurity failures, it is far from finished. The EC's reckless mismanagement of voter information, its failure to respond to urgent security concerns, and its continued deployment of flawed IT systems paint a troubling picture of an institution that is either unwilling or incapable of safeguarding our democratic processes.

This crisis cannot be ignored. Without urgent intervention, the EC's data security failures could erode public confidence in elections, undermine national security, and expose millions to identity theft and fraud. Institutions such as the Audit Service, Parliament, National Security, and the Data Protection Commission must rise to the occasion, demand accountability, and implement reforms to prevent future disasters.

Ghanaians have spoken. They have FINISHED their part by participating in the elections, but the work of fixing the Electoral Commission is UNFINISHED. The time for action is now. If we fail to act decisively today, the next electoral crisis will not be one of mere data leaks, but a full-scale collapse of public trust in our democracy.