

**Alolga Akata-Pore**  
**E:aporelolga@proton.me**  
**M:0263149776**  
**24<sup>th</sup> August 2024**

**Honourable Albert Kan-Dapaah**  
**Minister of National Security**  
**Ministry of National Security**  
**Accra, Ghana**

**Dear Honourable Minister,**

**Subject: Urgent Request for Investigation into Potential Security Risks Stemming from Voter Data Breach**

I hope this message finds you well. I am writing to bring to your immediate attention a matter of grave concern that may have significant implications for the national security of Ghana, particularly in the context of the upcoming December 2024 general elections.

#### **Background of the Concern**

As a senior citizen and active participant in our nation's democratic processes, I completed my voter registration on May 12, 2024, during the Limited Voter Registration exercise. This exercise primarily targeted young Ghanaians who have recently turned eighteen (18) and are now eligible to vote.

However, on May 23, 2024, I received an unsolicited campaign text message from an individual claiming to be Dr. Bawumia, a presidential candidate in the upcoming elections. The message contained highly specific information that raises serious concerns:

- **Knowledge of My Voter Registration:** The sender was aware that I had registered to vote in the upcoming December 7th elections, a registration that was only possible through the May 2024 Limited Registration exercise.
- **Accurate Identification of the Parliamentary Candidate:** The sender correctly identified the parliamentary candidate representing their party in my constituency for the 2024 general elections.
- **Use of My Data for Campaign Purposes:** The sender explicitly solicited my vote, asking me to support both himself and the parliamentary candidate of his party in my constituency, which indicates that my personal data is being used for targeted campaign activities without my consent.

This incident raises serious concerns about the potential breach of personal and biometric data, particularly for young Ghanaians who are barely 18 years old and therefore particularly vulnerable. If this sensitive data were to fall into the hands of criminals or other malicious actors, it could pose a significant threat to national security.

## National Security Implications

The unauthorized access and use of voter data, especially biometric information, could have far-reaching consequences:

1. **Exploitation of Vulnerable Populations:** Young Ghanaians, who are just beginning to engage with the political process, could be targeted for manipulation, coercion, or exploitation if their personal data is compromised.
2. **Undermining Electoral Integrity:** The integrity of the upcoming December 2024 elections could be severely compromised if voter data is used to influence or intimidate voters, or if it is weaponized in disinformation campaigns, including the deployment of deepfakes. Furthermore, if this breach has indeed occurred, it raises serious concerns about the integrity of previous elections. The possibility that similar breaches might have influenced past electoral outcomes cannot be overlooked and warrants immediate investigation.
3. **Violation of Fairness Principles:** The Electoral Commission (EC) has long upheld the principles of fairness, integrity, and transparency as the foundation of Ghana's democratic processes. **Fairness** ensures that all political parties and candidates compete on a level playing field, without any undue advantage. Integrity refers to the adherence to ethical standards, protecting the electoral process from manipulation or corruption. **Transparency** requires that the entire electoral process is conducted openly, with all procedures and decisions made visible to the public to foster trust. In this case, the apparent breach of voter registration data undermines these core principles. The targeted campaign messaging I received, based on my recent voter registration, suggests that one political candidate or party gained premature access to sensitive voter information. This unfair advantage distorts the competitive balance, as other candidates and parties did not have access to the same level of detailed voter data at that time. Even if the EC subsequently released voter registration data as part of an exhibition exercise, such data would not include all the elements utilized by the individual who breached the system. The information used in the unsolicited message including the precise timing of my registration and the specific targeting of campaign content based on this data indicates that the individual had access to more detailed and privileged information than would be publicly available during any standard exhibition exercise. My biometric data is a clear example of the data that would not be on public exhibition.

This breach not only compromises the fairness of the electoral process but also erodes public confidence in the integrity and transparency of the EC's operations, raising serious concerns about the overall legitimacy of the upcoming elections.

4. **Broader Implications of Biometric Data Use:** It is important to highlight that no established democracy including the United Kingdom, the European Union, the United States, Canada, Australia, New Zealand, Russia, China, and Vietnam

uses biometrics in their electoral processes. The reliance on biometrics in Ghana and other developing countries is particularly troubling. The unnecessary use of thumbprints makes it easier to trace and potentially expose a voter's choice, thereby compromising the secrecy of the ballot, a fundamental principle of democratic elections.

To better protect voter privacy and uphold the integrity of the electoral process, I strongly recommend considering alternative methods employed by other democracies. For instance, in Uganda, voters have the option to either place a tick or use a thumbprint, while countries like Brazil and India utilize advanced touch screen systems. These methods provide enhanced security and privacy, ensuring that the confidentiality of voters' choices is maintained. This approach would be more in line with the principles outlined in the Data Protection Act, 2012 (Act 843), particularly Sections 17, 18, 19, 20, and 21, which emphasize the protection of personal data, the right to prevent unauthorized processing, and the need for data to be used only for its intended purposes

5. **Impunity and Disregard for Data Protection:** The manner in which this data has apparently been accessed and utilized reflects a blatant disregard for the Data Protection Act, 2012 (Act 843), which mandates the safeguarding of personal data. The impunity with which this breach has occurred erodes public trust in our national security institutions and raises serious concerns about the adequacy of the security measures currently in place.
6. **Potential Breach of Other National Systems:** It is important to note that the Electoral Commission's database must be one of the most defended databases in the nation, if not the most defended. If this database has been breached, it raises alarming questions about the security of other critical national systems. The implications of such breaches could be catastrophic, potentially exposing sensitive national information and compromising the security and stability of the entire country.

### **Request for Urgent Action**

Given the seriousness of these concerns, I respectfully urge the National Security Secretariat to take the following actions:

1. **Immediate Investigation:** Conduct a comprehensive investigation into the potential breach of voter data, focusing on how this data was accessed and whether there are any broader security risks. This investigation should include determining if any insider threats or third-party vendors were involved and whether similar breaches have affected previous elections.
2. **Assessment of Security Protocols:** Review the existing security measures surrounding the storage and handling of voter data, particularly biometric information, and recommend enhancements to prevent future breaches.

3. **Protection of Vulnerable Populations:** Implement measures to protect young voters and other vulnerable populations from being exploited or targeted due to compromised data.
4. **Assessment of National Security Risks:** Given the potential breach of the EC's highly defended database, I urge a broader assessment of other critical national systems to determine their vulnerability and the necessary steps to reinforce their security.
5. **Coordination with Relevant Authorities:** Work closely with the Electoral Commission, the Data Protection Commission, and other relevant bodies to ensure that all necessary steps are taken to secure voter data and maintain the integrity of the upcoming elections.

### **Conclusion**

The protection of voter data is not just a matter of privacy; it is a critical component of our national security. Ensuring that the upcoming elections are free, fair, and secure is essential to maintaining public trust and social stability in Ghana. I trust that your esteemed office will take swift and decisive action to address these concerns and safeguard the rights and security of all Ghanaian voters.

Thank you for your attention to this urgent matter. I look forward to your response and to the actions that will be taken to mitigate these risks.

Yours faithfully,

Alolga Akata-Pore  
E:aporelolga@proton.me  
M:0263149776