South African Electoral Commission's mobile app for voters: Data privacy and security dimensions

Nawal Omar
Researcher, Research ICT Africa (RIA), Cape Town
https://orcid.org/0009-0008-4665-1227

Scott Timcke
Senior Research Associate, Research ICT Africa (RIA), Cape Town
https://orcid.org/0000-0001-7125-8306

Abstract

In 2014, the Electoral Commission of South Africa (also known as the "IEC") launched a mobile app to support voter participation in electoral processes. The app, called IEC South Africa, can be used to verify, update, and confirm a voter's registration details and voting station. It also provides an interface for special-vote applications and real-time election results. This study conducted a privacy and security analysis of the app, through a compliance review of the IEC's privacy policy in terms of the South African data protection legislation, followed by an analysis of the app's APK files, permissions, third-party trackers, and vulnerabilities, including API (application programming interface) calls. The analysis revealed several security and privacy concerns, including inadequately secured API keys, the potential for unauthorised access, and the potential for data breaches. In addition, the presence of advertising and analytics trackers suggested third-party data-sharing, raising concerns about transparency and user consent. The study draws attention to the need for the IEC to take action to address the app's security and privacy weaknesses. The study also demonstrates the importance of data minimisation, transparent practices, and adherence to privacy policies in order to maintain user trust and security in electoral technology.

Keywords
elections, voters, technology, mobile apps, data privacy, data security, South Africa, Electoral Commission, IEC

DOI: https://doi.org/10.23962/ajic.i34. 18132

Recommended citation

Omar, N., & Timcke, S. (2024). South African Electoral Commission's mobile app for voters: Data privacy and security dimensions. *The African Journal of Information and Communication (AJIC), 34*, 1-21. https://doi.org/10.23962/ajic.i34. 18132

1. Introduction

The IEC South Africa mobile application (app),[1] made available by the Electoral Commission of South Africa (also known as the "IEC") since 2014, provides an array of features that facilitate user engagement and election information access (SAnews.gov.za, 2014). Accessible on both Android and iOS platforms, the app allows users to verify, confirm, or update their residential addresses; to review their registration details; to verify their designated voting stations; to apply to cast special votes; and to access election results. In short, the app seeks to serve as a tool for streamlining and promoting civic engagement in the South African electoral process.

To harness the IEC app's functionalities, each user is required to input their 13-digit South African national identification number, along with their physical address details. This information serves as the basis for verifying and updating their registration status, ward number, and current voting station. Thus, one element of the app's functionality is the receipt of personal information such as ID number, physical and IP address, and email address.[2] Accordingly, the study presented in this article examined the data protection aspects of the app, with a focus on the privacy and security of users' personal information. Using open-source tools designed for Android app analysis, we sought to identify any potential risks or vulnerabilities posed by the app to its users. Users of the IEC App must create a profile to access certain features, such as registering to vote or checking their voter status. During the sign-up process, individuals must provide their South African ID number, which is used to verify their eligibility to vote. Additionally, the app may require users to input contact details, such as a phone number or an email address, to facilitate verification and ensure secure communication, especially for features like special voting applications. This information allows the app to send important notifications about election updates and deadlines. The IEC ensures that personal data collected through the app is protected in accordance with South Africa's Protection of Personal Information Act of 2013 (POPIA), with the data being used exclusively for election-related purposes (RSA, 2013).

Our study took place against the background of global and African continental trends towards the increased use of digital technology in democratic processes. The primary objectives of these technological solutions are to mitigate electoral fraud, augment transparency, and foster citizen trust in electoral processes (Micheni & Murumba, 2018; Obiefuna-Oguejiofor, 2018). The results of these technologically-driven efforts

[1] https://www.elections.org.za/pw/Voter/IEC-Mobile-App

[2] POPIA defines "personal information" as information about an identifiable and living natural person, and, where applicable, an identifiable and existing juristic person (RSA, 2013).

are mixed, with improvements seen in some processes and challenges persisting in others—owing in part to the complex nature of both digital technological systems and electoral procedures, which can result in deficiencies in transparency for votersand even for election administrators (see Cheeseman et al., 2018, for an overview).

2. Background: Elections and technology

Digital technologies are introduced into election-voting processes to enhance the processes' functioning and legitimacy, i.e., in order to make voting more efficient, trustworthy, and extensive (Power et al., 2021). The Information and Communication Technologies (ICTs) in Elections database, compiled by the International Institute for Democracy and Electoral Assistance, identified, as of March 2024, 41 African countries that were using digital technology for some aspect of their elections (International IDEA, 2024). Of those countries, two—Namibia and the Democratic Republic of the Congo—were using e-voting systems (International IDEA, 2024). Meanwhile, several African countries were employing technology for voter registration, verification, and management (including biometrics), and results-sharing (International IDEA, 2024). According to the International IDEA database, 28 African countries (see Table 1) were, as of December 2024, using at least one form of biometric data capture (photos and/or fingerprints) as part of their voter registration and identification procedures (International IDEA, 2024). South Africa does not use biometrics for voter registration and identification procedures.

Table 1: Biometric data capture for voter registration/identification in Africa

Biometric data capture during registration
Yes (with fingerprint scans and photos): 24 countries Yes (photos only): 1 country Yes (photos from civil registry): 1 country Yes (with additional biometrics like iris/signatures): 2 countries No: 13 countries Not applicable: 5 countries No data: 5 countries
Biometric data used for Voter ID at polling stations
Yes: 17 countries No: 25 countries No data: 8 countries
Electronic poll books used
Yes, with online access: 1 country Yes, with offline access only: 8 countries No: 38 countries No data: 3 countries

***Note*. Source: International IDEA (2024).**

To ensure the sustainable and safe adoption of technology in elections, data privacy and security are crucial. This is because technological systems may result in, inter alia, data breaches, misuse of personal data, erroneous electoral results, and/or manipulated or rigged electoral results. One concern is the opaque nature of certain proprietary systems. Of the 41 countries identified (as mentioned above) by International IDEA as using digital technology for some aspect of their elections, none was incorporating open-source technologies into these processes (International IDEA, 2024). Unlike proprietary systems, open-source platforms make their source code accessible, which promotes transparency, quicker issue resolution, and public trust.

Also useful in increasing public trust is the embrace of open data principles, which can significantly enhance the transparency and accessibility of electoral processes. Election agencies can open voting data for reuse without limits by adopting open data protocols. By using suitable formats, the public, reporters, observers, and civil society do their own analyses. In Burkina Faso's 2015 election, open data allowed citizens to check official results against independent monitoring (Carolan, 2015; Carolan & Wolf, 2017).

With respect to the impact of emerging technologies on elections, tools such as blockchain and encryption are gaining attention in some parts of the world, due to their potential to boost security and transparency (Barnes et al., 2016). Notably, the US state of West Virginia implemented a blockchain-based mobile voting app in 2018 (Tambanis, 2019), thus allowing overseas military personnel to securely vote. Estonia has been using blockchain in national elections since 2014 (Mulholland, 2021). Proponents of AI suggest that this cluster of technologies can get more citizens involved, help officials to make data-informed choices about elections, and assist voter registration (see UNDP, 2021). However, it must be borne in mind that AI tools, like all ICTs, are socio-technical in nature. Put differently, the perceived legitimacy of digital election technologies hinges on the political will of all political parties and citizens to accept the process (Evrensel, 2010).

In the 2010s, many development agencies pushed biometric tech for voter registration, selling expensive systems as the "new standard" (Bassey & Netshipise, 2013). It was claimed that such systems would curb political meddling. Where democracy is shaky, biometrics can indeed improve credibility somewhat, but their utility in established democracies is less clear (Gelb & Diofasi, 2016). As Debos (2016, p. 1) writes, "even comprehensive biometric systems don't guarantee fair, transparent elections". And Iwuoha's (2018) study of rural Nigerian voters found them to be wary of biometrics.

With regard to the use of digital technology by South Africa's IEC, the organisation introduced voter management devices (VMDs) in 2021, for the aforementioned local government elections. A VMD "is a tablet with internet access and customised for election management only. This hand-held device can function as the

IEC's voter registration portal, track live voter participation, and facilitate the management of voting staff and logistics" (Maseko, 2024, p. 28). The aim was to create a live, centrally connected voters' roll, thus preventing double-voting and improving ballot management (Mzekandaba, 2021). Despite the fact that initial challenges affected thousands of voters, the IEC has defended the VMDs as a crucial advance in electoral management (Khumalo, 2021).

Also in 2021, the IEC launched an online voter registration facility, allowing new voters to register and existing voters to update their information remotely. This initiative was part of the IEC's ongoing efforts to increase accessibility and convenience for voters, particularly young and first-time voters. In order to maintain the integrity of the voters' roll, the online system includes security measures such as one-time-PIN verification and ID document submission.

However, the IEC has faced some setbacks in its digital initiatives. In March 2024, the IEC reported an unauthorised disclosure, on social media, of non-public, IEC-held candidate lists filed by political parties, prompting an investigation and raising concerns about data privacy (Moyo, 2024). At the time of finalising this article in mid-2024, the IEC had, in response to the leak, notified the Information Regulator, was working to establish the source of the unauthorised disclosure, and was seeking to address the leak's implications in terms of POPIA (Moyo, 2024; RSA, 2013).

At the same time as technological elements are having a growing influence on the conduct and credibility of electoral processes, numerous non-technological factors continue to strongly impact the legitimacy of elections. Election bodies continue to require sufficient and reliable funding for staffing and implementation of their duties, including voter registration, candidate nominations, campaign finance oversight, voting, and counting. Concurrently, public monitoring can improve the fairness of election administration by, for instance, monitoring vote-tallying or exposing how prejudice and gender gaps can alienate people from democracy (see Schaffer, 2008, p. vii). The success of electoral management bodies also, crucially, depends on their (actual and perceived) independence (Mozaffar, 2002). Ethnic divisions and patronage politics can erode such independence, as can lingering colonial-era institutions, norms, and practices. Thus, it is essential to insulate an electoral management body from its country's executive branch of government (Fall et al., 2011). Severe challenges emerge when electoral agencies are perceived as favouring incumbents (Akokpari, 2012).

In summary, while digitising election processes has clear uses, care must be taken to ensure that the use of such tools does not neglect or exacerbate other, non-digital, forces that are fundamental to politics. As Akokpari (2012) has found, African elections often happen in an "atmosphere of insecurity" (2012, p. 1).

3. Methodology

This study, conducted in July to August 2023, was a security and privacy analysis of the Android version of the IEC app. First, we conducted a compliance analysis of the IEC's privacy policy against South African data protection legislation, particularly POPIA (RSA, 2013). This examination aimed to assess the alignment of the app's stated privacy practices with legal requirements. Next, adopting a static-analysis approach (as opposed to dynamic analysis[3]), we conducted a scan of the app's APK (Android Package)[4] files, and we scrutinised the app's code and configurations.[5] The objective was to identify, without the need for manual execution, potential security weaknesses and privacy concerns. The static analysis focused on three main components:

- Sensitive permissions and API calls: Evaluating the app's interaction with user devices and potential privacy risks.
- Third-party trackers: Assessing embedded trackers and their impact on user privacy.
- Vulnerabilities: Identifying misconfigurations, weaknesses, and other vulnerabilities that could compromise app security.

To initiate the analysis, the research team obtained the most recent Android version (as of July 2023) of the IEC app using the scrapper 4CAT.[6] The analysis used 4CAT (to extract details pages for the app listing), and AppInspect,[7] which decompiled the app to its source code. The analysis also employed additional tools, including Disconnect[8] and Exodus,[9] to cross-verify some of the obtained results. To conduct the static analysis of the IEC app's vulnerabilities, we downloaded the source APK

[3] Dynamic analysis involves observing an application's behaviour during execution, often using tools such as Android emulators that simulate the Android operating system in a virtual environment. While these emulators are valuable for understanding app behaviour, especially in scenarios involving potential malware (or during simulated cyber-breaches aiming to identify vulnerabilities), the legal uncertainties associated with dynamic analysis prompted our decision to solely rely on static analysis. Dynamic analysis remains an option for prospective IEC app developers to explore and address potential issues, as static analysis has certain limitations that may lead to false positives or negatives, and static analysis may also require the manual configuration of rules or standards.

[4] An APK (.apk) is a file used for packaging and distributing applications specifically designed for the Android operating system. It contains the program's code, resources (such as images and layouts), configuration files, and metadata required for installation and execution on Android devices. APK files can be obtained from app stores such as Google Play.

[5] Static application security testing (SAST) examines the source code or compiled code of an application without executing it. It is a form of "white box" testing, where the security analysis is performed on the application's static code or binaries (Autili et al., 2021).

[6] https://github.com/digitalmethodsinitiative/4cat/wiki/Installing-4CAT

[7] https://appinspect.phil.uni-siegen.de

[8] https://disconnect.me/disconnect

[9] https://reports.exodus-privacy.eu.org

from Google Play, uploaded it to the Quick Android Review Kit (QARK) (Trummer, 2015), a specialised tool for Android security assessments, and ran specific queries to look for vulnerabilities as indicated in the QARK documentation page (LinkedIn, 2019).

To validate and contextualise our findings, we compared our analysis results against the information provided to users in the app stores and the app's privacy policy. This allowed us to identify any disparities and assess the extent to which the application adhered to its stated privacy and security practices. We were careful to avoid any testing methods that could potentially raise legal or security concerns for the operating environment or user data.

4. Findings and analysis

Compliance with POPIA

South Africa's POPIA gives effect to the constitutional right to privacy; regulates the use of personal details such as ID numbers, contact details, and physical addresses; and restricts the use of information about the educational, medical, financial, criminal, or employment history of an individual (RSA, 2013). Section 18 requires notification of the data subject when personal information is collected: "the responsible party must take reasonably practicable steps" to ensure that the data subject is aware of how their data is being collected, which data is being collected, and why and where it is being retained (RSA, 2013). In its preamble, POPIA states that "the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information" (RSA, 2013).

The IEC app does not have its own privacy and security provisions. Rather, the IEC website's terms and conditions are linked, in Google Play and Apple's App Store, as the privacy and security policy for the app. The IEC website's provisions on privacy, as detailed in section 7 of its online disclaimer (IEC, n.d.), contain broad language that fails to address the specific data collection and sharing practices of its app. Section 7 of the disclaimer states:

> 7.5. The IEC may collect, maintain, save, compile, share, disclose and sell any information collected from users, subject to the following provisions:
> 7.5.1. IEC shall not disclose personal information from Users unless the User consents thereto.
> 7.5.2. IEC shall disclose information without the User's consent only through due legal process.
> 7.5.3. IEC may compile, use and share any information that does not relate to any specific individual.

The above-listed IEC privacy provisions refer to the collection of personal information that is not disclosed in the data safety section in the Google Play app store. In addition, the terms and conditions fail to emphasise users' privacy and data rights in respect of the personal data that is collected.

Meanwhile, the IEC's security provisions, provided in section 9 of its online disclaimer (IEC, n.d.), state that the "IEC is under no legal duty to encrypt any content or communications from and to the IEC's website and is also under no legal duty to provide digital authentication of any page on the IEC website".

However, in terms of section 19 of POPIA, the IEC has a legal duty to secure personal information that it collects. Thus, the IEC's data privacy and security provisions, as stated in their online disclaimer, do not comply with POPIA. Also, as analysed below in the "Permissions" subsection, the IEC privacy provisions cannot justify certain permission requests (e.g., ACCESS_FINE_LOCATION) that the IEC app makes.

App details

In July 2023, using 4CAT, app details pages for the IEC app were extracted, containing information about the title and app version, app developer names, publication date, date of recent update, download statistics, reviews, and ratings.

Table 2: IEC app details (as of July 2023)

Title and app version	IEC South Africa, 5.1.7
Category	News & Magazines
Published date	April 15, 2014
Updated on	December 9, 2022
Developer link and ID	https://play.google.com/store/apps/developer?id=Electoral+Commission+of+South+Africa+(IEC) , za.org.elections.iecapp
Developer name	Electoral Commission of South Africa (IEC)
Number of downloads	100,000
Data safety	No data shared with third parties; no data collected
Rating (out of 5)	4.04/5
Number of reviews	1,114

Note: **Source: Public data for the IEC app in Google Play, collected by authors using 4CAT.**

Google Play displays estimated download numbers for an app once it surpasses 1,000 downloads, with downloads representing active installs.

Permissions

An app's permissions list shows what specific data or features an app can access, or might request access to, on a mobile device on which the app is installed. An app's permissions are listed as part of its description in Google Play. The IEC app's permissions list is presented in Table 3.

Table 3: IEC app's permissions list

Permission	Description
Location	Approximate location (network-based)
Location	Precise location (GPS and network-based)
Location	Access extra location provider commands
Photos/media/files	Read the contents of your USB storage
Photos/media/files	Modify or delete the contents of your USB storage
Storage	Read the contents of your USB storage
Storage	Modify or delete the contents of your USB storage
Wi-Fi connection information	View Wi-Fi connections
Other	View network connections, view network access, read Google service configuration

Note: **Source: Collected by authors using 4CAT.**

The analysis of the app's permissions found several permissions classified, by Google's protection levels, as "dangerous" or "special level", meaning that these apps could compromise users' data security (Android Developers, n.d.-b). The permissions in question included:

1. ACCESS_COARSE_LOCATION: Access approximate location only in the foreground.
2. ACCESS_FINE_LOCATION: Access precise location only in the foreground.
3. WRITE_EXTERNAL_STORAGE: Modify or delete the contents of your shared storage.

These permissions are categorised as "dangerous" because they can directly impact user privacy and security if misused. Android requires that apps explicitly request these permissions from the user at runtime, allowing users to make informed decisions about whether to grant these potentially risky permissions to an app.

It is important to note that permissions that are not classified as dangerous may still reveal sensitive information, especially in a political context. The IEC app permissions include access to Wi-Fi information, which allows the app to retrieve information about which Wi-Fi networks the user is connected to. Such data can reveal information such as for how long certain users stayed in a similar location, how often, when exactly, and so on (Alepis & Patsakis, 2019).

While the IEC app's data safety provisions claim no data-sharing with third parties, the permissions list presents a different perspective. The difference might be due to data being processed locally on devices without being shared, or certain types of data not being counted. Notably, the absence of data details, including details on the collection of users' IDs, amplifies privacy concerns. Moreover, the presence of ad trackers (see the subsection on "Trackers" below) contradicts the IEC app's data safety provisions' assertion of no third-party data sharing. According to the Google Play Developer documentation, differences between the app permissions list and the data safety section could result from:

- the app accessing data for on-device processing without collecting or sharing it;
- data collection occurring in a way not governed by permissions; and
- services or data types listed in permissions not being covered in the data safety section.

As mentioned in this article's Introduction, the collection of users' ID numbers introduces potential privacy breaches due to the wealth of information encoded within them. The South African ID number is a 13-digit code with the format YYMMDDSSSSCAZ:

- The first six digits (YYMMDD) represent the date of birth (e.g., 940510 for 10 May 1994);
- The next four digits (SSSS) denote gender, with 0000–4999 for females and 5000–9999 for males;
- The next digit (C) indicates citizenship status (0 for a South African citizen, 1 for a permanent resident, and 2 for a refugee); and
- The last digit (Z) is a checksum digit, validated using the Luhn algorithm.

Decrypting this number reveals extensive personal information about voters, underscoring the need for encryption to protect sensitive app data. However, according to the app information, currently no data encryption is used. Moreover, concerns arise from the lack of information about user data deletion requests. The IEC data privacy and data safety provisions do not currently address users' ability to request data deletion (IEC, n.d.). To address these concerns, it is imperative to adopt data minimisation and transparency measures.

Trackers

As seen below in Table 4, we identified, using AppInspect, seven third-party trackers being used by the IEC app. A tracker is a piece of software in a mobile app whose task is to gather information on the person using the application, how they use it, and/or the smartphone they are using. Trackers can collect and transmit sensitive user data, such as personal information, browsing habits, location data, and more, without the user's explicit knowledge or consent.

The integration of trackers into an electoral body's mobile app introduces both opportunities and challenges. Trackers can offer election organisers valuable insights into voter engagement, preferences, and behaviour. Furthermore, trackers can help to identify potential issues or glitches within the app, ensuring a seamless user experience during critical moments like real-time election results reporting. However, the use of trackers in election apps also raises important concerns about user privacy and data security. Transparency is of paramount importance, requiring clear communication with users about the types of data being collected, how it will be used, and the security measures that are in place to protect it. Striking the right balance between harnessing the benefits of app trackers and safeguarding users' personal information is crucial to maintaining trust and legitimacy in the democratic process. Therefore, the responsible integration of trackers in election mobile apps requires adherence to stringent privacy standards, compliance with relevant regulations, and a commitment to ethical data handling practices.

Table 4: Seven trackers identified

App ID, version name, version code	APK_SHA256	Classes	Trackers	Tracker categories	Domains	Tracker count	Domain count
za.org.elections.iecapp 500017 5.1.7	c9829d0d0c87d09ec89880f8338d121cae3f709f6894eb427e3ce81639970ea0	com.microsoft.appcenter.ingestion.AppCenterIngestion	Google	xray	googlesyndication.com	4	4
		com.microsoft.appcenter.ingestion.OneCollectorIngestion	Microsoft		appcenter.ms		
		com.google.android.gms.common.internal.zzaj	App Center		microsoft.com		
		com.google.android.gms.auth.api.signin.GoogleSignInOptions	AdSense		Google		
		com.google.android.gms.ads.identifier.zze					
		com.google.android.gms.common.internal.zzaj	Google AdMob	exodus	Google.com	1	1
		Microsoft Visual Studio Microsoft Visual Studio	App Center Analytics App Center Crashes	exodus		2	

Note: **Source: Output from the IEC app, generated by authors using AppInspect.**

From our analysis, and as summarised in Table 3, we found the following categories of trackers:

Advertising trackers

Google AdMob,[10] a mobile advertising platform provided by Google, is different from Google AdSense.[11] AdMob is focused on mobile app advertising, while AdSense is designed for website publishers to display targeted adverts on their sites. AdMob allows app developers to monetise their apps by displaying adverts from various advertisers. The package name "com.google.android.gms.common.internal.zzaj" might be used internally within the app to handle AdMob functionalities. AdMob provides various advert formats, such as banner adverts, interstitial adverts, native adverts, and rewarded adverts. These adverts can be displayed within the app to generate revenue for the app developer. Additionally, AdMob offers various tools and features to track advert performance, user interactions, and other metrics to optimise advertising revenue. These trackers aim to identify the app user to serve them targeted adverts. The goal of such a tracker is, thus, to monetise the app.

Analytics and crashing trackers

These tracking capabilities allow developers to monitor the performance and use of their apps, track user engagement, and gain insights into crashes or issues that users may encounter, such as app centres. The presence of advert trackers within the app suggests potential third-party data sharing, contrary to the app's stated data safety policies. Advert trackers can construct detailed user profiles, enabling targeted adverts and potentially influencing user behaviour. This has particular importance in election contexts, as user data can be "weaponised" to influence voter conduct.

Moreover, analytics trackers that gather user behaviour data have the capability to anticipate future actions to a certain degree. Predictive analytics harness historical data to project forthcoming events or conduct (Cote, 2021). Despite their potency, predictive analytics remain inherently flawed, susceptible to unforeseeable variables and the evolving nature of user actions over time. In the elections setting, this imperfection can be manipulated, potentially leading to targeted campaigns aimed at voters based on the extracted data. Given that predictive analytics rely heavily on expansive datasets, robust measures to safeguard user privacy are necessary. The utmost consideration for privacy is imperative when dealing with user behaviour data.

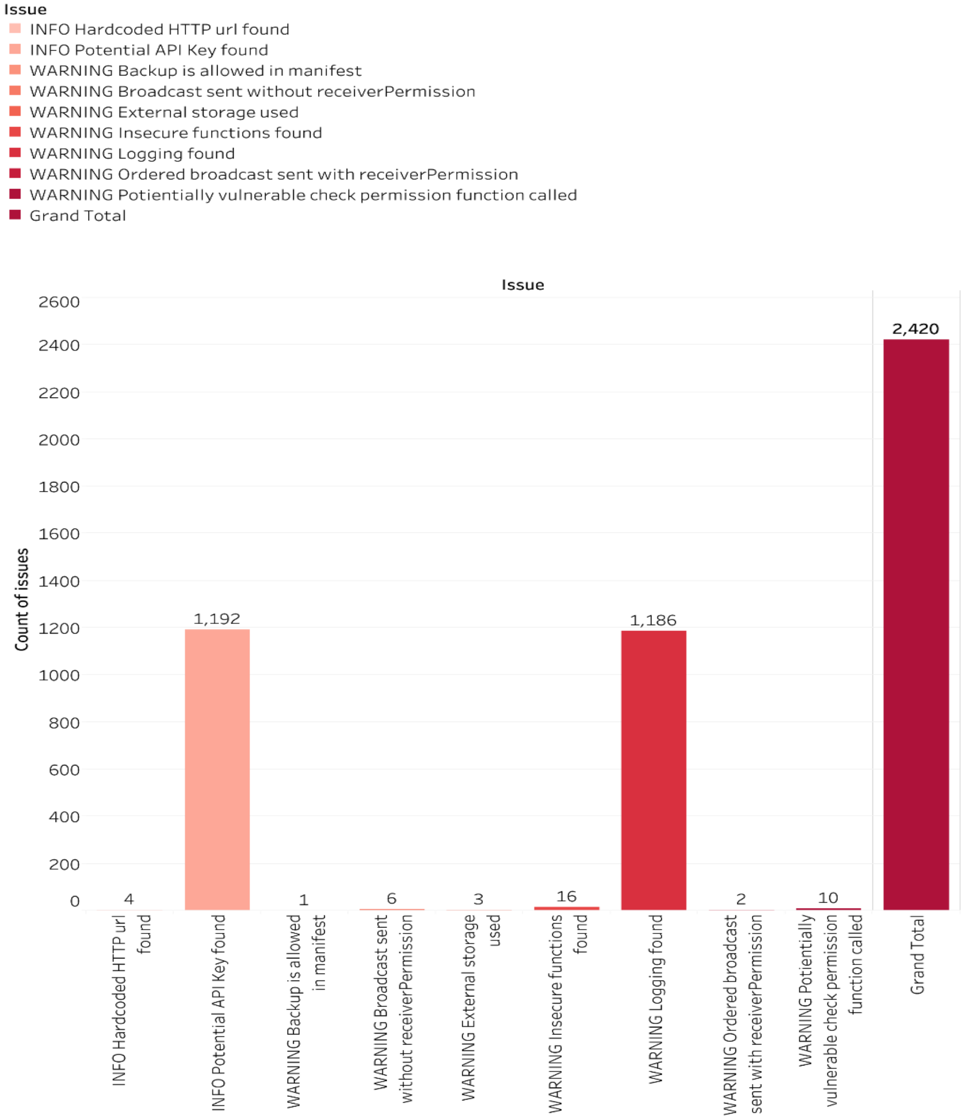
Vulnerabilities

We conducted static analysis of the app's vulnerabilities using QARK, as described in the "Methodology" section. This analysis revealed several vulnerabilities. Figure 1 and Tables 6 and 6 summarise the findings from the analysis.

[10] https://admob.google.com/home

[11] https://adsense.google.com/start

Figure 1: Vulnerabilities identified with QARK



Note. **Source: Authors, based on QARK analysis.**

According to the QARK analysis, 1,190 potential API keys were identified in the source code, alongside warnings of issues that could lead to serious security breaches (Table 5).

Table 5: Potential API keys identified with QARK

Issue	Description	Count
INFO Hardcoded HTTP url found	Application contains hardcoded HTTP url: http://schemas.android.com/apk/res/android, unless HSTS is implemented, this request can be intercepted and modified by a man-in-the-middle attack.	4
INFO Potential API Key found	Please confirm and investigate the API key to determine its severity.	1,190
INFO Potential API Key found	Please confirm and investigate for potential API keys to determine severity.	2
WARNING Backup is allowed in manifest	Backups enabled: Potential for data theft via local attacks via adb backup, if the device has USB debugging enabled (not common). More info: http://developer.android.com/reference/android/R.attr.html#allowBackup	1
WARNING Broadcast sent without receiverPermission	A broadcast, sendBroadcast which does not specify the receiverPermission. This means any application on the device can receive this broadcast. You should investigate this for potential data leakage.	6
WARNING External storage used	Reading files stored on {storage_location} makes it vulnerable to data injection attacks. Note that this code does no error checking and there is no security enforced with these files. For example, any application holding WRITE_EXTERNAL_STORAGE can write to these files. Reference: https://developer.android.com/reference/android/content/Context.html	3
WARNING Insecure functions found	The content provider API provides a method call. The framework does no permission checking on this entry into the content provider besides the basic ability for the application to get access to the provider at all. Any implementation of this method must do its own permission checks on incoming calls to make sure they are allowed. Failure to do so will allow unauthorized components to interact with the content provider. Reference: https://bitbucket.org/secure-it-i/android-app-vulnerability-benchmarks/src/d5305b9481df3502e60e98fa352d5f58e4a69044/ICC/WeakChecksOnDynamicInvocation-InformationExposure/?at=master	16
WARNING Logging found	Logs are detected. This may allow potential leakage of information from Android applications. Logs should never be compiled into an application except during development. Reference: https://developer.android.com/reference/android/util/Log.html	1,186
WARNING Ordered broadcast sent with receiverPermission	A broadcast, sendOrderedBroadcast which specifies the receiverPermission, but depending on the protection level of the permission (on the receiving app side), may still be vulnerable to interception, if the protection level of the permission is not set to signature or signatureOrSystem. You should investigate this for potential data leakage.	2
WARNING Potentially vulnerable check permission function called	Be careful with use of Check permission function Apps may be vulnerable to Privilege escalation or Confused Deputy Attack. This function can grant access to malicious applications, lacking the appropriate permission, by assuming your applications' permissions. This means a malicious application, without appropriate permissions, can bypass its permission check by using your application permission to get access to otherwise denied resources. Use - checkCallingPermission instead. Reference: https://developer.android.com/reference/android/content/Context.html	10

***Note*. Source: Authors, based on QARK analysis.**

Some security concerns arising from this analysis include inadequately secured API keys that can be exploited for unauthorised access, data breaches, and API abuse. Proper API key security is essential to protect user privacy and security. Regarding API key management, it is crucial to avoid hardcoding them in the application's source code. Secure storage strategies outside the source code must be implemented.

Furthermore, logging sensitive information exposes critical data to potential attackers, compromising security. Logs should not be compiled into the application except during development. While invaluable for debugging, logs should be handled differently in production due to security, privacy, and compliance concerns:

- Privacy compliance: Unnecessary logging might breach privacy laws and lead to legal consequences;
- Sensitive information leakage: Detailed error messages and technical data in logs can be exploited by attackers.

Additionally, voters' mobile devices could be geolocated and physically tracked, resulting in privacy risks. Sensitive personal information (such as religion, political, social, and cultural information) can be inferred from mobility traces, and connections to various networks introduce security and privacy risks. Third-party cross-domain tracking combines physical and online profiles. It can provide a more complete view of a user's behaviour and introduces new privacy and security risks. Cross-device tracking, where third parties try to link together the devices that belong to a user, or cross-app tracking, where an app tries to identify or track the other installed apps on the device, are also expanding practices that introduce new and severe privacy concerns. Cross-device and cross-app tracking predict user traits from mobile apps. For example, user traits, such as religion, relationship status, spoken languages, interest, and family structure, can be predicted from a subset of the list on mobile apps. User traits can also be tracked by third parties on the internet when the user goes online.

Table 6 provides a snapshot of the IEC app's structure, dependencies, and network communications, which can provide some insight for security analysis, compatibility checking, or understanding the app's functionality. The table shows how the IEC app incorporates various third-party services, and the presence of advert-related classes and domains. While secure communication is implied by the use of HTTPS URLs, the presence of analytics and the advert-related component suggests that the IEC app probably collects user data for advertising purposes, thus raising potential privacy considerations.

Table 6: IEC app's structure, dependencies, and network communications

App ID, version name, version code	APK_SHA256	Classes	Domains	Domain count	URL count
za.org.elections.iecapp 5.1.7 500017	c9829d0d0c-87d09ec89880f-8338d121cae3f-709f6894eb427e-3ce81639970ea0	android.support.v4.content.res.TypedArrayUtils com.microsoft.appcenter.ingestion.OneCollectorIngestion com.google.android.gms.common.internal.zzaj com.google.android.gms.auth.api.signin.GoogleSignInOptions com.google.android.gms.ads.identifier.zze	mobile.events.data.microsoft.com pagead2.googlesyndication.com schemas.android.com plus.google.com www.googleapis.com	5	5

Note: **Source: Output from QARK analysis generated by authors.**

5. Conclusions

To safeguard user privacy and security, app developers must ensure transparent data collection practices and obtain explicit user consent. Thorough privacy and security reviews of third-party services are crucial to minimise risks, especially when considering the potential privacy concerns posed by Google AdMob, Google AdSense, and App Center trackers, which collect data for adverts and performance improvement. Additionally, the potential presence of API keys and logs, along with other security vulnerabilities, creates significant cybersecurity risks for the app and users' data.

Adhering to privacy policies set by advertising platforms and transparently disclosing data collection, opt-out options, and data deletion are vital steps in maintaining user trust and security. Data minimisation is also essential, as it helps to reduce privacy risks. For example, storing generalised location data instead of precise coordinates exemplifies data minimisation. The IEC app's privacy and security issues must be addressed immediately. By prioritising user privacy, the app's developers can ensure data security and trust, fostering a safer digital environment.

As seen above, this study has identified discrepancies between permissions granted and data safety claims. Among other things, South African ID numbers are collected, and the presence of advertising and analytics trackers suggests third-party data-sharing.

The integration of ICTs (either systems or mobile apps) into the democratic process demands meticulous planning and thoughtful design to ensure public confidence. Drawing lessons from past experiences with electronic voting and dedicating adequate time and resources to implementation are essential steps. All stakeholders, including election managers, observers, international organisations, vendors, and standardisation bodies, must be proactive and cautious in adapting to the rapid evolution of technology (International IDEA, 2011). This entails continuous updates, security enhancements, and privacy measures to safeguard data integrity and foster transparency. We have identified potential security vulnerabilities within the IEC app that could compromise the security of voters' sensitive information. Furthermore, the app's use of dangerous permissions, as previously discussed, heightens the possibility of security risks. Consequently, it is imperative to prioritise the security of the app.

To counteract the potential negative outcomes arising from exploiting vulnerabilities in election apps, an in-depth analysis is indispensable, before an app's deployment, for pinpointing and rectifying security weaknesses that attackers could exploit. Our approach encompassed the use of static analysis to evaluate the IEC app, with the aim of identifying critical vulnerabilities. Similar techniques, including the employment of a range of open tools tailored to specific requirements, can amplify the capabilities of the analysis of the controls that secure hardware, software, networks, and data. This kind of analysis can aid in strengthening an app's security and safeguarding of sensitive voter data.

For election officials, gaining a comprehensive understanding of the risks that they could encounter during the implementation of digital systems is imperative for effective risk mitigation. As this study has illustrated, security audits can assist in pinpointing key areas of risk, ensuring that cybersecurity meets critical requirements, and establishing a solid foundation for collaborative risk management at all levels. The design, construction, and operation of such AI-powered systems should be guided by best practices and adherence to existing legal frameworks.

The insights emerging from this study can serve as a reference point for policymakers and future researchers. Moreover, the findings shed light on potential security enhancements and best practices for app developers. Of central importance is the fostering of a culture of transparency and accountability among system developers and governments, encouraging them to proactively address potential shortcomings in their applications to create a safer and more secure digital environment for users, particularly before an election process begins.

Acknowledgements
We wish to thank Hanani Hlomani, Andrew Rens, and Araba Sey for early inputs on the design of the study. The journal's editors and peer-reviewers helped us to deliver the best version of the manuscript.

Funding

The research informing this article was made possible by a grant to the Research ICT Africa (RIA) Just AI project from Canada's International Development Research Centre (IDRC) and the Swedish International Development Cooperation Agency (SIDA).

Data availability

The data supporting the results of this study is available upon written request to Scott Timcke at stimcke@researchictafrica.net

AI declaration

No generative AI tools were used in the research or in the production of this manuscript.

Authors' contributions

N.O.: Methodology, data collection, sample analysis, data curation, data visualisation, writing and revisions.
S.T.: Conceptualisation, methodology, writing and revisions, project management.
Both authors read and approved the final manuscript.

Competing interests

The second-listed author, Scott Timcke, was an IEC election observer during the 2024 South African national and provincial elections. Nevertheless, the authors have no competing interests to declare.

References

Akokpari, J. (2012). Is electoral politics a new source of human insecurity in Africa? *Afro Asian Journal of Social Sciences*, *3*(2), 1–24.

Alepis, E., & Patsakis, C. (2019). Unravelling security issues of runtime permissions in Android. *Journal of Hardware and Systems Security*, 3, 45–63. https://doi.org/10.1007/s41635-018-0053-2

Android Developers. (n.d.-a). Android debug bridge (adb). https://developer.android.com/tools/adb

Android Developers. (n.d.-b). Permissions on Android. https://developer.android.com/guide/topics/permissions/overview

Autili, M., Malavolta, I., Perucci, A., Scoccia, G. L., & Verdecchia, R. (2021). Software engineering techniques for statically analyzing mobile apps: Research trends, characteristics, and potential for industrial adoption. *Journal of Internet Services and Applications*, *12*(3), 1–60. https://doi.org/10.1186/s13174-021-00134-x

Barnes, A., Brake, C., & Perry, T. (2016). *Digital voting with the use of blockchain technology*. Plymouth University. https://www.economist.com/sites/default/files/plymouth.pdf

Bassey, I., & Netshipise, N. (2013). Extending e-democracy to enhance voter registration and identification: South Africa elections perspective. *International Journal of Computer Science & Engineering Technology*, *4*(1), 35–43.

Carolan, L. (2015, December 10). Why data was crucial to Burkina Faso's first election since uprising. *Data Blog*. World Bank. https://blogs.worldbank.org/en/opendata/why-data-was-crucial-burkina-faso-s-first-election-uprising.

Carolan, L., & Wolf, P. (2017). *Open data in electoral administration*. International IDEA. https://doi.org/10.31752/idea.2017.5

Cheeseman, N., Lynch, G., & Willis, J. (2018). Digital dilemmas: The unintended consequences of election technology. *Democratization*, *25*(8), 1397–1418. https://doi.org/10.1080/13510347.2018.1470165

Cote, C. (2021, October 26). What is predictive analytics? 5 examples. *Business Insights Blog*. Harvard Business School Online.

Debos, M. (2016, May 4). Biometric voting in Chad: New technology, same old political tricks. *The Conversation*. https://theconversation.com/biometric-voting-in-chad-new-technology-same-old-political-tricks-58663

Enguehard, C. (2008). Transparency in electronic voting: The great challenge. Paper presented to Conference on "E-democracy – State of the art and future agenda", 22–24 January, Stellenbosch, South Africa.

Evrensel, A. (Ed.) (2010). *Voter registration in Africa: A comparative analysis.* Electoral Institute for the Sustainability of Democracy in Africa (EISA). https://www.eisa.org/wp-content/uploads/2023/05/edited-volume-2010-voter-registration-comparative-analysis-south-africa-eisa-publication.pdf

Fall, I. M., Hounkpe, M., Jinadu, A. L., & Kambale, P. (2011). *Election management bodies in West Africa: A comparative study of the contribution of electoral commissions to the strengthening of democracy*. Open Society Foundations. https://www.africanminds.co.za/wp-content/uploads/2016/05/9781920489168_txt.pdf

Gelb, A., & Diofasi, A. (2016). *Biometric elections in poor countries: Wasteful or a worthwhile investment?* Center for Global Development. https://doi.org/10.2139/ssrn.2848544

Gentile, B. (2010, September 30). *Transparency, participation, and collaboration: The distinguishing principles of open source*. opensource.com. https://opensource.com/principles

IEC: Electoral Commission of South Africa. (n.d.). Disclaimer. https://www.elections.org.za/pw/Disclaimer

IEC: Electoral Commission of South Africa. (2021, July 14). Electoral Commission launches online voter registration. https://www.elections.org.za/content/About-Us/News/Electoral-Commission-Launches-Online-Voter-Registration/

International Institute for Democracy and Electoral Assistance (International IDEA). (2011). *Introducing electronic voting: Essential considerations*. https://www.idea.int/sites/default/files/publications/introducing-electronic-voting.pdf

International IDEA. (2024). ICTs in elections database [Dataset]. https://www.idea.int/data-tools/data/icts-elections

Iwuoha, V. C. (2018). ICT and elections in Nigeria: Rural dynamics of biometric voting technology adoption. *Africa Spectrum*, *53*(3), 89–113. https://doi.org/10.1177/000203971805300304

Jones, S. (2017). *Digital solutions for political finance reporting and disclosure: A practical guide*. International IDEA.

Khumalo, J. (2021, November 1). IEC defends faulty Voter Management Devices amid party complaints, reports of issues. *News24*. https://www.news24.com/news24/southafrica/news/iec-defends-faulty-voter-management-devices-amid-party-complaints-reports-of-issues-20211101

LinkedIn. (n.d.). Quick Android review kit (QARK). Github. https://github.com/linkedin/qark

Micheni, E., & Murumba, J. (2018). The role of ICT in electoral processes: Case of Kenya. In *2018 IST–Africa Week Conference (IST–Africa)* (pp. 1–11), Gaborone. https://ieeexplore.ieee.org/abstract/document/8417188

Mozaffar, S. (2002). Patterns of electoral governance in Africa's emerging democracies. *International Political Science Review*, *23*(1), 85–101. https://doi.org/10.1177/0192512102023001005

Maseko, M. (2024). Voter management devices in South Africa's elections, 2021–2024. *Journal of African Elections*, *23*(1), 25-48. https://doi.org/10.20940/JAE/2024/v23i1a3

Moyo, A. (2024, March 11). InfoReg demands answers on political candidate lists leak. *ITWeb*.https://www.itweb.co.za/article/inforeg-demands-answers-on-political-candidate-lists-leak/JBwEr7n3eaaM6Db2

Mulholland, P. (2021, January 26). Estonia leads world in making digital voting a reality. *Financial Times*. https://www.ft.com/content/b4425338-6207-49a0-bbfb-6ae5460fc1c1.

Mzekandaba, S. (2021, November 5). New tech "catapulted" electoral management, says IEC. *ITWeb*. https://www.itweb.co.za/article/new-tech-catapulted-electoral-management-says-iec/JN1gP7OYgWwqjL6m

Obiefuna-Oguejiofor, O. (2018). Advancing electronic voting systems in Nigeria's electoral process: Legal challenges and future directions. *Journal of Sustainable Development Law and Policy*, *9*(2), 187–219. https://doi.org/10.4314/jsdlp.v9i2.10

Power, S., Khumalo, S., & Trott, W. (2021, May 24). *Democracy 2.0: Digital voting systems*. alt.advisory. https://altadvisory.africa/2021/05/24/democracy-2-0-digital-voting-systems

Republic of South Africa (RSA). (2013). Protection of Personal Information Act 4 of 2013 (POPIA). https://popia.co.za

SAnews.gov.za. (2014, May 4). IEC releases mobile phone apps. https://www.sanews.gov.za/south-africa/iec-releases-mobile-phone-apps

Schaffer, F. C. (2008). *The hidden costs of clean election reform*. Cornell University Press.

Tambanis, D. (2019, February 5). *Election voting: Blockchain case studies*. *Medium*. https://medium.com/bpfoundation/election-voting-blockchain-case-studies-18321c379529

Trummer, T. (2015, August 17). Introducing QARK: An open source tool to improve Android application security. https://security.linkedin.com/content/security/global/en_us/index/posts/2015/introducing-qark

UN Development Programme (UNDP). (2021, November 17.) AI-powered fact-checking tool iVerify, piloted during Zambia election, shows global promise.