Data Protection and Privacy Brief for Election Observers in Uganda

Democratic engagement is increasingly mediated by digital technology, from campaigning to election results transmission. These technologies rely on collecting, storing, and analysing personal information to operate. They raise novel issues and challenges for all electoral stakeholders on how to protect our data from exploitation.

Elections are about more than voting and the entire election cycle is increasingly data dependent. Voter registration, voter authentication, voting and results transmission all involve the collection of at least some personal data. Political parties depend on data to drive their campaigns, from deciding where to hold rallies, which campaign messages to focus on in which area, and how to target supporters, undecided voters and non-supporters, including with ads on social media. Data exploitation during the election cycle, therefore, risks undermining fundamental democratic processes.

It is important to note that election related technologies thrive on the use of personal data whether through the use of social media platforms for political campaigning, biometric registration of voters or, police monitoring of political rallies.

The purpose of this Data Protection and Privacy briefing for election observers in Uganda is to provide a starting point for discussions that promote transparency and accountability in the use of technology in Uganda's democratic processes, both by the electoral commission and the use of personal data by political parties in campaigning. The goal is to support the conduct of elections that meet international standards, and to help in ensuring the credibility of election results thereof.

Legislation

International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy. The right to privacy is enshrined by the:

1. Universal the Universal Declaration on Human Rights; Article 12
2. International Covenant on Civil and Political Rights: Article 17
3. Convention on the Rights of the Child: Article 16
4. International Convention on the Protection of All Migrant Workers and Members of Their Families: Article 14

At the regional level, the right to privacy is protected by:

1. Cairo Declaration on Human Rights in Islam: Article 18
2. Arab Charter on Human Rights: Articles 16 and 21
3. African Commission on Human and People's Rights Declaration of Principles on Freedom of Expression in Africa
4. African Charter on the Rights and Welfare of the Child: Article 19

Privacy

The 1995 Ugandan constitution explicitly recognises the right to privacy and calls for its protection: Article 27 specifically notes that: (1) No person shall be subjected to— (a) unlawful search of the person, home or other property of that person; or (b) unlawful entry by others of the premises of that person. (2) No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.

Data Protection

In February 2019 Uganda enacted the Data Protection and Privacy Act. The DPPA aims at protecting the privacy of individuals and of personal data by regulating the collection and processing of personal information. It also seeks to provide for the rights of persons whose data is collected. The Act applies to collection, holding and using personal data within Uganda and data collected outside Uganda relating to Ugandan citizens. Two years on from the adoption of the data protection law, there are still concerns about lack of enforcement.

Political parties and actors increasingly rely on personal data to profile and target voters with personalised communications. This practice raises issues in relation to the lawfulness of data acquisition and the level of awareness of individuals regarding how their personal data may be used or shared. Data protection or subsequent regulations are yet to address this in Uganda.

Electoral Laws and the Electoral Commission

In July 2020, the Parliament of Uganda passed amendments to electoral laws that, among other issues, provide for the adoption and use of technology in the management of elections. The Electoral Commission (Amendment) Act 2020[1] amends Section 12 of the Electoral Commission Act[2] relating to additional powers of the commission and regulation of ballot papers by adding the following to Section 12 (1):

"(1a) the commission may, in the exercise of its powers under subsection (l), adopt technology in the management of (lb) notwithstanding the general effect of subsection (1a), the commission shall put in place an electronic display system at every tallying centre on which the votes being

1 file:///C:/Users/UW/Downloads/The%20Electoral%20Commission%20(amendment)%20Act%202020.pdf

tallied shall be displayed to the general public.

(1c) The Minister shall, in consultation with the commission, by statutory instrument, make regulations prescribing the manner in which technology will be used in the management of elections.

(ld) The statutory instrument referred to in subsection (1c) shall be laid before Parliament for information.

The amendments signal forthcoming regulations regarding the use of technology in elections by the electoral commission. Although the technology in question is not specified in the amendments to the Act, it could be related to voter registration (including biometrics), voting, and tallying and results transmission. It will therefore be important for election observers to examine the electoral legal framework alongside the Data Protection and Privacy Act to ensure that personal data is collected and processed within the law and in accordance with international standards during the election cycle.

As a first step, the forthcoming regulations should consider:

- Procedures and requirements for the use of information technology during registration, authentication, electronic voting, counting and tabulation must be accurately reflected in the electoral legislation.
- Previous court challenges to Digital Technologies and the resulting jurisprudence should also be consulted if any.
- Laws and regulations related to the use of technologies in elections need to guarantee respect for international standards of free and fair election and of data protection.
- Access can be provided through the possibility of the electoral commission to test Digital Technologies in an adversarial manner (in which specialists attempt to identify security weaknesses or other flaws in an unscripted manner), or through the review of documentation from the start of the project, including feasibility studies, procurement material, manuals, evaluation and certification reports, source codes, or electronic logs of the system.
- Regardless of which view prevails, Uganda's electoral Laws should clearly address this issue and provide necessary details so that observers, candidates and political parties know precisely what rights they have to access Digital Technologies.
- In terms of security of the Digital Technologies, it is important for election observers to establish whether electoral laws and regulations include criminal provisions for attacks on Digital Technologies systems such as data breaches and theft, with appropriate sanctions for violations. The Digital Technologies should be able to

2 https://www.ec.or.ug/docs/Electoral%20Commission%20Act,%20Uganda.pdf

comply with privacy by design and has in place safeguards against unauthorised access and/or loss of personal data.

- Election observers need to pay special attention to the legal provisions for complaints and appeals relating election results. The legal framework should allow for complaints and legal challenges to be related to the use of the system itself during the voting and counting process or to other elements of the process, such as certification, or to concerns that the Digital Technologies system has failed to function properly.

Election observers should assess the existing laws and regulations in light of the issues raised in these points above.

Automated Data processed by the Electoral Commission and Political Parties.

The protection of an individual voter's personal data has become more critical with the proliferation of electronic technologies in elections. In addition to the general right to privacy and protection of one's personal data, there are specific standards that apply when personal data are "automatically processed".

It is important that election observers assess legal provisions against standards for the automatic processing of data, as well as the general right to privacy as it relates to the election cycle. Personal data is defined as any information relating to an identified or identifiable individual.

Automatic processing includes the following operations if carried out in whole or in part by automated means: collection of data, storage of data, analysing those data, their alteration, erasure, retrieval or dissemination.

Election observers therefore, must ensure that the automatic processing of personal data is subject to the following principles:

- Provisions for the regulation of the automatic processing of personal data;
- Personal data are only collected for specific, limited, explicitly stated and legitimate purposes with the consent of the person;
- Personal data that are processed must be adequate, relevant, correct and, if necessary, up to date;
- All reasonable measures must be taken to complete, correct, block or erase data that are incomplete or incorrect;
- Personal data are not processed for any purpose incompatible with that for which they are collected and no more personal data are processed than is necessary;
- Sensitive data revealing criminal convictions, political opinions, religious beliefs or other beliefs, as well as personal data concerning health may not be processed automatically unless domestic law provides appropriate safeguards
- Appropriate security measures are taken for the protection of personal data against accidental or unauthorized destruction or loss, as well as against unauthorized access, alteration or dissemination;
- Personal data are not kept for a period longer than is necessary;
- Voters are made aware of the existence of automated personal-data files, the categories of personal information contained in the files, and who controls the files;

- Every person has the right to access in an intelligible form, at reasonable intervals and without excessive delay or expense, confirmation of whether her or his personal data are stored in an automated file;
- Every person has the right to have personal data corrected or erased if they are inaccurate or have been processed contrary to the law;
- Every person has a right to a remedy if a request for correction or erasure is not honoured and the request was justified;
- Domestic law must provide appropriate sanctions and remedies for violations of these basic principles; and
- Any exception or restriction in the basic principles are, as with other exceptions and restrictions on human rights, limited to those that are necessary for the protection of fundamental values in a democratic society.

Procurement and Security of Digital Technologies

As the Electoral Commission Act (Amendment) 2020 provides for the adoption and use of technology in the management of elections, we would like to open a discussion as to the transparency, openness and accountability in procuring and securing such technology, and how election observers could go about observing this. Recommendations are:

- If the Digital Technologies are supplied by private vendors, electoral laws (such as the forthcoming regulations as proposed in the Electoral Commission Act (Amendment) 2020 should carefully regulate the responsibility of vendors in order to ensure that there are consequences for failure to fulfil contractual obligations.
- Private vendors should not replace any relevant functions of the electoral commission, which should remain in full control of the electoral process.
- Finally, it is necessary that the legislation covering Digital Technologies be in line with the Data Protection and Privacy Act 2019 and international human rights standards.

The above data protection electoral observer brief should be respected and applied to any data collected during the entire election processes.

Block 381, Plot No. 26, Nsibambi village,
P.O.Box 71314 Clock Tower K'la
Tel: +256 414 697635
Email: info@unwantedwitness.or.ug, Website: www.unwantedwitness.or.ug
Unwantedwitness-Uganda @unwantedwitness unwantedwitness