The Principal Secretary  
Ministry of Interior and Coordination of National Government  
4th Floor, Harambee House  
Harambee Avenue  
NAIROBI

By email: ps@interior.go.ke

Dear Principal Secretary,

RE: Public Participation on National CCTV Policy

Greetings from the Centre for Intellectual Property and Information Technology law (CIPIT) at Strathmore Law School. CIPIT is a Think Tank established in 2012. The scope of our work includes evidence-based research and training in intellectual property and information technology law and policy, especially as they contribute to African law and human rights.

CIPIT is contributing to emerging African approaches to artificial intelligence, and have been active in convening experts on AI development from across the continent. We are also deeply invested in developing the law and policy for robust and inclusive identity, and in that vein we previously submitted a memorandum on the Huduma Bill, 2019 to your Ministry. In our submissions, we highlighted on the intersection between privately held identity data and official ID. CCTV images, in conjunction with other technologies such as facial recognition, contribute to an individual’s digital identity, and influence issues from privacy to evidentiary law. Use of facial recognition has had grave implications on human rights. While it has been useful in immigration procedures at spaces such as airports, it has had many false negatives, especially in law enforcement. People have been wrongly identified using facial recognition from CCTV feeds and then subsequently wrongfully convicted and punished. Jurisdictions that have had long experience with facial recognition, for example San Fransisco are now banning use of facial recognition software to protect human rights. We therefore maintain that such issues require wide discussions due to their far-reaching implications on governance, and we appreciate the Ministry’s efforts toward public participation.

In response to your call for memoranda, we submit herewith our input on the draft National CCTV Policy 2019, more particularly outlined in the attached memorandum. We appreciate the need for guidelines on CCTV as CCTV is a tool that can enhance public safety and emergency response coordination. Conversely, it can also be used for mass surveillance in ways that abrogate human rights. A CCTV policy therefore ought to balance these two complementary interests -- security and human rights. To this end, we recommend that the following changes to the document. The policy should:

a) Discuss protection of the right to privacy in CCTV installations by introducing, among others, data protection principles and creation of awareness among stakeholders on privacy and data protection with CCTV;
b) Further to the right to privacy, incorporate privacy impact assessments in CCTV installations;

c) Delineate use cases and limits for CCTV data by itself or in conjunction with other technologies such as facial recognition;

d) Include grievance redress mechanisms involving private or public CCTV installations; and

e) Expand stakeholders to include public who are surveilled by CCTV as well as courts.

Please find attached a detailed analysis of the policy. CIPIT is available and willing to contribute further input to the policy as it develops. You may contact CIPIT at cipit@strathmore.edu or +254 0703 034 612.

Yours Sincerely,
CIPIT, Strathmore Law School

(Attachment: CIPIT’s analysis of the National CCTV Policy)
<table>
<thead>
<tr>
<th>Clause</th>
<th>Heading</th>
<th>Recommendation</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Scope</td>
<td>Define and limit the scope of “private” CCTV and exclude small home CCTV from registration requirements</td>
<td>The policy ought not to be applied to all private CCTVs as this is contrary to the proportionality principle embodied in Article 24 of the Constitution. Proportionality demands that there be a legitimate aim being pursued by any limitation of rights. -Subjecting private CCTVs to public authorities as detailed in the policy is a limitation on the right to privacy, as private CCTV owners are also required to register, make available site plans, link with security agencies etc. -These measures are disproportionate, as the legitimate aim being sought by the authorities (public security) may be contrary to the use being employed in the private sphere, such as watching over children in the home. This would therefore be a disproportionate limitation on privacy placed on private owners.</td>
</tr>
<tr>
<td>4</td>
<td>New clause</td>
<td>include discussion on the use of CCTVs in adducing evidence in court, which ought to be compatible with the Evidence Act, Sections 78 and 106</td>
<td>-There have been court cases where photographs and videos captured by CCTVs have been incorrectly adduced in court leading to them being deemed inadmissible. See Erick Indimuli Siaya v Republic (2016) eKLR</td>
</tr>
<tr>
<td>5.1</td>
<td>Guiding principles</td>
<td>Clarify that the publication of ownership and operation of CCTV systems applies to systems in public spaces</td>
<td>It ought not be compulsory to make ownership of private CCTVs within private spheres such as the home public knowledge, as this defeats privacy considerations where</td>
</tr>
</tbody>
</table>
### Add new

Add guiding principles on privacy and data protection:

Owners and operators of CCTV should publish their CCTV policy on the internet etc. The policy should among others:

1. State why the owner and operator has CCTV
2. Name the person responsible for operating the system
3. Describe the CCTV system in use, explaining the image capturing process, together with any other technology used in conjunction
4. Explain what kind of data is captured by the CCTV system as a whole
5. Explain how long the owner/operator keeps the data and why the retention periods have been chosen
6. Explain if and which third parties have access to the CCTV data and the nature of access (is it remote, continuous, on request etc)
7. Explain the process through which a person who needs CCTV data eg for a legal process may request for it
8. Explain the circumstances under which a person’s images may be disclosed
9. Explain how a person aggrieved by CCTV data may have their grievances addressed with timelines for the process
10. Explain the process

This would ensure protection and promotion of the right to privacy. It also promotes the right of access to information in a proactive way.

---

The CCTVs are used for domestic or household purpose. See *Durant v FSA (2003)*
| 6 | Roles and responsibilities | Add new actors: Kenya National Commission on Human Rights with among other roles:  
   a) Advice CCTV Committee on human rights implications of CCTV and related technologies  
   b) Create public awareness on human rights and CCTV  
Add new actors: Civil Society Organisations with among other roles  
   a) Defend public interest in CCTV policy making  
   b) Advice on the balance between security and human rights | This is in line with policy statement 3.3 on privacy and human rights |
| 8.1 | Policy directives | Replace policy directive 8.1 with All institutions, businesses, and facilities with public areas may install CCTV Systems to cover the public areas | The policy should not mandate all businesses and premises with public areas to have CCTVs. Kenya has a variety of businesses including startups, kiosks, nonprofits and informal establishments, it may not be able for many of these to meet the compliance cost of installing and maintaining CCTVs in their premises. |
| 8.2 | Policy directives | Clarify to whom CCTV installations should be registered  
   **Alternatively**, link registration to Data Protection Framework so that CCTV owners/operators register as data controllers/processors | It is not specified |
<p>| | | Clarify the rationale, purpose for registration of CCTV and uses of the registration information | Policy directives could also be used to harass business people and reduce the ease of doing business in the country. Explaining the rationale, purpose and encourages a |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>8.5</strong></td>
<td><strong>Access by security agencies</strong></td>
<td>Clarify what is meant by reasonable access and specify the mechanisms for ensuring that such a directive is not abused. For instance, should there be an order for access, who should sign the order, what constitutes “security agencies”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Article 31 guarantees the right to privacy and unwarranted access to private property. Reasonable access must therefore be described and limited</td>
</tr>
<tr>
<td><strong>8.6</strong></td>
<td><strong>Footage use in investigations</strong></td>
<td>Include the role of courts in determining access to footage for records</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is already provided for under section 36, National Intelligence Service (NIS) Act (2012). Is it possible for the policy to include an elaboration as to what criminal offences would entail? What can and cannot be a criminal offence may be left to interpretation (i.e., cases of corruption by high status individuals may not be seriously investigated in the same way a petty theft would be).</td>
</tr>
<tr>
<td><strong>8.8</strong></td>
<td><strong>Restricted areas</strong></td>
<td>Define “restricted area”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The phrase is too open ended and the common <em>wananchi</em> may not be aware of the Restricted Areas in the country.</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td><strong>New guiding principle</strong></td>
<td>Add: Protection of children Owners and operators with CCTV systems operating in spaces with children shall take special measures to ensure that the systems uphold the safety of children and protect children’s data from misuse. For example, access by third parties to children’s data should be more strictly controlled and where in doubt, subjected to interpretation by the court. Children’s data should also not be retained for longer than necessary to avoid profiling of children into their adulthood.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kenya is a signatory to treaties that guarantee special protection of children because they have limited legal capacity. Schools and universities are installing CCTV and they should be guided on the higher standard they must uphold while handling children’s data.</td>
</tr>
<tr>
<td>11</td>
<td>Additional references</td>
<td>Kenya Data Protection Bill, 2019</td>
</tr>
</tbody>
</table>