Joint EC-UNDP Thematic Workshop on Sustainability in Electoral Administration:

Adequate Resourcing for Credible Elections

National identity cards – Niall McCann, 7 March.

- Presentation structure
  - Some background on NIDs
  - Policy issues and data protection
  - Sustainable use of NIDs for voter registration

National ID cards

Some background on NIDs

1. NIDs – two elements:

   1. The card;

   2. The database;

   - *The card is the part of the 'iceberg' that is visible;*

   - *Huge policy vacuum.*

National ID cards

– NB: a NID database may be a population register but is NOT a civil registry:

– *Different data*:

- NID (*name, DOB, address, ID number, sex, place of birth, etc., but also sometimes religion/ethnicity, or even criminal record, voting history, etc*).

- CR (*record of birth, death, marriage, divorce, other name changes*).

– *Different purpose*:

- CRs (record of 'key life events,' evidence of individual's clam to an identity).

- NIDs (multipurpose).

National ID cards

- – 25 of 28 EU states (from Jul 2013) issue NIDs
- – No NIDs in UK, IRL and DK (or USA).
- – Africa? Morocco (includes lots of CR data), Kenya, Zambia, South Africa, etc…
- – Cost? Free to $80 (Austria).
- – 2006, joint EU guidelines on NIDs agreed. M*achine readable*. (often OCR -data cannot be added).
- – Trend moving to microchips;
  - more data can be held;
  - **data can be added**
  - (***Is card owner aware?***).

NIDs - Policy issues and data protection - 1

– *Control of data*:

- Who manages the NID system? Interior Ministry? Specialist state agency?

- Who has access to the data?

- Who can amend it/delete the data? Central data server administrators only? Or remote, off-site officials?

- Is there one database, that state agencies access according to their 'user profiles'? Or multiple databases, linked by a number unique to each individual?

- How much data is kept on the *card* (microchip) itself? Who can read it? Who can amend it/delete it?

NIDs - Policy issues and data protection - 2

– *Privacy issues*:

– Is there a data protection law?

– A legal redress for citizens to challenge either the accuracy of the data or how it is used, e.g. via a Data Protection Commissioner or Ombudsperson?

– Is there a freedom of information law? Does the citizen have the right to know what data is kept on them by the state?

NIDs - Policy issues and data protection - 3

- *'Real' vs. digital identity:*
  - Which identity has primacy in law?
  - The 'physical' identity of the person, as per official paper documents issued by the state
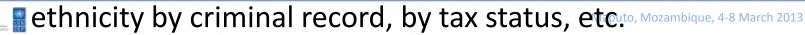 - Or the 'digital' identity of the person, as per the data carried in the database(s) or the card?

- *Some practical issues*
  - Does the data die with the person?
  - Get deleted if no longer relevant? (e.g. tax history)
  - Onus on cardholder/family or state to ensure accuracy?
  - Etc...

Controversies over the use of NIDs

- Cost! (e.g. Afghanistan - $220m – $800m);
- Invasion of citizen privacy?;
- Potential for identity theft for criminal purposes;
- Security of system, vulnerability of hacking;
- Sovereignty concerns over ownership and security of data;
- Intellectual property rights of vendors;
- Racial or ethnic 'profiling';
- Database merging:
  - 'single point of failure' for identity management;
  - Abuse of data by state agencies, e.g. cross-referencing ethnicity by criminal record, by tax status, etc.

The future….10 years?

- – Replacement of paper documents with digital 'documents' added to NIDs (e.g. e-birthcerts)
- – NIDs for children and 'baby biometrics.'
- – Private sector battle to datamine NID data;
- – Continued data-merging, driven by e-commerce and security sectors?;
- – Machines replacing humans in verifying NID data (e.g. airport fast-entry schemes);
- – More biometrics ➔ less need for cards, e.g. iris-scanning
- – *Ultimately, no need for NID*?

Sustainable use of NIDs for VR

– In electoral terms, NIDs can be used…

- To identify oneself in a VR exercise;

- To establish eligibility in a VR exercise;

- To identify oneself on polling day;

- To register as a candidate, poll worker or party agent/domestic observer;

- ***To create the voter register.***

Sustainable use of NIDs for VR

– Concerns and challenges;

- Reliance of data accuracy of other institutions;
- Politically tainted NID affects EMB independence?;
- Public distrust of NIDs causing VR backlash?;
- Expectance of EMB to be at the forefront of data protection issues;
- Allocation of voters issue;
- Accuracy of NID database not responsibility of EMB;
- VR-led NID creation risks overloading EMB;
- Risk to integrity of NID process – VR interested in those of voting age. Identify fake whether paper or digital
- Neither process should be held up or hostage to the other;

Sustainable use of NIDs for VR

- Tips for proper VR/NID linkages ;
  - Determine limitation of EMB responsibilities early;
  - Unless established address/postal code systems, allocation to polling centres responsibility of EMB;
  - Create cross-Ministerial task force, involving key ministries:
    - Health;
    - Justice;
    - Education;
    - Social welfare;
    - Defence/interior.
  - Realistic operational plans/budgets on long-term basis;
  - Determine citizen rights and *responsibilities*.

Final thought...

Home | **News** | Sport | TV&Showbiz | Femail | Health | Science&Tech | Money | Debate | Coffee

News Home | World news | Headlines | Pictures | Most read | News Board

New ID cards are supposed to be 'unforgeable' - but it took our expert 12 minutes to clone one, and programme it with false data

By STEVE BOGGAN
Last updated at 9:42 AM on 06th August 2009

Comments (41) | Add to My Stories

Adam Laurie is no ordinary hacker. In the world of computing, he is considered a genius - a man whose talents are used by government departments and blue-chip companies to guard against terrorists and cyber-criminals.

But even by his standards, what he is about to demonstrate is mind-boggling - and deeply disturbing.