Biometrics, surveillance technologies and the rise of the ‘security state’ in South Africa

Providing biometric data as a means of identification is supposed to drastically reduce fraud and identity theft, however, many are unaware that there are a number of potential dangers for users of this technology, finds Marc Davies.

Fingerprints are among our most intimate markers of identity and we are told that no two are alike. But we can lose control over how others use these very personal markers.

Through registration of bank accounts, identification documents at the Home Affairs Department, border control or social grant MasterCards, most people living in or visiting South Africa have been captured by one biometric database or another.

Handing over biometric data like fingerprints as a means of identification is routinely sold by recipients as an effective means to prevent fraud and identity theft. Governments the world over, including in South Africa, also encourage the rollout of biometric systems in the name of national security or the fight against terror. The databases on which biometric data is paired with a person’s biographic information, however, are not impenetrable, and neither are they immune to abuse.

Against a widely-marketed and often self-congratulatory narrative of technological innovation and enhanced security advanced by many corporate interceptors of biometric data, South African activist and independent academic Dale McKinley’s recent research warns of many potential hazards of this technology that are not necessarily well-known.

Photo credit: Toshiyuki IMAI via Flickr (http://bit.ly/2n6oVF2) CC BY-SA 2.0

Biometric identifiers are hugely invasive of the right to privacy, McKinley argues, because there is “nothing more private than an individual’s biological property”. He says that should this data, wittingly or unwittingly, be corrupted or stolen, there is no way to replace or correct this data. Lost or deliberately snatched data in the event of a hacked database, for example, would provide a basis for a range of potentially egregious abuses, he argues.

So severe are the potential threats to one’s very identity, along with the risk of personal information being auctioned to the highest corporate bidder, that the UK Home Office in 2010, for example, overturned the requirement for citizens to possess smart ID cards after substantial uproar among citizens and politicians. This included high-profile condemnation by former LibDem leader Nick Clegg and former Prime Minister David Cameron. Concerns over the potential for mass surveillance, discrimination, and the high cost of producing and managing smart ID cards underpinned this backlash.

In November last year, a French state watchdog called for the suspension of a similar centralised "mega-database" that would store 60 million people's biometric information. Joe McNamee of a European digital rights group told the BBC that adoption of centralised databases across many nations along with pushes for greater sharing of information across state departments is becoming an "ideology rather than a tool [for safety]".

Despite alarming risks, there are significant benefits to the use of biometrics, says Professor Jane Duncan of the University of Johannesburg.

Legitimate beneficiaries of social grants in South Africa – of which there are some 17 million people – can be identified using fingerprints and voices, Duncan told the Huffington Post South Africa. The usefulness of biometrics in this instance is notable: in the event of a lost ID booklet or forgotten PIN code, for example, an individual can access grant money without administrative difficulties. This is undeniably crucial for millions of people for whom access to grants may mean avoiding immediate impoverishment or increased deprivation.

The dangers, Duncan says, arise when a database is hacked, information is leaked or personal details are used or sold for purposes other than those consented to by the citizen (or "customer"). Furthermore, she argues, a distinction must be made between one-to-one and one-to-many biometrics. Where the former refers to communication between a biometric identifier like a fingerprint and a single database, the latter implies the use of a centralised or multiple databases that can all intercept the same biometric information. It is this latter form of biometrics, used widely in South Africa, that is most potentially problematic for Duncan.

For McKinley, the mandatory provision of one's cellphone number which is linked to the South African Social Security Agency (Sassa) smart card is indicative of another dimension of risk, namely the commodification of people's information. According to a previous *Mail&Guardian* report, beneficiaries of grants are subsequently inundated with "special offers" of small loans, funeral cover and airtime deals. The third-party company, CPS/Net1, which has to date been responsible for the delivery of payments, has used the database to create a massive network to market financial services to grant beneficiaries, according to McKinley.

More fundamentally, existing legislation in South Africa designed to ensure the safeguarding of individuals' information is yet to be practically implemented. The Protection of Personal Information Act of 2013 (POPI) is law but has not been fully implemented yet. The office of the Information Regulator, set up only in December last year to give teeth to this legislation, is still only in its infancy. According to Duncan, this means measures which invade personal privacy, such as biometrics, have been rolled out for years in the absence of a functional information and privacy regulator.

In light of the scope for both hacking by third parties and mass surveillance on the part of the state, the absence of strong social and political mobilisation around these issues concerns Duncan.

"People aren't even aware of these issues or the dangers," she said. "But it is starting to happen. We have a history of surveillance in South Africa and many activists have historic memories of how the state can misuse information and this could be the basis on which a privacy movement is built." According to Duncan, evidence has emerged of journalists, trade unionists and activists being placed under surveillance by the state using a range of privacy invasive technologies, some of which are imported and unregulated. Biometrics, in this context, are just one of the avenues through which surveillance or abuse of personal information on the part of the state or private sector can occur.

Duncan pointed to neighbouring Mauritius as an example of how mass resistance — supported by opposition parties, artists, trade unionists and social movements — coalesced into a movement that forced government to dismantle its own biometric database. Public consciousness in Mauritius about the potential perils of biometrics and other surveillance technologies has evidently grown much faster than in some of its neighbours including South Africa. "Until we also become aware of the potential threats to our personal information, we won't have a grassroots privacy movement emerging and will remain at risk," she said.

Marc Davies (@MarcDDavies) is a journalist with The Huffington Post South Africa and a former student in African Development at LSE.

The views expressed in this post are those of the author and in no way reflect those of the Africa at LSE blog or the London School of Economics and Political Science.

March 22nd, 2017 | Featured, Society | 0 Comments