DIGITAL INNOVATION AND ITS IMPACT ON PRIVACY LAW

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Sadia Rizvi | July 14, 2020

The speed of digital innovation and the emergence of technologies such as facial recognition and fingerprint authentication has brought with it privacy and cybersecurity concerns. In the recent months, after the killing of George Floyd, law enforcement authorities in the United States deployed powerful surveillance tools to monitor and track the protests against systemic racism and police brutality. Drones were flown over certain states and facial recognition software was used with some police body cameras. Authorities and individuals campaigned against the use of such software, warning that the software will be used for mass surveillance and racial profiling. Tech giants such as IBM and Microsoft have refused to sell their software for uses inconsistent with their organisational principles of transparency. Repeated studies have also shown that facial recognition technology has inherent biases and inadequately represents people of colour.

In South Africa, the Protection of Personal Information Act ("**POPIA**")[1] sets out the circumstances in which data can be collected, gathered and stored. POPIA states that any usage of data other than for its specified purpose, is deemed to be illegal, and responsible parties would be liable to a fine. However, there are valid concerns that technology such as facial recognition, if not properly checked, can be deployed as a tool of mass surveillance.

The enactment of POPIA and other legislation such as the Cybercrimes Bill of 2017 are positive steps to try to mitigate the unintended consequences of emerging technologies. However, there are several principles that businesses and online platforms developing and using facial recognition technology must be cognisant of. These principles will also apply to any business or authority which collects personal information of people.

Consent

Express consent should be obtained when enrolling an individual into a program that uses facial recognition technology, or when sharing such information to a third party.

Purpose

Consumers must be notified of the purpose that the information is being collected for and limited to this purpose.

Transparency

Consumers must be made aware and notified about how their data is to be used, stored, shared and maintained.

Security

The integrity of the data must be kept secure through comprehensive security programs which prohibits unauthorised access or disclosure to unauthorised persons. Technological and physical safeguards must be implemented.

Integrity

Reasonable measures must be taken to ensure that the data is accurate and up to date as far as possible. Individuals must also be allowed view their data and correct inaccurate data. Where a user requests the deletion of their data, this must be complied with.

Accountability

When information is shared with third parties, reasonable measures must be taken to ensure that the third party has safeguards in place to ensure compliance with all of the above principles.

The right to privacy is protected under section 14 of the Constitution of South Africa. The enactment of POPIA is a huge step towards protecting these rights, especially in the digital sphere. It often argued that although software, such as facial recognition, aids security, it can also be exploited for ulterior purposes. Presumed consent will also be an issue where the software is deployed in public spaces, as the subjects have not consented to the capture of their image. As this technology becomes increasingly prevalent, especially in law enforcement, stricter rules and regulations are required to ensure that such technologies are not abused.

[1] Act 4 of 2013.