
DATA PROTECTION AND PRIVACY

ALERT

SEPTEMBER 2014

IN THIS ISSUE

.....
FACIAL
RECOGNITION ...
A NECESSARY EVIL?
.....

FACIAL RECOGNITION ... A NECESSARY EVIL?

An investigative report was recently released by *DigBoston* (a free, alternative newsweekly published in Boston, Massachusetts) in respect of a new event-monitoring facial recognition surveillance system used by the City of Boston (City) as part of a pilot project during two public music events held in May and September 2013. The City used this system to track and monitor concert goers, without their knowledge. Utilising existing security cameras together with the system, the City tracked the thousands of concert goers and filtered their appearance (with the system being capable of distinguishing people by characteristics such as glasses, skin tone and beards) into data points which could then be cross-checked against certain identifying characteristics. The data captured through the software was transmitted to a hub, where, according to the report, city representatives, Boston Police and the software service provider support staff could watch, in real time, everything and anything whilst simultaneously monitoring social media key words related to the event.

According to the report, although the purpose of using the system was to enable the City to pick up on 'suspicious activity' (for example alerting the authorities when: (a) a person loiters near a doorway (as if trying to gain entrance), or (b) a person climbs a perimeter barricade/s; or (c) an abandoned object is found or left near barricade/s), it seems that the system was able and planned to be used to capture the face of every person who approached the door. The system, and particularly the extent to which it can and was used, while useful in certain respects, raises certain privacy concerns, as was highlighted in the report.

When considering this in the South African context, regard must be had to the Protection of Personal Information Act, 4 of 2013 (POPI), a South African legislative initiative designed to give effect to the right to privacy enshrined in section 14 of the Constitution and to provide for comprehensive and robust South African data protection laws. POPI prohibits the processing of personal information, unless it is carried out in accordance with the principles set out in POPI, including, amongst others, that there must be a level of awareness among data subjects of the collection of their personal information and the reasons or purpose therefor. POPI defines both 'processing' and 'personal

information' extremely widely, with 'personal information' being defined to include biometric information. It is clear from the definitions of 'personal information' and 'processing' in POPI that biometric verification will constitute 'processing' of 'personal information'. As such compliance with the conditions for lawful processing of personal information, as set out in POPI, are likely to be required when using technologies such as the system used by the City.

A responsible party using verification and monitoring technologies will need to ensure that it, amongst others, and with due regard to the exceptions under POPI (including where, for example, processing is required for the proper performance of a public law duty by a public body such as the SAPS): (i) uses personal information for the purpose of which it was collected; (ii) obtains consent from affected persons (data subjects); and (iii) secures the personal information adequately.

In addition to the protections afforded by POPI, the South African Constitution recognises the right to privacy of each individual (which includes the right to be free from intrusions and interference in one's personal life). South African courts have, however, also recognised that this right is not absolute as the scope of personal privacy

continued

is considered to diminish when a person enters into communal relations and activities involving business and social interactions. This notwithstanding, it is imperative that any person processing personal information, be cognisant and aware of the provisions under POPI together with Constitutional considerations and

protections. It is clear that, under POPI, transparency towards data subjects is key.

M van Zweel and Simone Gill



¹The Information Commissioner's Office 'Employment Practice Code'. Available at www.ico.gov.uk [Accessed 12/03/2014]

CONTACT US

For more information about our Data Protection and Privacy services, please contact:



Nick Altini

National Practice Head
Director
Competition
T +27 (0)11 562 1079
E nick.altini@dlacdh.com



Gillian Lumb

Cape Town Regional Practice Head
Director
Employment
T +27 (0)21 481 6315
E gillian.lumb@dlacdh.com



Preeta Bhagattjee

National Practice Head
Director
Technology, Media and
Telecommunications
T +27 (0)11 562 1038
E preeta.bhagattjee@dlacdh.com



Simone Gill

Director
Technology, Media and
Telecommunications
T +27 (0)11 562 1249
E simone.gill@dlacdh.com



Aadil Patel

National Practice Head
Director
Employment
T +27 (0)11 562 1107
E aadil.patel@dlacdh.com



Brigit Rubinstein

Director
Dispute Resolution
T +27 (0)21 481 6308
E brigit.rubinstein@dlacdh.com



Faan Coetzee

Executive Consultant
Employment
T +27 (0)11 562 1600
E faan.coetzee@dlacdh.com

This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

BBBEE STATUS: LEVEL THREE CONTRIBUTOR

JOHANNESBURG

1 Protea Place Sandton Johannesburg 2196, Private Bag X40 Benmore 2010 South Africa
Dx 154 Randburg and Dx 42 Johannesburg
T +27 (0)11 562 1000 **F** +27 (0)11 562 1111 **E** jhb@dlacdh.com

CAPE TOWN

11 Buitengracht Street Cape Town 8001, PO Box 695 Cape Town 8000 South Africa
Dx 5 Cape Town
T +27 (0)21 481 6300 **F** +27 (0)21 481 6388 **E** ct@dlacdh.com