ENSafrica | Africa's largest law firm **issue 1** | 2019-10

ENSafrica privacy in brief

ENSafrica's specialist data privacy and cybersecurity law experts are pleased to provide you with our first **privacy in brief focusing on data privacy**, a content-rich weekly newsletter dedicated to showcasing various topics and newsworthy stories covering issues related to privacy law and compliance.

feature article

Is privacy and the 4IR compatible?

In this week's feature article we deal with privacy issues emanating from the fourth industrial revolution ("**4IR**") and consider the impact of the often much-hyped 4IR initiatives on privacy rights.

4IR refers to the current stage of human development where disruptive technologies and trends such as the Internet of Things ("**IoT**"), robotics, virtual reality and Artificial Intelligence ("**AI**") are changing the way people in societies live, interact and work. Along with other governments in Africa, such as Ghana, as well as globally, South Africa has embarked on an ambitious programme to harness 4IR for future economic growth and development. The question arises however, just how does a country's 4IR ambitions match with the universally accepted constitutional and human right to privacy and with privacy laws in general; just how compatible is the 4IR development with privacy?

The impact of 4IR technologies on the right to privacy is best illustrated by way of some examples of technologies which raise major privacy (and in some cases, even safety) concerns:

- *The TV that watches you:* smart TV's are gaining popularity among consumers. Some Smart TV's not only track what you watch but in some cases listen and record your conversations or can even "watch" you through its built-in camera.
- *Cayla, the Talking Doll:* a talking doll named Cayla has been banned in Germany due to the software being easily susceptible to a hack, but more creepily, the doll was said to have recorded conversations of children and their parents
- *Smart Cities:* smart cities, or cities where key infrastructure or components of infrastructure are connected to the internet or networks, present a major risk of being hacked or may be subject to cyber terrorism. The impact on citizens and the security of the city as a whole presents major risks, including privacy risks. A good example is the use of surveillance cameras and the potential for abuse thereof to the detriment of the privacy of citizens.
- *Healthcare IoT:* as technology evolves and IoT devices become more integral to operations and other healthcare solutions, the threat to privacy increases

exponentially. The risk of hacking and the impact on human life is even more concerning.

- *Rise of the Machines:* as AI becomes increasingly used in the mainstream, coupled with robotics, there is a fear that machines will become more intrusive especially when it comes to privacy.

South Africa has privacy legislation in the form of the Protection of Personal Information Act, 2013 ("**POPIA**").To date, the most of POPIA is still not in force and effect. In Africa, only 15 of 54 countries have some form of privacy legislation in place. In the absence of active and adaptive legislation (i.e. legislation that can quickly adapt to changes in technological advancements) and more detailed guidelines on the development of 4IR technology, including issuing guidelines and best practices for the ethical adoption of AI and making Privacy by Design a more prescriptive requirement, the privacy rights of individuals and corporations remain at risk.

Companies and government departments investing in the development of 4IR technologies would do well to pre-empt privacy-related issues and ensure that privacy rights of citizens are kept at the forefront of the development process. Training of development teams on privacy laws and rights, including training on Privacy by Design and the ethical and legal implications of AI, is critical.

POPIA in brief

POPIA requires that a responsible party must ensure that the eight conditions for lawfully processing of personal information are complied with. In this week's edition, we cover processing condition 1, Accountability. We also compare this to the relevant corresponding provision under the General Data Protection Regulation 2016/679 ("**GDPR**"), being article 5(2).

POPIA: processing condition 1. The responsible party must ensure that the processing conditions in Chapter 3 of POPIA, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

GDPR: article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, the processing principles set out in article 5(1) of the GDPR (referred to as the "accountability" principle).

ENSpired (compliance) tip of the week

Two critical aspects which responsible parties should consider as part of demonstrating accountability is the formal appointment of an information officer and ensuring that accountability documents (i.e. policies, procedures and practices) are drafted, implemented, monitored and maintained.

In terms of section 109(3) of POPIA, the Information Regulator must take certain matters into consideration when determining an appropriate fine for a breach of POPIA, including any failure to carry out a risk assessment or a failure to enforce suitable policies, procedures and practices to protect personal information.

It is thus crucial to be able to demonstrate to the Information Regulator that your organisation complies with POPIA, by means of risk assessments having been conducted by the information officer and sufficient data protection policies, procedures and practices having been implemented.

cybersecurity

Cyber losses: Covered?

With a sharp rise in the number and complexity of cyber-attacks occurring over the last few years, resulting in major disruptions and losses to businesses (including business interruption costs, reputational damages, fines and penalties, and theft of funds), an important strategy deployed by businesses, in order to mitigate cyber-losses, is the purchase of cyber-insurance policies to cover such losses.

With this in mind, it is important to ensure you have the right cover for any losses resulting from a cyber-event:

- Cyber insurance policies are intended to cover losses associated with data breaches, cyber extortion/ransomware, the costs of the appointment of various professionals (such as forensic services, legal assistance) in managing a cyber-event, business interruption costs flowing from cyber breaches, and even compensation for certain fines/penalties imposed by the regulator (where possible). In other words, these types of policies generally cover economic/indirect losses, and third party liability, to your business following a cyber-event.
- Commercial crime policies, on the other hand, are intended to cover losses arising from theft, fraud, forgery and/or dishonesty (by employees, vendors and third parties), often committed through electronic means. In other words, these types of policies mainly cover direct/tangible losses of funds or assets from/to your business.

In taking out insurance cover for cyber-losses, do not overlook the type of cover your business needs: review your policies in order to ensure that you have the appropriate insurance coverage.

what? why?

As the Cookie crumbles

While most people think of a chocolate biscuit, a “cookie” can also be a small text file, which is used to recognise repeat visitors or users of a site, facilitate on-going access to and

use of a website, allows tracking of usage behaviour and compiles aggregate data that can enable improved functionality. Some websites also use "web beacons" which are small, clear picture files used to follow your movements on a website. For example, storing your preferred settings for the next time you visit.

The information collected from cookies enables website owners to tailor their websites to users' needs, help website owners retrieve the correct information related to unique log-ins, link browsing information to users, make improvements to their website or services and serve users with targeted advertising.

There are different categories of cookies, including necessary cookies, performance cookies, functionality cookies, targeting/advertising cookies and social media cookies. Necessary cookies generally enable users to effectively use a website and all its features. Performance cookies collect information about how users interact with websites in order to learn user behaviour and improve the website and/or services. Functionality cookies enable website owners to provide a more personalised experience. Targeting/advertising cookies are used to deliver advertisements that are relevant to users and their interests. Social media cookies tend to be third-party cookies from social media platforms that enable in-depth campaign reporting and tracking of social network users when they visit websites, by using a tagging mechanism provided by those social networks.

The provisions of POPIA will apply to your use of cookies on your website, to the extent that your website uses cookies to track unique user information and collect personal information (such as IP address or location, name, age, gender, etc.). In such instances, and in order to comply with POPIA, your website should have a cookie notice and your cookie policy should form part of your privacy notice. A cookie notice or cookie policy clearly communicates to users whether websites use cookies and if so, which cookies are being used. Such notice or policy should also make users aware of how to disable the use of cookies and the consequences of allowing cookies to be used on the website.

Data commercialisation

Free Wi-Fi – "if the service is free, you are the product"

In this segment, we discuss how businesses can utilise technology, including Big Data, for commercial benefit without infringing privacy laws or allowing privacy laws to stifle innovation. In this week's edition, we showcase the offering of free Wi-Fi services by businesses to members of the public.

There is an increasingly popular adage which suggests that "if the service is free, you (or your personal information) are the product". The offering of free Wi-Fi services exemplifies this adage. Most people love free stuff and in these times, Wi-Fi is more in demand than ever; free Wi-Fi even more so. Malls, banks, restaurants, airports, schools, offices and even cities are increasingly offering visitors access to free Wi-Fi services and with good reason. From a data commercialisation perspective, the benefit of offering free Wi-Fi to visitors is immense. Take for example a shopping mall operator that offers free Wi-Fi to patrons of the mall. Offering free Wi-Fi enables the operator to monitor and track patrons

in real time. By monitoring shopper behaviour and tracking shoppers in real time using beacons and other technologies, the operator is able to identify various trends (both historical and in real time). Such research and trends are of great economic value in the hands of shopping mall tenants and advertisers (or for that matter, security companies, law enforcement, other third parties or the operator itself). This in turn leads to the operator not only generating income from traditional rental income, parking income and billboard advertising, but also enables the operator to generate an additional revenue stream by selling data derived from the free Wi-Fi service to tenants, advertisers and other interested third parties. This is one example of how a company can take a very traditional business and, by exploiting data, generate an additional income stream.

From a privacy perspective however, one questions how this can be done lawfully, especially when you consider the exposure and potential "selling" of personal information to third parties. The answer is that this can be done very easily, in full compliance with privacy laws.

The key to commercialising data in the world of privacy requires specific expertise. Navigating privacy laws in order to derive the full value from data commercialisation initiatives requires an appreciation and deep understanding of technology, of data laws and of business objectives. Clients considering embarking on any data commercialisation activities or Big Data projects are strongly encouraged to contact us to discuss how we can assist in adding value to your business without infringing privacy laws.

ENSide Africa

In this section we focus on data privacy across Africa, and in the coming weeks we will focus on specific jurisdictions which have data privacy laws in effect and also on jurisdictions where data privacy is not regulated. In Africa, 15 of 54 countries have some form of data privacy law in place with certain jurisdictions having draft laws. When doing business in Africa it is essential that Africa not be treated as one homogenous mass and that each jurisdiction be assessed on its own merit. Also, making an assumption that certain wealthier countries such as South Africa and Nigeria have more sophisticated data privacy regimes than other African countries is simply incorrect.

case spotlight

Google the Google fines

In January 2019, the French data protection authority announced that it had fined Google EUR50-million for not properly disclosing to users how data is processed across its offerings – including its search engine, Google Maps and YouTube – to present users with narrowly targeted ads.

In a similar vein, Google was previously fined EUR150 000 by the French regulator as its privacy policy did "not sufficiently inform its users of the conditions in which their personal data are processed, nor of the purposes of this processing".

The Spanish regulator also levied a fine of EUR900 000 against Google. Dutch and Italian regulators also threatened fines. In the UK, the Information Commissioner's Office agreed not to levy a fine, provided Google changed their privacy policy in a timely manner, which it did.

It is clear that Google was not fined for not having a privacy policy, but for having one that did not sufficiently inform data subjects regarding the use of their data. It could therefore not demonstrate accountability with the notification requirements imposed under the EU Directive on Data Protection and the GDPR, which replaced the EU Directive in May 2019.

strange times

Deepfakes – as real as it gets!

Deepfake is an AI-based technology used to produce or alter video content so that it presents something that did not actually occur. The word is a portmanteau, 'deep' refers to deep learning and 'fake' clearly represents the untrue or sham nature of the video, audio or image created. Deepfake technology has evolved to such an extent that companies and law enforcement are currently struggling to differentiate between real and fake media (images, video and sound clips), with some companies even offering financing to start-ups to develop more sophisticated technology to identify whether media is a deepfake or not.

Tools for editing media are not new, consider, for example, Photoshop. The power of deepfakes, however, is that the technology has made it cheaper and much easier to produce realistic deep fake video or audio clips. The production of a deepfake, begins with feeding data into the software. The data can be in the form of photos (if one were creating a video) or voice clips (if one were making audio). The more data that can be fed into the software, the more accurate the statistical connections the software will be able to compute.

The concern about deepfakes originally centred around beliefs that the technology would be used to manipulate politics and even elections, however, the effect on ordinary citizens is equally concerning.

Some examples of the effect of deepfakes and their impact:

- a deepfake video is released right before election day depicting the lead candidate engaging in some form of nefarious activity. The realistic nature of these videos will make it very difficult for the average person (or for that matter, even technology experts and law enforcement) to consider the possibility of fake news, especially in light of the fact that we generally accept the veracity of video content;
- another recent trend identified was the prominence of non-consensual deepfake pornography (placing someone's facial image on a pornographic video) – accounting for 96% of the total deepfake videos online. Unfortunately the study found that all such videos targeted women. Fortunately, South Africa has recently passed legislation, the Films and Publication Amendment Bill, which criminalises "revenge

porn". Depending on how the new law will be interpreted it is likely that non-consensual deepfake pornography could fall within the ambit of revenge porn; and
- in September this year, in what may be the first, a deepfake cybercrime was reported. In this case a deepfake audio clip was used. The clip imitated a chief executive's voice to trick an unsuspecting subordinate into transferring USD240 000 into a secret account. The company's insurer, Euler Hermes, explained that the company's managing director was called late one afternoon and his superior's voice demanded that the subordinate wire money to a Hungarian account to save on "late-payment fines", sending the financial details over email while on the phone. A spokeswoman from Euler Hermes said, "The software was able to imitate the voice, and not only the voice: the tonality, the punctuation, the German accent."

The rise of deepfakes shows how your personal information (think of all those selfies you have taken, or consider the voice data that your devices have gathered) is capable of being used in these strange times in which we now live.

in the news

Google: A UK Court of Appeal granted an appeal from a decision of the UK High Court to allow for a class action arising from a data privacy breach against Google. In issuing its ruling the Court confirmed a number of key legal principles including:

- an individual's personal data has economic value and loss of control of that data is a violation of the right to privacy which can, in principle, constitute damage without the need to demonstrate pecuniary loss or distress. The Court can therefore award a uniform per capita sum to members of the class;
- individuals who have lost control of their personal data have suffered the same loss and therefore share the "same interest"; and
- class actions suits, or representative actions, are in practise the only way that such claims can be pursued.

Nigeria: The National Information Technology Development Agency has entered into a strategic partnership with the European Data Protection Office to enable Nigerian businesses to comply with the GDPR.

Facebook: Europe's top court ruled that Facebook can be ordered to police and remove illegal content worldwide.

upcoming events

ENSafrica will be hosting POPIA, GDPR and Information Officer training workshops in Durban, Cape Town and Sandton. For more details and to register, please click here.

our services

ENSafrica has a highly specialized team of privacy and cybersecurity lawyers with deep expertise and experience in assisting clients with all aspects of POPIA compliance, GDPR assistance, cybersecurity and insurance, and data commercialization. Our unique services includes the provision of a POPIA Toolkit, which contains data protection policies and other documentation which can be tailor-made for your organisation and help fast track your organisation's POPIA compliance journey. We also provide training on awareness initiatives, risk assessments, policy and procedure implementation, and also provide a helpful service to Information Officers requiring support in implementing POPIA.

Contacts

Ridwaan Boda

Director | Technology, Media and Telecommunications

+27 83 345 1119

rboda@ENSafrica.com

Era Gunning

Director | Banking and Finance

+27 82 788 0827

egunning@ENSafrica.com

Wilmari Strachan

Director | Technology, Media and Telecommunications

+27 82 926 8751

wstrachan@ENSafrica.com

Nicole Gabryk

Director | Dispute Resolution

+27 82 787 9792

ngabryk@ENSafrica.com

Rakhee Dullabh

Senior Associate | Technology, Media and Telecommunications

+27 82 509 6565

rdullabh@ENSafrica.com