feature article

The city under attack

On the 24th October 2019, the City of Johannesburg tweeted that it had “detected a network breach which resulted in an unauthorised access to its information systems”. It shut down its website and several customer facing systems – including the city’s website, e-services and billing system – as a precaution.

A bitcoin ransom note received by several city employees from the “Shadow Kill Hackers” reads “All your servers and data have been hacked. We have dozens of back doors inside your city. We have control of everything in your city. We also compromised all passwords and sensitive data such as finance and personal population information.”

The hackers demanded the payment of 4.0 bitcoins by October 28 at 5pm failing which all the data will be uploaded onto the Internet.

At the same time several banks reported Internet problems seemingly linked to cyberattacks.

If the Protection of Personal Information Act, 2013 ("POPIA") had been fully effective, the City of Johannesburg and the banks would (probably) have been obliged to notify the Regulator and the affected data subjects. POPIA would also require that “responsible parties” (such as the City and the banks) secure the integrity and confidentiality of personal information in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of personal information, as well as to prevent unlawful access to or processing of personal information. POPIA is not prescriptive as to the exact security measures to be undertaken, but the organisation is obliged to have due regard to generally accepted information practices and procedures which may apply to it generally or may be required in terms of specific industry or professional rules and regulations.

Notwithstanding the fact that POPIA is not entirely in force and effect yet, the office of the Information Regulator is proactively monitoring organisations that have endured security compromises, and is currently receptive to responsible parties voluntarily reporting security compromises to.

South African companies that fall within the jurisdiction of the European Union’s General
Data Protection Regulation 2016/679 ("GDPR") should also note that they are already under an obligation to report data breaches. In the case of a personal information breach, the organisation must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal information breach to the competent supervisory authority, unless the personal information breach is unlikely to result in a risk to the rights and freedoms of natural persons. Fines for non-compliance with the GDPR range from EUR20-million to 4% of an organisation’s worldwide turnover.

**POPIA in brief**

*Condition 4: further processing limitation*

Further processing of personal information must be compatible with the purpose of collection, unless the data subject has consented to such further processing. To assess whether further processing is compatible with the purpose of collection, the responsible party must take various factors into account, including the relationship between the purpose of the intended further processing and the purpose for which the information has been collected; the nature of the information concerned; and any contractual rights and obligations between the parties.

*GDPR: article 5(1) (b)*

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (the “purpose limitation” principle).

**ENSpired (compliance) tip of the week**

The information officer should conduct privacy impact assessments to determine whether, in the absence of consent, the further processing of personal information by the organisation is compatible with the reason for collection. If not, consent would have to be obtained or the further processing should be discontinued.

**case spotlight**

In April 2018, the Bulgarian Commission for Personal Data Protection imposed a fine of roughly EUR500 on a bank for calling a client for the unresolved bills of his neighbour. This provoked the client to evoke his right to be forgotten. After not receiving any answer from the bank he filed another motion, for which the bank did take action in the statutory period. Nonetheless, the client filed a complaint with the supervisory authority.
The bank was fined on the basis that the processing of the client’s personal information was not linked to his consumer credit agreement. This was found to be in breach of article 5(1) (b) of the GDPR (the purpose limitation principle which is similar to processing condition 4 of POPIA). Since the purpose for which the personal information was processed was different from that communicated at the time of conclusion of the contract, the bank had, according to the supervisory authority, to request additional consent from its client, which it failed to do.

cybersecurity

Cyber-attacks make for costly business

As noted above, in the past week a number of South African banks, municipalities and internet service providers have been hit by targeted cyber-attacks (specifically distributed denial-of-service attacks) which have prevented these entities from being able to provide some services to customers (and could also have resulted in a compromise of confidential details of clients and customers). Cyber-attacks that stop the day-to-day business activities of organisations can lead to expensive business-interruption costs (as well as loss of profit, loss of clients and reputational harm).

Most general liability insurance policies do not cover business-interruption costs resulting from a cyber-attack. It is therefore vital for organisations to ensure that they have appropriate insurance cover by way of a specialised cyber liability insurance policy. Cyber insurance policies are generally offered as cover for a combination of first party costs (such as legal costs, forensic costs, data recovery costs, ransom payments etc.) and financial losses caused by business interruption, as well as third party liability claims resulting from a cyber-event. Having the correct insurance cover in place can help organisations recover from losses associated with data breaches and cyber-attacks, which could otherwise cripple a business.

what? why?

Social media – one of the biggest risk areas for information leakages

Social media platforms have enabled organisations with limited resources to use social media to reach broader, untapped audiences with minimal spend. A good social media strategy can catapult an organisation’s marketing efforts whilst not breaking the bank. News headlines around the world have shown us that employees can be the best and worst brand ambassadors for an organisation, making its employees one of the most powerful assets in the organisation. When it comes to privacy laws, a social media page is one of the biggest risk areas for leakage of personal information, especially personal information such as photographs and video clips. Numerous examples have been cited wherein employees have unwittingly or even maliciously disclosed personal information of the company or of other data subjects on social media pages, often compromising sensitive deals and the company’s reputation. Given this risk, it becomes vital that organisations have and continually update a social media policy, as well as provide proactive training to employees,
social media managers and users of social media pages.

A social media policy should address the following:

- acceptable guidelines for the use of social media, including when (e.g., during breaks) and how (e.g., respectfully and without infringing rights of others);
- what is considered inappropriate behaviour (e.g., illegal, offensive, defamatory, discriminatory, etc., post);
- the proper reference and use of an organisation’s brand and trademarks and whether or not they can be used by employees in social media posts;
- what information may not be shared on social media, such as confidential or proprietary information;
- a consideration of protecting people’s privacy (which will include the privacy of juristic entities under POPIA);
- who the authorised representatives are and what their duties are in respect of posting official material on behalf of the organisation;
- who to contact regarding any social media related posts/concerns that may impact the organisation; and
- consequences for not complying with this policy, including disciplinary action that may be taken.

A good social media policy should clearly specify the parameters within which employees may operate while empowering them to be the best brand ambassadors for your organisation.

---

Data protection and cybersecurity in M&A transactions (part 1 of 4)

In July 2019, the UK’s Information Commissioner’s Office ("ICO") levied a fine of EUR99-million (about ZAR1.9-billion) on Marriott Hotels due to a data compromise which had occurred on Starwood Hotel’s systems in 2014, prior to Marriott’s acquisition of Starwood in 2016. Without getting into the full details or an assessment of the case, the ICO specifically cited Marriott’s failure to conduct due diligence on Starwood’s IT infrastructure as an explanation as to why Marriott was being fined for Starwood’s mistakes. The ICO commented that its investigation had revealed that Marriott "failed to undertake sufficient due diligence when it bought Starwood...". In addition to being imposed with the hefty fine, Marriott also incurred millions of dollars in costs of remediating the data breach, an incalculable cost in reputational harm, and is now faced with multiple class action lawsuits from affected clients.

In our four part series on data protection and cybersecurity in M&A transactions, we deal with key issues to be considered from a data privacy and cybersecurity perspective when acquiring a business. In the weeks to come, we will focus on risk identification and risk mitigation in M&A transactions including:

- data protection and cybersecurity as the subject matter of due diligence efforts, including the need to ask the right questions when buying a business;
• data protection and data sharing during the due diligence process, including the risks associated with sharing too much information; and
• transfer and use of data by the acquirer post-acquisition, including circumstances where a target is purchased specifically because of the value of its data.

Data privacy and cybersecurity is not just an IT or regulatory problem; companies engaging in M&A activity would do well to learn from some of the lessons arising from the Marriott case including:

• the importance of conducting a thorough privacy and cybersecurity due diligence in the context of mergers and acquisitions;
• realising that buyers of businesses in particular cannot be absolved a target’s cybersecurity failures (even past failures); and
• compelling parties and their advisors in M&A transactions to be more cognisant of the importance of data privacy legislation at all stages of the transaction, from inception of interest until post acquisition, and to take proactive measures at each stage to ensure compliance with legislation and best practises.

---

**ENSide Africa**

**Angola**

In this section we focus on data privacy across the African continent. This week we look at the Republic of Angola. Law 22/11 (“the Act”) is the general law which regulates the processing of personal information. The Act applies to the processing of natural persons’ information by both public and private institutions. There is no obligation on institutions to appoint an information officer. Once established, the Data Protection Authority will be responsible for the oversight of the Act. Interestingly, the Act does not prescribe any notification requirements in case of a breach.

---

**strange times**

**The rise of the genetic informant**

When you think about personal information being captured on various websites, your mind will most likely skip to thinking about names, email addresses and other identifying factors. We do not often think about DNA falling into this category. Of course, a person’s DNA does form part of the definition of “personal information” in POPIA and should not be ignored. The use of DNA data online has become quite a controversial topic.

The use of various websites such as GEDmatch or FamilyTreeDNA allows a person to upload their personal DNA information obtained from a home testing kit to find out and learn about their family lineage. These websites are available to everyone, but appear to be particularly popular in the United States. GEDmatch, was a site first created by volunteer genetic genealogists to help people learn more about their ancestors or find estranged
family members. However, in 2018 the GEDmatch website drew significant media coverage after it was used by law enforcement to identify a suspect in an on-going serial killer case which began in the late 1970s.

“Forensic genetic genealogy” is the term used to describe the use of genetic databases by law enforcement to find potential suspects through family members’ DNA. A suspect’s DNA is uploaded onto the relevant database and a family tree is built. If successful in formulating a family tree, the investigator will then reverse engineer the family tree of the unknown suspect based on the trees of the people who share their DNA with the suspect in question. It has been stated that investigators need only to match up to a third cousin on both the maternal and paternal side of the suspect. This might make it sound difficult to identify a suspect, however it has been reported that about 60 percent of Americans (mainly of European descent) can be identified as of today (even if they have never used a DNA home kit or uploaded this data onto a website). It is also reported that soon GEDmatch will likely be big enough for law enforcement to establish the source of almost any anonymous DNA sample. This is very different from the due process norm that law enforcement may only use a database containing the DNA of people who have already been arrested at some stage in the past.

This may sound like a great new-age, albeit strange, method of catching criminals. However, a number of ethical issues have been raised. For example, if we are going to be technical, if your DNA is linked to a suspect, you have inadvertently helped identify your own family member as a criminal (whether you might know the person or not). In these instances would you become a “genetic informant” and should you then be concerned about your safety? (Particularly in light of the fact that the forensic genetic genealogy method has been limited to use in only violent crimes).

The reliance on forensic genetic genealogy also raises some serious privacy concerns. In the first instance, most people who had originally uploaded their DNA were not aware that the website would potentially share this data or allow it to be used for law enforcement purposes. When this was first done, it had been reported that the websites had in fact done so in secret, only updating their terms of use after the fact. There have also been further cases where the website owners have allowed a flagrant disregard of their terms of use, only to again broaden the scope of processing under their terms of use after the fact. Clearly, this shows the importance of being open and transparent when it comes to the purpose of processing on a website. Additionally, one need not even have uploaded one’s DNA information to be caught up in an investigation, as each DNA sample would contain the DNA of relatives, both close and distant. This raises the issue of not having consented to your personal information being processed at all. The practice clearly exposes millions of people who have never taken a DNA test to possible police identification, raising difficult questions around due process in criminal investigations.

Finally, many privacy experts have indicated a further concern – the trove of very personal information which can be obtained from a person’s DNA. Genetic genealogy is drawn from hundreds of thousands of genetic variants called SNPs (single nucleotide polymorphisms). The technique can give away details about a person’s appearance, medical conditions and possibly even their predisposition to mental health problems (and this excludes the additional information such as whether a person was born out of wedlock or perhaps was
the product of incest, which could also be exposed). This type of personal information is afforded special protection under POPIA (as it constitutes “special personal information”) which further shows the difficult privacy questions that should be addressed should this practice continue on a global scale. Furthermore, should we start being concerned about employers and insurance companies accessing this type of data without our knowledge? This apparently has not happened yet, but is certainly possible.

Forensic genetic genealogy is yet another example of how our personal information can be used online in ways that we may never have imagined – stranger times indeed. Regardless of which ethical or moral standpoint you take, it is quite clear that a privacy policy or terms of use has great value in informing consumers what information will be processed and, more pointedly in the context of this article, how that personal information will be used. A clear, transparent and easy to understand privacy policy could save your business from the reputational harm that is likely to arise in the event that the terms are not clear and informative.

**in the news**

*United States:* The Federal Trade Commission in the United States has brought a case against a developer of a spying app for the first time. The app allowed purchasers to spy on the movements and online activities of users of the target device, which was installed without the knowledge or permission of the user, thereby infringing on the privacy rights of the persons being monitored.

*Google:* The Australian Competition and Consumer Commission is taking Google to court for misleading users on how their location data is processed.

*Facebook:* Facebook has agreed to pay a EUR500 000 fine to the UK’s Information Commissioner’s Office arising from its involvement in the Cambridge Analytica scandal, which occurred in 2015. Facebook has opted to pay the fine but has made no admission of liability. It is noted that the fine is based on the pre-GDPR methodology for calculation of fines.

**upcoming events**

ENSafrica will be hosting POPIA, GDPR and Information Officer training workshops in Durban, Cape Town and Sandton. For more details, please get in touch with us.

**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 commercialisation. 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, privacy impact assessments, policy and procedure implementation, and also provide a helpful service to Information Officers requiring support in implementing POPIA.

We will be hosting a Marketing and Advertising seminar on 21 November, which will holistically deal with the complicated issues under POPIA, the GDPR and other relevant legislation. For more details, please get in touch with us.

Contacts

Ridwaan Boda
Executive | Technology, Media and Telecommunications
+27 83 345 1119
rboda@ENSafrica.com

Era Gunning
Executive | Banking and Finance
+27 82 788 0827
egunning@ENSafrica.com

Wilmari Strachan
Executive | Technology, Media and Telecommunications
+27 82 926 8751
wstrachan@ENSafrica.com

Rakhee Dullabh
Senior Associate | Technology, Media and Telecommunications
+27 82 509 6565
rdullabh@ENSafrica.com

Nicole Gabryk
Executive | Dispute Resolution
+27 82 787 9792
ngabryk@ENSafrica.com

This email contains confidential information. It may also be legally privileged. Interception of this email is prohibited. The information contained in this email is only for the use of the intended recipient. If you are not the intended recipient, any disclosure, copying and/or distribution of the content of this email, or the taking of any action in reliance thereon, or pursuant thereto, is strictly prohibited. Should you have received this email in error, please notify us immediately by return email. ENSafrica (ENS and its affiliates) shall not be liable if any variation is effected to any document or correspondence emailed unless that variation has been approved in writing by the attorney dealing with the matter.