Deloitte.
Legal

Deloitte Legal – Representing Tomorrow
International Privacy Day 2017

With International Privacy Day being celebrated recently, we recount the top data protection events of 2016.

South Africa: Information Regulator Appointed

On 26 October 2016, former IEC chairperson Advocate Pansy Tlakula ("Tlakula") was appointed as South Africa's Information Regulator. Her role includes being an independent supervisory authority responsible for monitoring and enforcing compliance as well as handling complaints related to the Protection of Personal Information Act ("POPI").

The pertinent question posed by most South African citizens and organisations since the appointment of Tlakula, is when POPI, which was promulgated into law on 26 November 2013, will commence.

As per the transitional arrangements in section 114 of POPI, once the commencement date has been set, all responsible parties will have 12 months therefrom to become fully compliant with POPI. POPI defines responsible parties as being public or private bodies or any other persons which, alone or in conjunction with others, determine the purpose of and means for processing personal information.

The Minister of Justice and Constitutional Development may provide for the extension of the aforementioned 12-month period for compliance to a maximum of 3 years from the POPI commencement date. Now that Tlakula's appointment has become official, the process of drafting regulations required to implement POPI can commence.

Among others, and alongside Tlakula, Advocate Collen Weapond ("Weapond") has also been appointed as a full-time member of the Information Regulator, according to the Information Regulator media statement dated 2 December 2016. Weapond will, among other things, oversee and implement the execution of POPI. What does this mean for persons who must comply with POPI? Going forward, it will be imperative that responsible parties review, on an ongoing basis, its data processing activities so as to avoid possible penalties for non-compliance.

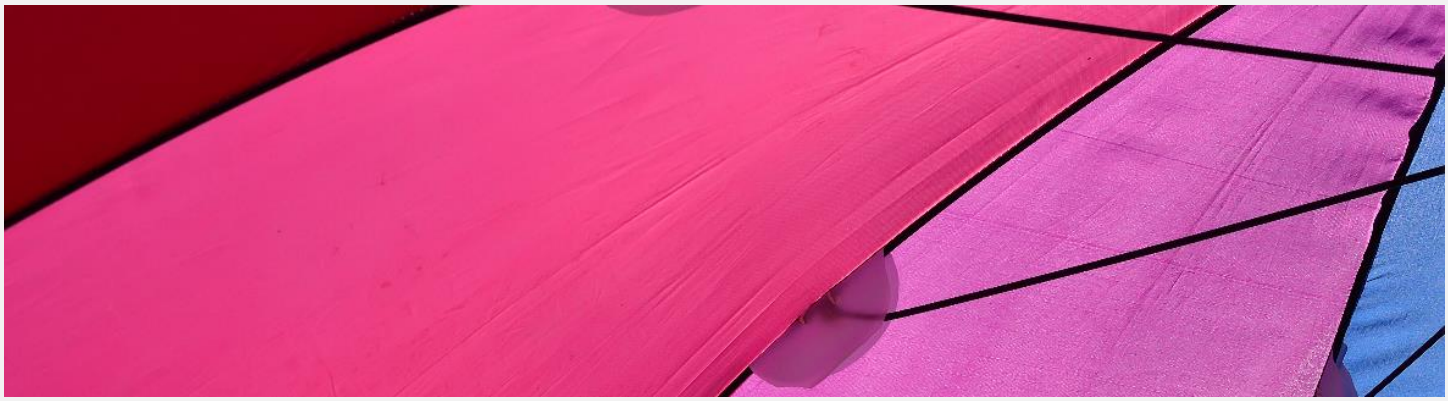
A fundamental aspect of POPI that will significantly affect responsible parties in future, is that of personal information breach or incident management. POPI requires that entities processing personal information secure the integrity and confidentiality of personal information in their possession, through implementing reasonable security measures. POPI does not delineate the perimeters of 'reasonable security measures'; however, this would differ from entity to entity. POPI furthermore, requires mandatory notification of any security compromises involving personal information. The importance of developing and implementing reasonably sound security measures and breach information management is demonstrated by an incident involving a reputable South African investment, savings, insurance and banking group ("the Group"), which transpired in 2016.

A certain customer of the Group had received e-mail communications from the Group which were intended for two other customers. The communications contained confidential information, including identity numbers, addresses and banking account details. The Group thereafter, in response to being alerted of the error, issued a statement to the effect that a high premium is placed on their customers' personal information, which they aspire to protect at all costs. Fortunately for the Group, the customer to whom it had erroneously dispatched the e-mail communications to, was an honest and conscientious customer who immediately alerted the Group to the error so that the Group could implement immediate damage control.

However, the ramifications could have been dire, had the leaked personal information fallen into the wrong hands – identity theft of the Group's customers' identities, followed by law suits, loss of customers and revenue, and a tarnished reputation.

Had POPI been in effect at the time that the breach had occurred, the mandatory breach notification procedures would have been triggered, and the Group would have had to provide notification of the breach, not only to the affected customers, but also to the Information Regulator, who would have taken suitable steps, including the administering of fines, imprisonment and enforcement notices against the Group, for failing to adequately protect its customers' personal information. Hence, it is crucial, depending on the entity in question and the type and sensitivity of personal information collected and processed, that at the very least, security measures such as password-protection and encryption be implemented.

Furthermore, a breach incident management framework needs to be developed and implemented, as breaches are inevitable in this technologically advanced age. Thus, a proactive (rather than reactive) and risk-based approach to handling personal information breaches is imperative.



International: Privacy Shield between United States and European Union

On 2 February 2016 the European Union ("EU") and the United States ("US") Government reached a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes: the EU-US Privacy Shield Framework ("Privacy Shield"). The Privacy Shield was designed by the US Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the EU to the US in support of transatlantic commerce.

On 12 July 2016, the European Commission finalised the adoption of the Privacy Shield. The origin of the Privacy Shield stems from the repeal of the old EU-US Safe Harbour Agreement. In order to facilitate personal data flows between the EU and the US for commercial exchanges whilst ensuring data protection, the European Commission recognized the Safe Harbour framework as providing an adequate level of protection despite there being no general data protection law in the US.

In 2013, the European Commission pointed to a number of weaknesses of the Safe Harbour regime, notably a lack of transparency by companies concerning their adherence to the framework and a lack of effective enforcement by US authorities of those companies' compliance with the framework's privacy principles.

Further concerns were raised regarding the scale and scope of certain US intelligence programmes (such as the Prism Programme), and the level of access by US public authorities (such as the National Security Agency) to EU citizens' personal data, transferred to the US under the Safe Harbour framework.

The European Court of Justice, in the case of Schrems v Data Protection Commissioner, declared the Safe Harbour Agreement invalid, confirming the need for a stronger and new framework for transatlantic commercial data flows.

The Privacy Shield provides important new safeguards and ensures a higher level of protection of the fundamental rights of EU individuals, thus providing the necessary legal certainty for companies on both sides of the Atlantic.

The Privacy Shield goes beyond its Safe Harbour predecessor by not only covering commitments in the commercial sector but also, and for the first time in EU-US relations, in the area of access to personal data by public authorities including for national security purposes. The most important achievements of the Privacy Shield include:

1. strong obligations on companies and robust enforcement;
2. clear limits and safeguards with respect to US Government access;
3. effective protection of EU individuals' privacy rights with several redress possibilities; and
4. annual joint review mechanism.

A threat to the viability of the Privacy Shield manifests in the form of recently inaugurated US President Donald Trump, whose stance on electronic surveillance in the war on terror and bulk data collection has raised concerns amongst non-US cloud users. At present, his administration has yet to outline their plans regarding the Privacy Shield.

Time will tell whether the failings of the Safe Harbour Agreement and subsequent challenges to the Privacy Shield will derail the progress made under the new regime.

Further International Transfer Arrangements Globally
The EU is currently in the process of concluding an arrangement with the Asia-Pacific Economic Cooperation ("APEC") with regards to the cross-border transfer of personal information between the EU and Asia. This is demonstrative of the fact that data privacy is not entirely concentrated between the EU and US, but has become a global phenomenon, especially in light of the APEC Cross Border Privacy Rules ("CBPR") framework, which seeks to enforce privacy principals and protections along the same lines as Privacy Shield. This will usher in a new era for data privacy which will enhance the exchange of personal information for economic purposes.

Apple Bites Back

2016 saw the debate between iPhone manufacturer Apple Inc. ("Apple") and the Federal Bureau of Investigation ("FBI"). The dispute arose following the San Bernardino mass shooting.
Syed Rizwan Farook and Tashfeen Malik opened fire at a holiday party at the Inland Regional Centre in San Bernardino on 2 December 2015. 14 people were killed and 22 injured before both shooters were killed in a gun battle with police.

The FBI challenged Apple to unlock an iPhone belonging to one of the shooters in order to uncover evidence. Apple declined, citing fears that this would create a "master key" to unlock any iPhone, not only the specific one, potentially resulting in customer loss of confidence in the brand and the plummeting of sales.

Further, Apple believed this to be an invasion of its customers' privacy and that there should be a limit to the control government should have over public surveillance of not only the residents of the U.S but also globally. While the process to create a backdoor into the iPhone is unclear, Apple feared to do so would set a precedent with several other authorities in the U.S asking for iPhones to be unlocked. While the iPhone is not an impenetrable device, with Apple under no impression to the contrary, Apple's refusal is in creating the backdoor themselves. Ultimately prior to a verdict being passed, the FBI's "spymasters" found an alternative method in order to unlock the device, and subsequently withdrew its case. This particular case has not been the first of its kind in US legal history. In 2001, the FBI ordered a major vehicle communications system manufacturer to turn on the unit's built-in microphone to survey the driver. The vehicle communications system manufacturer complied leaving the FBI with full access to listen in.

Which rights are ultimately being guarded? While the FBI will contest that the data on the accused's iPhone is pivotal to their investigation, is it necessary to have a "master key"? If commercialised, what impact

would it have on the privacy of individuals? Society has become less and less comfortable with the global impact of the potential invasion of privacy by the FBI.

Alexa, how do we solve this murder?

In 2015 James Clapper, the US Intelligence Chief, warned that agencies will turn to the Internet of things to increase their surveillance abilities and 2017 may see that threat become reality. Amazon is embroiled in a legal battle with the Arkansas Prosecuting Authority over the use of Amazon's voice-activated Echo smart speaker (a digital personal assistant with abilities to listen, translate, process and store voice requests) to access data stored in a cloud in order to assist with the murder investigation implicating James Bates.

While a discovery hearing is scheduled for March, authorities issued a warrant for Amazon to provide recordings from the night of the alleged crime. Amazon subsequently complied with the warrants on 8 February 2016, but only supplied a portion of the information requested. Alexa works in a similar fashion to Apple's SIRI by constantly listening for "wake" words and thereafter records and listens for instructions for a period before reverting back to standby mode. A witness recalls the device being used to play music and thus possibly having recorded information pertinent to the case.

Technology is integral to simplifying daily life; as such authorities will increasingly seek to use technology to enhance their investigations. The line blurs between protecting the public and infringing on an individual's right to privacy. In the first instance if technology can be used to solve vexed cases, the greater public will benefit. On the contrary, imagine the instance where ever device with a microphone and recording capabilities is able to serve as a witness against you.

WhatsApp's Double Jeopardy

In April 2016 WhatsApp released an update adding end-to-end encryption for all chats and messages. What does this mean? WhatsApp now securely encrypts every message, call, picture, video or any other type of file sent. Interestingly, WhatsApp does not have the ability to intercept and view messages being stored. To date, WhatsApp has suffered numerous exposures over poor security standards. In May 2011, a security flaw allowed users' accounts to have their session hijacked (gaining unauthorised access to information by exploiting a valid usage session), their traffic intercepted and logged by a package sniffer. As a result, this encryption sought to correct past failings.

Just as users thought they could rest easy another flaw has been identified. Deleting a chat from your WhatsApp window will see it clear immediately and although the chat is supposedly removed from your window, it still exists on your smartphone as WhatsApp never deletes them permanently. Jonathan Zdziarski, an iOS researcher who identified this, found that WhatsApp keeps a forensic trace of the chat logs even after deletion by the user. Zdziarski also revealed that if an attacker has physical access to your phone, the stored data can be accessed.

WhatsApp accounts alone hold some of the public's most personal data, but now a person in possession of your phone could open even deleted chats. Personal Data should be protected and destroyed in a manner that safe guards an individual's right to privacy; but now with these traces, deleting a message with account details or a person's contact details may not be enough.

WhatsApp set out to prevent hacking of devices, accounts and chats and to provide users with the required protection that WhatsApp previously failed to provide. Despite the reassuring pop-up before each new message about the encryption, WhatsApp's frailty around privacy and data protection remains foreboding.

Privacy is an ever important cog in a functioning society; never more so than now. There is a fine line in balancing an individual's right to absolute privacy and the limiting of this right by governments in their combatting of terrorism, fraud and corruption and especially cyber breaches. In world where persons are increasingly making use of ever-advancing technology for the storage of their personal information as well as the prevalence of cyber breaches, the protection of this information is vital. It will be a laborious task ahead for the newly appointed South African Information Regulator as well as privacy regulators globally in ensuring this balancing act is met.

Recent developments in the office of the Information Regulator have indicated that the Information Regulator has made progress in its establishment and it is in the process of drafting the Regulations. It is imperative that every organisation in South Africa is aware of its POPI obligations and has begun to implement POPI compliance

For more information, contact:

Dean Chivers
Risk Advisory Africa Leader: Governance, Regulatory & Risk
Tel: +27 11 806 5159
Email: dechivers@deloitte.co.za

Daniella Kafouris
Associate Director: Risk Advisory Southern Africa
Tel: +27 11 209 8101
Email: dkafouris@deloitte.co.za