YAHOO'S 500 MILLION USER BREACH: NOTIFICATION REQUIREMENTS UNDER SOUTH AFRICAN LAW

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Lucien Pierce | October 5, 2016

Yahoo has **announced** that that the information of about 500 million users has been stolen. The information was stolen during late 2014. There are serious consequences for Yahoo, which include reputational and financial harm. Any regulatory and civil disputes are likely to be dealt with under Californian law (which is what Yahoo's terms of service stipulate). If Yahoo was based in South Africa, it would need to consider the impact of a number of laws including preparing for the, yet to be effective, Protection of Personal Information Act, 2013 ("POPI").

Percentage that experienced a cyber or data breach

In South Africa, data breaches can currently be dealt with quietly, without too much adverse publicity and no risk of penalties that regulators in other jurisdictions are entitled to impose. The lack of reporting requirements explains the graph above: the US **law firms** and **UK businesses** included above were obliged by law to report breaches. **South African businesses** only look good because they are not yet required to report.

Once POPI becomes law however, all organisations operating in South Africa, whether public or private, will be obliged to disclose breaches. It is therefore imperative that you really protect the integrity of personal information in your possession or under your control, by taking appropriate, reasonable technical and organisational measures to prevent the loss of, and unlawful access to, personal information.

POPI makes it obligatory to report breaches. It deals with breaches at section 22 and says:

- If you have reasonable grounds to believe that you have had a breach, you must notify the Information Regulator and the person whose personal information has been stolen (section 22(1));
- The notification must be made as soon as reasonably possible after you discover the breach, taking into account law enforcement needs and other necessary measures (section 22(2)); and
- You may only delay notification to the person (you are still require to inform the Information

Regulator) if the public body investigating or the Information Regulator instructs you to (section 22(3))

There are other provisions in section 22 that explain how you should go about notifying the people whose information has been stolen.

Yahoo's breach is neither new nor unique. There have been serious breaches and attempted breaches of personal information in the past few years. LinkedIn, Adobe and Dropbox suffered massive breaches. The South African Revenue Service, Sony, Lockheed, Citigroup, the International Monetary Fund, the Payments Association of South Africa had to take action to counter major reputational damage. Each of these organisations has had to publicise the information breach suffered and work hard to manage and repair the damage done to their reputations.

Breaches by User Numbers in Millions, Source: **haveibeenpwned.com**

All of the above organisations would likely have also suffered some sort of financial loss. Yahoo was sold to Verizon recently and the breach was not disclosed as part of the transaction: **Verizon** is not happy about this. Yahoo will need to notify its users of the breach. It may well have to also pay for "security freezes" for each of its users. At US$20.00 per user for say just 100 million of the affected users, Yahoo is looking at forking out US$2 billion! That doesn't include the cost of lawyers, PR agencies and regulatory fines.

It is almost impossible to prevent a breach from happening, but being prepared, knowing what is required of you and knowing how to act when it happens, will go a long way to reducing the reputational and financial harm your organisation is likely to suffer.

If you are doing business in South Africa, start preparing for POPI.