# POPI and your website security

By Chemory Gunko

5 Feb 2015

The Protection of Personal Information (POPI) Bill holds untold benefits for South African businesses looking to participate in the global marketplace.

But alongside that comes ramifications for every business operating in South Africa - and your website is not immune from landing you in hot water under POPI.

So what should you look at in order to ensure that your website is secured and meets the requirements of these rather stringent data privacy laws?

President Zuma signed POPI into effect at the end of 2013 and we haven't really heard too much about it since then.

FreeDigitalPhotos.com

This makes sense though, as we expected at least a year's delay while a commission was established and a Commissioner appointed. To be fair, the economic dip has probably put the whole thing on the back burner, too.

Now, however, we're a year after the POPI Bill was signed into effect and the first prosecutions can't be too far off.

You can bet your bottom dollar that they're going to be looking for companies to make examples of, which is no joke when you consider they were talking two years' imprisonment or fines of R10m as a starting point for transgressions. And if you haven't appointed a Privacy Officer, those penalties will be levied against you as the CEO or MD, personally.

So does your current website meet POPI requirements, or are you going to have to do an overhaul before you fall foul of the law?

## Hand-coded vs CMS

CMS or content managed system website solutions like Joomla and Wordpress have become very popular over the last few years, and this makes perfect sense - there's no need to reinvent the wheel every time.

Most websites have the same basic functionalities and once you've perfected those you really want to put your energy into what differentiates the site: your look and feel and content.

On the other hand, with contiguous updates and changes to browsers and browser standards, CMS platforms that are regularly updated can really extend the longevity of your site, making it much more forwards compatible and responsive than traditional hand-coded websites could ever be - for literally a portion of the effort.

This really is your first port of call when it comes to website security: making sure that your website stays updated and you meet these contiguously changing browser standards.

Yes, there are those who are going to say to you that you open yourself to more risk by utilising open-source, easy accessible software, but the benefits way outweigh any risks. With a hand-coded site, you have no guarantee of security measures at all.

The good CMS platforms all have basic security features built into them, and where vulnerabilities are identified, updates usually plug these very effectively.

## Speaking of security...

On a hand-coded website, any security features will have to be created by hand, which ties you to the developer and the way they've structured their security. Do you even know where to begin checking if this security is effective?

One of the really cool features of good CMS platforms, like Joomla, is that you have companies of top developers who create dedicated security products, like full firewalls that empower you as a non-technical person to manage your own security at an advanced level, and pretty much mitigate all the potential threats.

You have functionality that enables you to block countries that are known for high volumes of hack attempts and even to identify specific users and block them by IP address. If you don't know, an IP or Internet Protocol address is the numerical equivalent of your URL.

To put it very simply, the internet registers the computer or device you're reading this article on as an IP address that uniquely identifies you and where you are based geographically. It can be traced back to you as a specific user and can even identify the device you were working on.

## Hosting and backups

Probably due to lack of knowledge, people have a very shotgun approach to choosing a web-hosting company. Sadly, not all web-hosting companies play in the same league.

The server you host on is going to make a huge difference to the security of your site and, aside from POPI implications, a hack on your website can get your domain temporarily blocked or even permanently banned by Google and the other search engines.

A really good web-hosting company will give you three great security features - regular virus scans with reports, good c-panel access so that you can manage a lot of technical issues and backups yourself, and most importantly, will run regular backups of both your website folder structure and the linked databases.

The fastest way to restore a hacked site? Roll back to an uninfected version and fix the vulnerabilities from there.

When it comes to Google and other search engines identifying your site as a harmful site, time really is of the essence, because someone who sees that horrible message saying that this is a potentially harmful site is very unlikely to visit it again.

Multiple incidents can also see your domain permanently banned and Google can take a very long time to reverse blocking or banning: at minimum you're looking at seven days. I've currently spent nearly three weeks trying to get a client's site revisited to have a block removed. If you've ever had to try and get hold of Google for anything, you'll know that it's basically impossible to actually speak to a person not involved in AdWords sales.

Can you really afford to be without your website as a marketing tool for three weeks or more?

## Common vulnerabilities

Without fail, every time I've been called in to fix a hack in the last few years, I've seen that the vulnerability lies in forms. So much so in fact that I only use forms where they are specifically requested or required by the client now - and never on my own sites.

Like all the other bells and whistles we've become accustomed to - sliding banners, video content and responsive design - forms are just one of those things that companies seem to believe they must have in order to have a professionally developed website.

There is definitely a place for forms, but the truth is that not every company needs them. For some companies forms generate a number of enquiries; for other companies they generate little to no enquiries and an email link works just as well.

Whether or not forms make a difference to the number of enquiries you receive is something that only you will know, making this a decision that can only be made by understanding at your individual circumstances.

If forms are not elements that return customer enquiries for you then your safest bet is to forgo them altogether. If you do decide to go with forms, then I'd spend the extra money to bring in a security expert who can pay special attention to securing the forms on your website, particularly if you allow for any kind of document upload.

If you do have to go with an upload facility, be very specific about the types of files you allow to upload and always use a Captcha to prevent automated virus injections.

Aside from viruses and hacks, the other vulnerability that forms create is that they store POPI-protected information on the back end of your website. If a hacker has gained access to your site, he can probably gain access to that contact information. This is a clear infringement of POPI.

POPI governs how data is collected, stored, managed, secured, used and transported, and someone gaining access to confidential personal and contact information that you've collected for your business is a direct violation of the Bill - one that you can face severe penalties for.

## Your Privacy Statement and the Openness Principle

The last immediate thing you need to worry about under POPI is the Privacy Statement on your website.

Your T&Cs basically state the terms and conditions for using your website, while your Privacy Statement speaks to the elements of POPI: what kind of information you gather, how you will utilise, manage and store this information, who you will share it with and a high level overview of the steps you take to secure this information.

Under the Consumer Protection Act (CPA), T&Cs, contracts and elements like privacy statements must be written in plain, simple English that the layman can understand - so you can't hide behind technical lingo, jargon or legalese either.

An important element to understand with your privacy statement under POPI is a factor called the openness principle. If you openly state how you will be using, sharing and managing the data you collect, and someone still elects to give you their information, then you are pretty much on the right side of the law.

So you want to ensure that every form has a checkbox where people agree to the terms of your Privacy Statement and T&Cs. Hyperlink the Privacy Statement and T&Cs wherever you mention them and always include the disclaimer that you reserve the right to change them without notice. Make this a required field, so that if they don't agree to your terms they cannot submit their data to you.

If something goes horribly wrong with a data leak or it can be proven that you are flouting the law, you will probably still be prosecuted, but for the most part the openness principle is going to be your saving grace under POPI.

An interesting fact here is one of the provisions of the Bill: you are required by law to report any infringements to the Commissioner yourself - not reporting an infringement can see you face penalties too.

## POPI in the real world

Obviously POPI is going to impact business on a much deeper level than just your website - and the Bill has a lot of implications for the way we conduct marketing in the digital space.

From ongoing training of staff to access control around information and even appointing a Privacy Officer, POPI has the power to impact pretty much every aspect of your business, and it has ramifications for a number of your internal processes.

If you haven't looked into the POPI Bill, or given it any thought, I'd strongly suggest you do that now.

If you don't you could find yourself crippled with a massive fine or even imprisonment... and following the international lead you can be sure the Commissioner will be looking for companies to make examples of once the commission is in place.

## ABOUT CHEMORY GUNKO

Chemory Gunko is a seasoned Creative Director, a certified NLP Practitioner, Ericksonian Hypnotherapy Practitioner, Energy ReSourcing Practitioner & Life Coach, among others. She works as a marketing consultant and provides copywriting, SEO, graphic design and Joomla! website services.
- POPI and your website security - 5 Feb 2015

View my profile and articles...