POPI and social media

Don't get too personal

How times have changed. Social media marketing has evolved from being a bit of fun on the side to an absolute must-have for all businesses that want to remain relevant. Social media isn't just fun and games, though: it gives you access to personal information like never before. The big question is how the rules of POPI apply when using social media for marketing and client service platforms.

Last year we published a blog on [Social Media in Financial Services](#) which serves as a good intro to this article. This month we dive into the details of how POPI in particular should impact your social media use.

Whose data is it anyway?

The main impact that POPI has on your social media activities is that all data collected from the various platforms is governed by the Act, even though the information was publicly available. If, for instance, you grab a client's phone number from LinkedIn to implement his or her investment, you will be obliged to protect the data thereafter.

P is for Privacy (and Policy)

Some customers unwisely expose their personal information such as their identity numbers on customer service pages. It's essential to remove the information immediately when this happens and start up a personal conversation by phone or email. The process of switching to a private conversation needs to be very clearly incorporated into your company's social media policy. And, if a third party such as an ad agency manages your social media pages, it's essential that they're aware of the Act and abide by the principles of privacy.

Tweeting under the influence

One of the Act's aims is to ensure that personal information is used only for its original purpose. This affects the rights to the use of the data on influencer's followers. Although you may pay an influencer to promote your brand, POPI regulates that their followers' data cannot be used for other marketing purposes. On a related legal note, it's important to specify who owns the content that influencers post. It's also essential that they clearly display that they are being paid to market the company or brand.

Beware of sudden lane changes

Another POPI challenge comes when a business changes how it uses a particular platform. For instance, a Facebook page which was initially used for customer service queries may, over time, evolve into a sales platform. Clients can easily unfollow you if they don't want the sales information, but POPI says that the onus is on the business to first gain permission from an individual. In short, businesses need to communicate upfront that by using the platform for

customer services, customers grant the business permission to send them different kinds of information.

This also relates to the data gained from competitions on social media. Participants need to know that by entering the competition they grant the business the right to send them marketing material. Alternatively, the data should be destroyed after the competition.

Thou shalt be hacked

Another of POPI's objectives is to ensure the safety of customers' data as security breaches are forever on the increase. A recent survey conducted in the US by PWC showed that 90% of large organizations suffered a security breach in 2018 and that 59% of employees steal proprietary data when they quit or are fired.

It's no longer a question of *whether* you'll be hacked, but *how* you'll be hacked.

McDonald's corporate Twitter account was hacked, and a message posted calling Donald Trump a "disgusting excuse of a President with small hands". McDonald's made a public apology, despite a generally positive response to the tweet.

So, be sure to check the company's security settings on each platform and use excellent anti-virus software. You should also scan and decode links to make sure they're the real thing and adopt a **very strong password policy.**

Big data can't be personal

Big data analytics has helped many businesses strike a balance between optimizing their marketing efforts and not annoying customers with unsolicited communication. However, in order to continue to maintain this balance and provide customers with the information they want, they do need access to as much data about their customers as possible. The trick is that a lot of this information is personal, meaning that the process of analyzing data may not be in keeping with POPI.

Don't panic, though. Businesses can still get excellent results from analytics without viewing personal information. There are excellent software solutions which hide sensitive data from the analysis but still yield very useful results. Businesses can also implement asset control so that only those with the right permissions can access personal information.

Clouding the issue

One of the most interesting aspects of POPI to consider is the offshore storage of data where POPI doesn't apply. If you're a Facebook user, for instance, your data is most likely stored in Forest City, North Carolina – a place which has the dubious distinction of being home to more computer servers than people. (Cloud hosting is also tricky with regards to POPI but that is a topic for another day.)

A word of warning for individuals

On a personal note, do remember that if you're active on social media and publish personal information, you won't be able to turn to POPI or your constitutional right to privacy if the information gets into the wrong hands.

This blog has detailed just a few of the ways in which POPI impacts social media…telling the whole story would fill a lengthy tome! That's what it makes a lot of sense to appoint a POPI compliance officer to work with a specialized lawyer and IT provider to structure a system and determine policy and procedure to ensure your company is compliant with POPI. Social media isn't a game anymore.

FinCommunications provides seminars on social media and the law. Feel free to email linda@fincommunications.com to take the conversation to the next level.