

# Too good to be true? What about your privacy?

7 December 2022 11 min read

It is common cause that the tech-bug has bitten us all (almost), and the evolution of the mobile application (“mobile app/app”) industry is but a symptom of the world’s newly found and embraced technophilia. Since the initial ‘app-craze’ of the early 2010s, the mobile-app spectrum has grown to include a variety of not only social media apps, but also more functional apps such as Apple’s ‘Find My iPhone’ and Android’s ‘Bouncer’ apps.

Smart, safe and efficient communication has become a priority for many of us who enjoy the fruits of the wonders that come with our techno-globalised world.

The shift from vanity to functionality in the mobile-app space is a breath of fresh air. However, it should be borne in mind that times have changed not only in respect of mobile app development and technological advancement, but also in terms of how we consider issues of privacy and the handling of individuals’ personal information.

In this article, we explore data privacy concerns in the context of the world-renowned Truecaller mobile app, and others whose services are similar thereto. More specifically, we will focus on concerns relating to compliance with the [Protection of Personal Information Act, 2013](#) (“POPIA/the Act”) in the context of the processing of the personal information of non-users/non-subscribers.

POPIA compliance strategy & governance framework – [Read article](#)

## How it works

The Truecaller mobile app (“[Truecaller](#)”) has over 320 million users active users across the globe. Truecaller is able to show the owner of a number that a user does not yet have through its universal database which is supported by crowdsourcing of data from users. There can be no doubt that the ability of a user to know the identity of the caller before even taking the call is beneficial for a number of reasons.

**However**, there may be data-privacy gremlins lurking in the background.

When a user downloads the Truecaller app directly from the Truecaller website, Truecaller prompts the user with an option to upload their full address book or contact list to the Truecaller servers, as part of the app’s crowdsourcing features. This information is then uploaded to the company’s database, which is stored on a foreign server. In addition to the prompts related to a subscriber’s address book or contact list, Truecaller allows subscribers to manually submit the details of a number which was not yet available on the Truecaller database.

There could very well be privacy concerns with the manner in which Truecaller’s goes about offering its service, especially considering those persons whose contact information – whether sourced from a Truecaller user’s contact list/address book, or submitted manually, forms part of the Truecaller database even though such a person may not have registered for the Truecaller service.

## Accordingly, Truecaller processes the personal information of two categories of data subjects.

The **first category** consists of those persons who have registered for the Truecaller service (i.e. primary data subject);

the **second category** consists of persons who have not registered for the Truecaller service but whose personal information has been crowdsourced by Truecaller as a result of access derived from the contact list(s)/address book(s) or manual submissions of existing subscribers.

## A POPIA perspective

---

At the outset, it should be noted that section 6 of POPIA provides for exclusions from the applicability of the Act, and states that POPIA does not apply to the processing of personal information in the course of a purely personal or household activity.

In *Cool Ideas 1186 CC v Hubbard* and Another, the Constitutional Court held that a fundamental tenet of statutory interpretation is that words in a statute must be given their ordinary grammatical meaning unless doing so would result in an absurdity.

Thus, even though POPIA does not define the term “personally activity”, the ordinary grammatical meaning of the phrase leads one to safely infer that a database of phone numbers and/or addresses stored on an individual's mobile, and used solely for the purpose of that individual's private communication with such individuals, constitutes the processing of personal information for personal use.

## Lawful basis for processing

---

In terms of the Protection of Personal Information Act 4 of 2013 (“POPIA”), a responsible party may only process the personal information of a data subject if such a party has a lawful basis to do so. Such a lawful basis may, for example, be consent the data subject, the responsible party's compliance with a legal obligation or based on a legitimate interest of the responsible party.

Indeed, it is entirely possible that Truecaller has a legitimate basis for processing personal information of a primary data subject who subscribes to the Truecaller service. However, on what basis is Truecaller processing all the contact information (i.e. address book and/or contact list) that the subscriber holds – which may or may not include the information of non-users.

What this means is that it is entirely possible that non-subscribers have no knowledge of the availability and/or use of their data by Truecaller, as derived from the manual submissions of users or the uploading of address books/contact lists of subscribers to the Truecaller servers.

**Furthermore**, Truecaller's privacy policy provides that personal information may be transferred to other users and/or third parties, and that such transfer may be to a country that does not have data privacy laws equivalent to the laws of the data subject's country of residence. It is unclear whether the transfer is in respect of the personal information of a subscriber (i.e. primary data subject), or if it includes the personal information of a non-subscriber (i.e. secondary data subject).

Nevertheless, section 72 of POPIA provides that a responsible party may not transfer personal information about a data subject to a third party who is in a foreign country unless, inter alia, the third party recipient is a law, binding corporate rules or binding agreement that provides an adequate level of protection.

## The measure of what constitutes an adequate level of protection is two fold:

- the law, binding corporate rules or agreement effectively upholds the principles of reasonable processing in terms of POPIA; and
- the law, binding corporate rules or agreement includes provisions that are substantially similar to POPIA insofar as the conditions for the lawful processing of personal information from the responsible party to the third party recipient.

Thus, it is neither here nor there if the transfer of personal information relates to a data subject who is Truecaller subscriber or non-subscriber, because the starting point of compliance in respect of transfers to foreign countries is whether the third party recipient is located in a jurisdiction whose privacy legislation offers a similar level of protection as South African privacy laws.

## Notification of processing – whose responsible anyways?

---

POPIA defines a responsible party as a public or private body which alone, or in conjunction with others, determines the purpose of and means for processing personal information. Conversely, an operator is defined as a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

Accordingly, the nature of the responsible party-operator relationship is one within which the responsible party is dominant to the extent that it is the responsible party who one determines the purpose for processing the information collected, the nature of the personal information collected, the duration for which it will be kept as well as the manner in which the information is processed.

POPIA provides that a responsible party must take reasonably practicable measures to notify a data subject of how it will use, store, transmit, collect and/or access the personal information of a data subject, even if such information is not collected directly from the data subject.

However, the Truecaller privacy policy states that users must confirm with another party (i.e. secondary data subject) whose details they share with Truecaller before sharing such details. In other words, this privacy clause shifts responsibility of notifying a data subject, whether primary or secondary, that his/her personal information is going to be processed by Truecaller.

Inasmuch as this privacy clause constitutes a proverbial 'passing-of-the-buck' by Truecaller, it is important to note that since Truecaller is the party who determines the mandate and process for collecting the personal information, be it from a primary data subject (i.e. Truecaller subscriber) or a secondary data subject (i.e. non-subscriber of Truecaller), then Truecaller remains the responsible party and cannot be absolved of its responsibilities in terms of POPIA simply because the information was collected from an operator – in this instance, the Truecaller subscriber.

Indeed, the Truecaller privacy policy provides for 'unlisting by non-users', and states that any person who is not a user and does not wish to have their contact information made available through the app's 'enhances search' feature may exclude themselves further from queries by notifying Truecaller via its website.

However, the concern is how exactly a secondary data subject would be notified that their personal information is on the Truecaller database in the first place, especially considering that Truecaller's privacy policy places the notification burden on operators (i.e. primary data subjects). To this end, Truecaller should notify, by SMS or email, each person who is added to its database, and direct such person to the Truecaller privacy policy – highlighting the data subject's ability to delist from the Truecaller database.

## Conclusion

---

Techno-globlisation, and the strides made in respect thereof, is something to be embraced and celebrated. However, the manner in which we engage with the wonders of our technocentric world should always be scrutinised in the context of whose personal information is collected (be via consent or some other lawful basis), how such information is accessed and what the information is used for.

Furthermore, individuals should take more accountability when it comes to the manner in which they allow for the accessing/sharing of the personal information of persons who may not necessarily want their information accessed by, inter alia, mobile apps; and remember that the consent they provide to such apps does not just effect the primary data subject, but have implications for secondary data subject too.

Irrespective of the various levels of accountability that exist in the context of the use of mobile apps such as Truecaller, the overarching theme that should always be borne in mind is the inability of a responsible party to shift its responsibilities to

operators (i.e. mobile app subscribers); and the insufficiency of consent when it comes to ensuring compliance with POPIA from secondary data subject point of view.

After all, when was the last time a friend, colleague, or even an acquaintance, obtained your consent to share or provide access to your personal information via an app on their mobile?

Footnotes

- [1] Dictionary.com “[Technophile](#)” available at accessed on 31 October 2022.
- [2] [Apple](#) available at on 31 October 2022.
- [3] Google Play “[Bouncer – Temporary App Permis](#)” available at accessed on 1 November 2021.
- [4] [Truecaller](#) is a Swedish company founded in 2009 in Stockholm, Sweden, by Nami Zarringhalam and Alan Mamed, available at about accessed on 28 October 2022.
- [5] My Broadband “[Truecaller violates South Africa's new privacy laws – Legal experts](#)” accessed on 28 October 2022.
- [6] My Broadband “[Truecaller violates South Africa's new privacy laws – Legal experts](#)” accessed on 28 October 2022.
- [7] My Broadband “[Truecaller violates South Africa's new privacy laws – Legal experts](#)” accessed on 28 October 2022.
- [8] My Broadband “[Truecaller violates South Africa's new privacy laws – Legal experts](#)” accessed on 28 October 2022.
- [9] POPIA section 1 – ‘data subject’ means the person to whom the personal information relates.
- [10] POPIA section 6(1)(a).
- [11] 2014 (4) SA 474 (CC).
- [12] POPIA section 9.
- [13] POPIA, section 11(a).
- [14] POPIA, section 11(c).
- [15] POPIA, sections 11(d).
- [16] My Broadband “[Truecaller violates South Africa's new privacy laws – Legal experts](#)” accessed on 28 October 2022.
- [17] My Broadband “[Truecaller violates South Africa's new privacy laws – Legal experts](#)” accessed on 28 October 2022.
- [18] Truecaller “[Truecaller Privacy Policy](#)”, accessed on 2 November 2022.
- [19] POPIA, section 72(1)(a)(i).
- [20] POPIA, section 72(1)(a)(ii).
- [21] POPIA, section 1.
- [22] POPIA, section 1 – natural or juristic person.
- [23] POPIA, section 1.
- [24] POPIA, section 1.
- [25] POPIA, section 18.
- [26] [Truecaller Privacy Policy](#) accessed on 1 November 2022.
- [27] My Broadband “[Truecaller violates South Africa's new privacy laws – Legal experts](#)” accessed on 28 October 2022.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)