**Opinion**

**29 January 2021**

**WhatsApp Online Privacy Concerns: Is this real or just a storm in a teacup?**

WhatsApp, a popular instant messaging platform owned by Facebook, recently announced new updates to its terms and privacy policy[[1]](#footnote-1). Key to these updates are how:

* Users’ data will be processed and shared with third parties;
* Business users can use Facebook-hosted services and manage their WhatsApp chats; and
* WhatsApp partners with Facebook to offer integrations (including sharing information) across Facebook Company Products[[2]](#footnote-2) (which are subject to separate, stand-alone terms of service and privacy policies).

All users of the WhatsApp messaging platform, except those located in the European Union (thanks to the enforceable and tighter privacy legislation in General Data Protection Regulation[[3]](#footnote-3) (GDPR)), will need to accept these updated terms and conditions, or may not be able to use the WhatsApp service after 8 February 2021[[4]](#footnote-4). This has expectedly caused a lot of hype, outrage and misinformation across various online and traditional media platforms, leading to a number of reviews, opinions and anti-WhatsApp movements. Still, users are faced with deciding their fate regarding WhatsApp.

**To WhatsApp or not to WhatsApp?**

Many people are looking for alternatives to the popular instant messaging application. Although this may be a burning concern for many users, it is certainly not the most critical to address, in our view. Instead, our biggest problem is that social mediausers continue to share their personal information without realising the impact that the presence of this information online can have on their privacy. Unfortunately, this is also aided by the default privacy settings that most platforms come with. Social media users freely provide their personally identifiable information, such as mobile numbers, email addresses, photos, names of family members, location, etc. and, thus, unknowingly compromise their privacy.

Additionally, there is a misnomer among users that changing from one platform to the other may change their online privacy “fortunes”. In fact, the opposite may be true, especially when a user is now compelled to use multiple platforms, because their contacts may be scattered across all of them. This will only mean their online privacy becomes even trickier to manage as all the platforms will now be collecting their personal data.

**Telegram, Signal and others: Same WhatsApp Group?**

Jan Vermeulen from MyBroaband[[5]](#footnote-5) recently published a comparison of these common alternatives, which covers a number of aspects, including technical differences, albeit it is not fully comprehensive. Therefore, in this piece, we will not repeat the same information.

We will rather focus on the prominent alternatives suggested, which are Signal[[6]](#footnote-6) and Telegram[[7]](#footnote-7). The common threads are that these platforms provide better online privacy and security. Furthermore, as a by-product, these two touted alternative platforms have experienced a surge in users signing up for their services in the past few days. If one decides to opt for these alternatives, it is important to consider the following features that may affect their online privacy:

**Telegram**: Certain personal and technical information will be collected as per their terms of usage[[8]](#footnote-8). This information includes the user’s contact number, profile name, picture, device data and IP address. If default settings are not changed (which many users are not aware of), this may adversely impact one’s online privacy.

This includes default settings of sharing one’s phone number, status, profile name and picture with “everybody”, even people that the user does not know. Further, if default settings are not changed, the user can be added to any group chats by anyone. Telegram also synchronises the user’s entire contact list with its servers, unless the user explicitly changes the default settings.

Another feature on Telegram that users may also not be aware of is what is called *“People Nearby”*, which allows one to find contacts and groups nearby their location. This allows one to pinpoint “unknown” contacts that are a few metres away, and join or view chats in public groups.

The negative and insecure side of the “*People Nearby*” feature is the exposure to explicit content and possibilities of being tracked. If the one’s children are also going to be migrating to Telegram, when one does so, they have to be very careful that such features are disabled for the sake of safety, which is not so obvious to non-technical users.

One other aspect to consider with Telegram is that chats are cloud-based. This is to allow one to access the Telegram service across multiple platforms and devices (e.g. mobile and web). However, this comes with the privacy limitation that cloud chats are not end-to-end encrypted, leading to the possibility of one’s chats being read by third parties, including Telegram, and ultimately impacting on one’s online privacy.

**Signal**: If one decides to migrate to Signal, they need to be aware that Signal also collects and stores limited personal and technical information, in order to operate its services. For one to also use Signal, they need to provide permission for Signal to access their contacts list, as well to things such as photos, and give it the ability to make recordings.

Depending on the app’s settings, one’s mobile device’s IP address may also be exposed. Signal also has limited features compared to WhatsApp and Telegram. On the positive side, Signal tends to support more privacy features, such as screen security, to prevent over-the-shoulder snooping, similarly to WhatsApp and Telegram.

When one opts to use Signal, they ultimately agree that their personal data (e.g. phone number), including other limited metadata, will be transferred and stored in the United States of America. However, the GDPR has a huge impact on strengthening a user’s privacy if the user is not from Europe, so this is also an important aspect to consider when deciding on privacy and platforms.

Signal also indicates that it may share a user’s information with third parties (e.g. YouTube or Spotify) to provide its services[[9]](#footnote-9). However, unlike WhatsApp, Signal is unequivocal that it does not sell, rent out, or monetise users’ personal data or content in any way.

There are many other security and privacy studies that have been done on these instant messaging platforms, and our intention is not to repeat those, but to indicate that, as much as many of the instant messaging platforms, including WhatsApp, use end-to-end encryption, this is not a panacea for online privacy. Chat messages can still be exposed and shared, for instance, with law enforcement agencies, particularly when illegal activities are being investigated.

**Other considerations**

Over and above the privacy and security issues, security and usability of these instant messaging platforms will always come into play when one decides to use one platform over the other. Online privacy, security and usability remain a conundrum for ordinary individuals.

As much as Signal is promoted as the most privacy-preserving platform compared to Telegram and WhatsApp, it may, in the meantime, suffer from usability issues, such as limited quality of video calls, photos and lack of features. In this instance, the strongest privacy may be overridden by the limited and/or low-quality communication features from users’ perspectives.

From the security point of view, Signal uses the same encryption software used by WhatsApp, which is open source. Telegram also uses its own proprietary encryption standards among other open source encryption standards. However, when it comes to cloud chats, no end-to-end encryption is enabled.

**What can social media users do?**

While we may agree that there are instant messaging platforms that collect and/or share a limited amount of personal information compared to others, our view is that online privacy is more than just data collection by the service providers. It is equally the information that social media users voluntarily share without considering privacy implications.

It is important for users and business to intensify privacy awareness when using any of the “free” online services. Further, there is a need to educate users on how to use technology platforms in a privacy-preserving manner, including guarding against overly sharing personally identifiable information, such as images, videos and any other confidential information, on these platforms.

It is our view that there is ‘*a false sense of online privacy*’ when users opt-in to provide their personal information in order to use free online services, which indicates a lack of online privacy understanding and awareness. As the common saying goes, "If you're not paying for something, you're not the customer; you're the product being sold".

We posit that, irrespective of an alternative messaging platform that users may opt for, online privacy is still one’s responsibility. In addition, it is also important for users to be aware that all the different instant messaging platforms have their pros and cons in terms of online privacy, security and usability. Therefore, it is important that users familiarise themselves with the usage and privacy terms of any service that they decide to adopt.

By Dr Jabu Mtsweni and Dr Noxy Gcaza

Dr Jabu Mtsweni manages the CSIR’s Information and Cyber Security Center.

Dr Noxy Gcaza is the CSIR’s research group leader for Governance, Privacy and Trust at the CSIR’s Information and Cyber Security Center.

*N.B. Both write this opinion piece in their personal capacity.*

For more information, please contact:

Dr Jabu Mtsweni on 072 407 4757

OR

Dr Noxy Gcaza on 074 279 7436

1. <https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en> [↑](#footnote-ref-1)
2. <https://faq.whatsapp.com/general/security-and-privacy/the-facebook-company-products> [↑](#footnote-ref-2)
3. <https://gdpr-info.eu/> [↑](#footnote-ref-3)
4. *This has now been delayed for at least 3 months\** [↑](#footnote-ref-4)
5. <https://mybroadband.co.za/news/security/382062-whatsapp-compared-to-alternatives-telegram-and-signal.html> [↑](#footnote-ref-5)
6. <https://www.signal.org/> [↑](#footnote-ref-6)
7. <https://telegram.org/> [↑](#footnote-ref-7)
8. <https://telegram.org/privacy> [↑](#footnote-ref-8)
9. <https://signal.org/legal/#privacy-policy> [↑](#footnote-ref-9)