# WhatsApp Is Crumbling And We Aren't Rumbling

Pompeii is a city of legend and myth whose story got frozen in time by ash and dust in a catastrophe that could have been avoided to an extent had its inhabitants listened to Mount Vesuvius' warnings. But they didn't, and their mistake will never be forgotten, as history isn't forgiving and the remnants are perfectly preserved.

Probably, dear reader, you may be wondering what Pompeii has to do with anything, particularly with any current news. Fortunately, if you keep reading (won't be long, I promise), you may have your questions answered.

We all know about WhatsApp, the giant in instant messaging services, the app we all have on our phones and has become a daily driver that makes our lives easier. It all started with good intentions — a way of allowing people to communicate easily and for free with their loved ones. But alas, in February 2014, the giant gave its first warning when it was bought by Facebook.

The second of many warnings that were to come revealed itself in the shape of the founders of the app fleeing the company because they considered whatever was happening in WhatsApp's backstage dangerous. To be precise, they fled because of the rampant privacy violations that were taking place systematically for all users. Yet, no one paid attention and so, Facebook kept rumbling and getting bigger by the day, not unlike Mount Vesuvius.

The last spectacular warning, the one that finally made people scratch their head, was a change in WhatsApp's new policy update. On January 6, 2021, WhatsApp announced an update on its terms of service and privacy policy to be effective from February 8, 2021, onward. The announcement also mentioned that users who refuse to accept the new policy would no longer be allowed to use WhatsApp.

This is the content of the controversial update that led to a mass exodus of users switching to alternative messaging apps including Signal and Telegram. Basically, the update gave an extraordinary amount of power to WhatsApp (aka Facebook) over their users' data, with no way of reasonably avoiding it.

The exodus that took place weeks ago shows how much the current generation values their privacy and is willing to take steps to protect it. However, it was not enough because this mass shift only sent WhatsApp to its damage-control mode. WhatsApp postponed its policy update until May 15, 2021 (so most people forgot about it again), and released a blog post explaining how user privacy is important to them. WhatsApp's users even saw a status message from WhatsApp of a banner explaining the users 'how private and secure WhatsApp is.'

Today, I will explain this post in clear and easy-to-understand terms. I will also try to convince the readers to delete WhatsApp and use an ethical alternative, or at least one that doesn't milk them like data cows.

# Does WhatsApp Protect And Secure Your Personal Messages? Let's Find Out.

***1. We can't see your personal messages or hear your calls, and neither can Facebook****: Neither WhatsApp nor Facebook can read your messages or hear your calls with your friends, family and co-workers on WhatsApp. Whatever you share, it stays between you. That's because your personal messages are protected by end-to-end encryption. We will never weaken this security, and we clearly label each chat, so you know our commitment. Learn more about WhatsApp security here.*

In theory, WhatsApp chats are end-to-end encrypted. WhatsApp, Facebook, or anyone in between, cannot read your messages. I say 'in theory' because there is no way of proving that. WhatsApp is a closed sourced proprietary software. A closed source software can be defined as a proprietary software distributed under a licensing agreement to authorised users with private modification, copying and republishing restrictions.

In simpler words, **the source code is not shared with the public for anyone to look at or change**. Closed source is the opposite of open source. Thanks, Wikipedia! So, we can't know what is going on behind the code. It is also quite likely that there is a backdoor in the WhatsApp source code, leaking all your sensitive data to governments, hackers, advertisers and the highest bidders.

Even with the encryption in place, and assuming that it's not a scam, WhatsApp regularly asks its users to make a security copy of their chats in the cloud, a copy that, by the way, is not encrypted and is indeed examined by, for example, Google Drive. So, like the Pompeii inhabitants, we are having our mistakes frozen and analysed forever.

This is why we should use an open sourced software.

***2. We don't keep logs of who everyone is messaging or calling****: While traditionally, mobile carriers and operators store this information, we believe that keeping these records for two billion users would be both a privacy and security risk, and we don't do it.*

This is hard to believe. Isn't WhatsApp collecting 'metadata' (that too, unencrypted) on its users?

Metadata is data about your actual data. It can be used to know a lot about you, like;

1. With whom you've been in contact, when and where.

2. When you are awake and when you go to sleep.
3. Which doctor you go to.
4. To whom you write a lot and to whom not at all.
5. When you are at work.
6. When you are sick and, when and where you go on a vacation.

From this type of data, WhatsApp/Facebook can create a profile about you, which they can sell to advertisers.

***3. We can't see your shared location and neither can Facebook****: When you share your location with someone on WhatsApp, your location is protected by end-to-end encryption, which means no one can see your location except the people you share it with.*

That's true because everything you share is protected by end-to-end encryption. Nobody can read your messages except the recipient.
This does not mean that WhatsApp or Facebook cannot collect your location data.

WhatsApp and Facebook cannot see your 'shared location'. But both of them can see your current location because it's as easy as looking at the signal of your mobile phone and finding out where it is coming from.

***4. We don't share your contacts with Facebook: When you give us permission, we access only the phone numbers from your address book to make messaging fast and reliable, and we don't share your contacts lists with the other apps Facebook offers.***

*"WhatsApp does not share your contact lists with other apps Facebook offers,"* and
*"WhatsApp does not share your contact lists with Facebook."*

Can you spot the difference?

***5. Groups remain private:*** *We use group membership to deliver messages and to protect our service from spam and abuse. We don't share this data with Facebook for ads purposes. Again, these personal chats are end-to-end encrypted, so we can't see their content.*

Groups remain private, really? A bug discovered on WhatsApp said otherwise. Over 400K, private WhatsApp group invite links are exposed to search engines. Your WhatsApp groups may not be as secure as you think they are. You can also watch this video to learn more.

# What Can I Do To Protect Myself And My Loved Ones?

First, look at open software options, Signal being the most famous one, thanks to its unbreakable encryption and the fact that they refuse to collect basically any data about you. Moreover, the

company can’t be bought or sold, as a consequence of its nature of being a non-profit organisation.

# Let’s switch to Signal!

If you don’t trust me, listen to Edward Snowden, Elon Musk, Jack Dorsey, Laura Poitras, Bruce Schneier and millions of other Signal users.

## You may have heard of Telegram, but why do I avoid recommending it?

Mainly, because it likes to keep its practices in the shadow, and is unclear when it comes to answering easy and direct questions. They do, however, have excellent functions and an amazing UI.

Let’s avoid being another Pompeii, simply by listening to all the warnings we have been issued so far, and knowing that there are many alternatives to WhatsApp (not only Signal or Telegram). Protect yourself and protect others. What is allowed today may not be so in the future, and everyone knows that once something gets uploaded on the internet, it there to stay forever.

So, what will you do, dear reader? Freeze or survive?

---

Revision #1
Created 5 November 2022 09:52:30 by ponytail
Updated 29 November 2022 05:45:15 by ponytail