BeTECHSavvy
Securing Your Digital World

NATIONAL TRADING STANDARDS
Scams Team

Are You Aware Of How Secure The

Popular Media & Messaging Apps Are?

Mitigating The Risks Of Use

Incorporating
Umbrella Consulting

Introduction

This document shows how much data & information is collected by popular apps; your digital identity & privacy is more at risk every day. Do not just give your privacy away!

Learn to take control of your digital self, in the same way that you would take control over your personal health, or your savings, or your right to vote.

Hi... My name is Ben Hill and I have always had a keen interest in computers and have over 20 years of experience in IT security & privacy, on numerous different Operating Systems, operating in various environments.

Having a productive but private online digital life is important for you, your business and your family to get the most from online experiences. With the amount of information that we share online, it is important that we retain the ability to define the boundaries of our digital lives. While many people already have their own go-to tips and tricks, for others, identifying a pragmatic approach to digital privacy and security might seem overwhelming.

Whilst the big Social Media companies claim that their applications are secure and private, are you aware of how much information they are ***REALLY*** harvesting from you?

I will break down the privacy / information collected by some of the popular Social Media / messaging apps!

Benjamin Hill

An introduction to a smart way to help protect your privacy online

Do not overshare on social media. Providing too much information on Facebook, Twitter, and Instagram could make it easier for cybercriminals to obtain identifying information, which could allow them to steal your identity or to access your financial information.

Unfortunately, many people do not take this advice. In a 2018 US study, the Identity Theft Resource Center found that approximately 52 percent of respondents shared personally identifying information through social media sites.

And that is just the start of the oversharing. The same study found that about 48 percent of respondents shared information about their children, while nearly 33 percent shared information about their location. A total of 42 percent of respondents shared information about their travel plans through social media.

To protect your privacy online, think twice. Does everyone in your social media profiles, need to know everything about you; which could make you an easier target for identity theft. Explore different privacy settings, too. You might want to limit the people who can view your posts to those you have personally invited.

Once online, always online: With anything you post online, it's out there for everyone to see, so be careful with the identifiable information you use in your social media profile and which sites you sign up to.

This all may seem like common sense, however, as we become more dependent on mobile technology and these applications to keep us connected in a digital world, we can easily become more complacent.

The major technology companies all claim to take your security and privacy seriously, but people should understand the difference between 'data / information ***security***' and 'data / information ***privacy***', as the two are very ***separate*** & ***different***.

Mobile phone manufacturers will all claim that their devices and operating systems are secure; Apple with its closed proprietary iOS, Samsung with its Knox security, Google with its Titan chip and there are advantages and disadvantages with both. Each manufacturer will have different data collection and transmission policies and how many people have read these in depth or do you take them for granted (I know that I used to)?

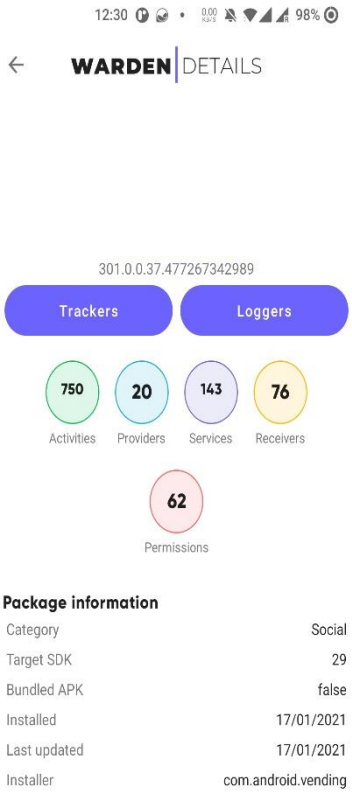
Many consumers are more concerned with the specifications of their devices (how good are the cameras?, how much storage does it have?, how powerful the device is, its design etc) than the security and privacy of the data stored within in. This has allowed manufacturers of technology and technology applications, to be less transparent about what information they collect and indeed, what they do with the information that they do collect. It is much easier to focus your attention on how secure a device/application is, rather than inform consumers on how much information they are harvesting.

A Comparison of the popular social media/communication applications

How I have examined the data / information privacy of the apps

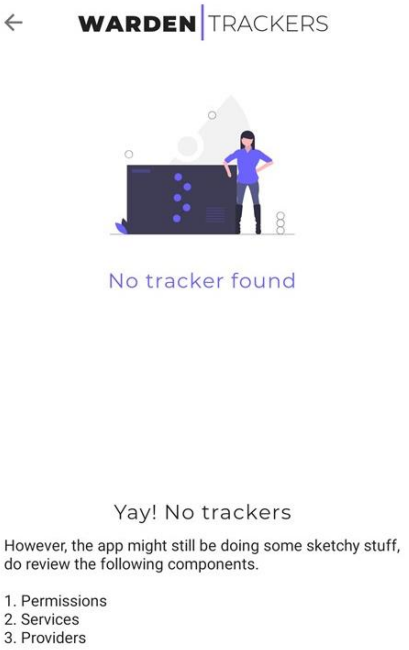
It is possible to view and adjust certain privacy settings in most Operating Systems including Windows, Mac OS, iOS and Android. It is also possible to install various applications on mobile devices to see even further, what information is being gathered and/or transmitted to the application Developers and to a degree, harden the system to prevent or lessen the amount of telemetry sent to the manufacturers.

I used an open-source application, **App Warden**, which analyses various privacy options of a mobile Application using a static list of trackers and loggers compiled by French non-profit **Exodus Privacy**.



It will let you disable various aspects of telemetry and information gathered that can then be passed on via built-in trackers or loggers.

The higher number of permissions granted and services used, allows for more activities (i.e. metadata or information) to be recorded and harvested. Most of the permissions are hidden by default on applications, to prevent disabling.



The more providers and receivers that are active within an application, then more activities can be sent via any trackers or loggers.

The application also shows which companies can track your information.

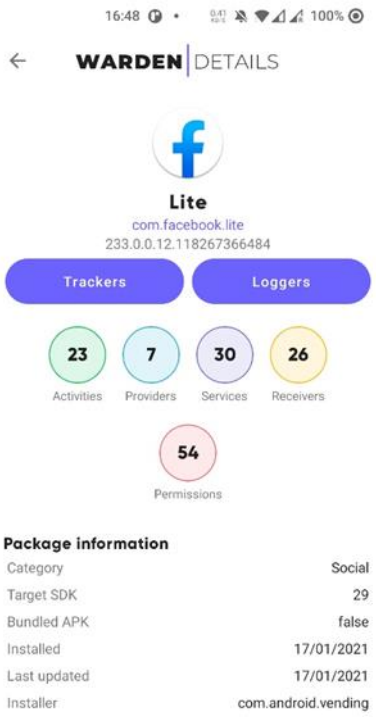
You may be surprised at how much information is being harvested and transmitted or tracked, not only by the application creator, but third-party companies too.

1. Facebook vs Facebook 'Lite'

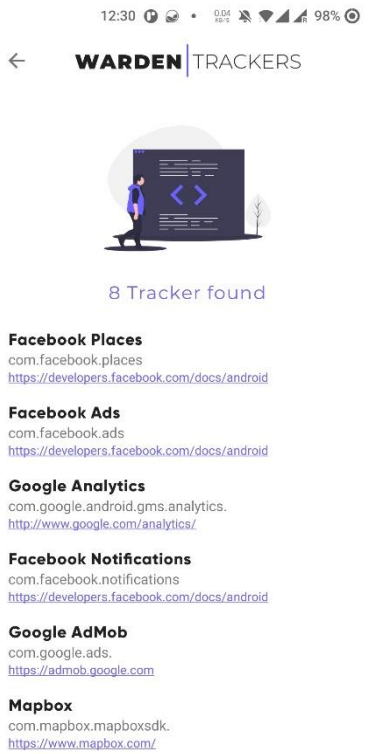
In looking at the Facebook Social Media applications, I compared the amount of data that is harvested, transmitted or tracked for the default applications (on the left below) versus their 'lite' version (on the right below).

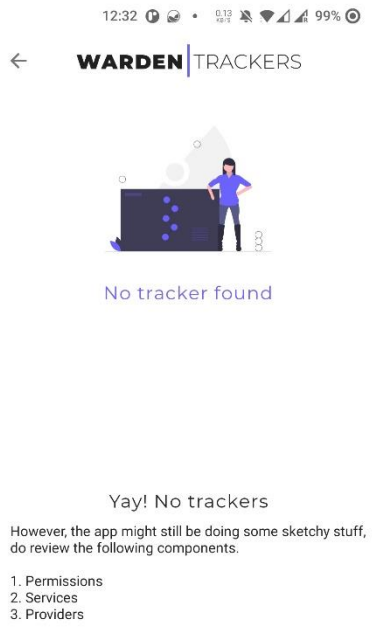
The lite versions were developed specifically for developing countries, where there is a need for connectivity, but where the price of data usage is higher. In these countries, targeted advertising is not done to the same degree as the advertising revenue is not generated to the same level as in the developed world.

If you must use an application for Facebook, you will see that the Facebook Lite has much better privacy, compared to the full version. Use this version for better privacy as well as using less data.



Funnily enough, unlike its bigger brother, has NO trackers or loggers! This is the perfect option for privacy conscious users!



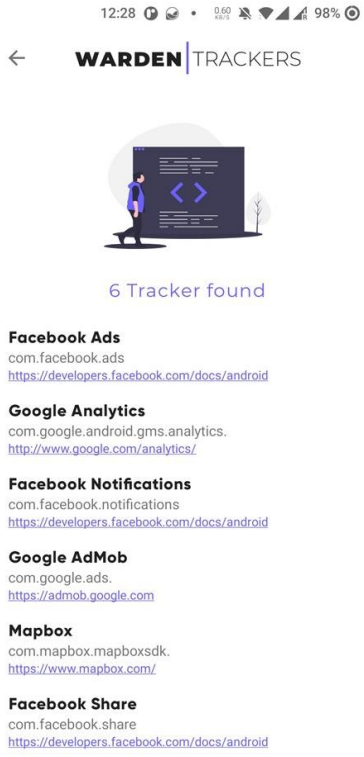


2. Messenger vs Messenger 'Lite'

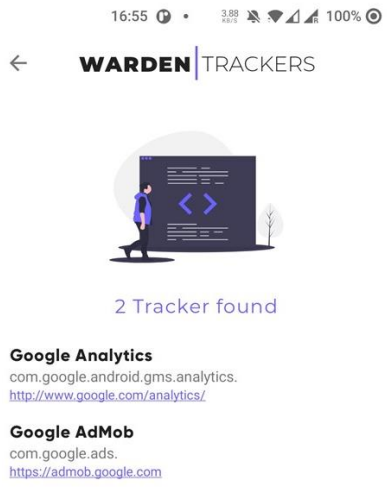
In looking at the Facebook messenger applications, I compared the amount of data that is harvested, transmitted, or tracked for the default applications (on the left below) versus their 'lite' version (on the right below).

The lite versions were developed specifically for developing countries where there is a need for connectivity, but where the price of data transmission is higher. In these countries, targeted advertising is not done to the same degree as the advertising revenue is not generated there.

If you must use an application for Facebook messenger, you will see that the Facebook messenger Lite has much better privacy, compared to the full version. Use this version for better privacy as well as using less data.

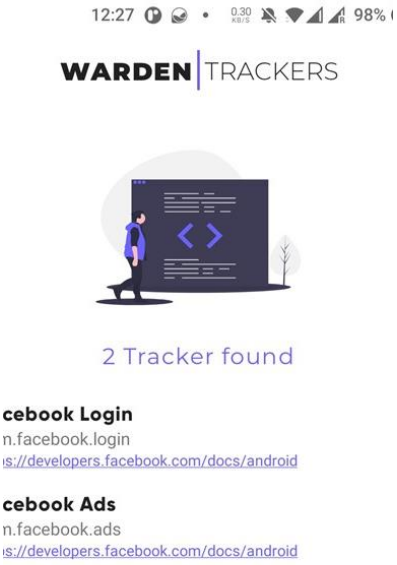


Funnily enough, unlike its Lite Facebook version, this has trackers, but a lot less than the full version!



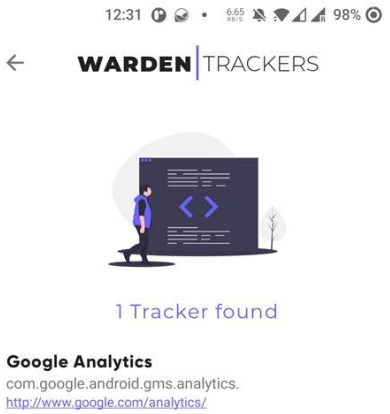
3. Instagram

Instagram as an application, poses a ***large*** privacy risk as it harvests & transmits an awfully large amount of data to Facebook and its companies. Although Instagram only has two trackers built in, it still sends a lot of information back to Facebook.



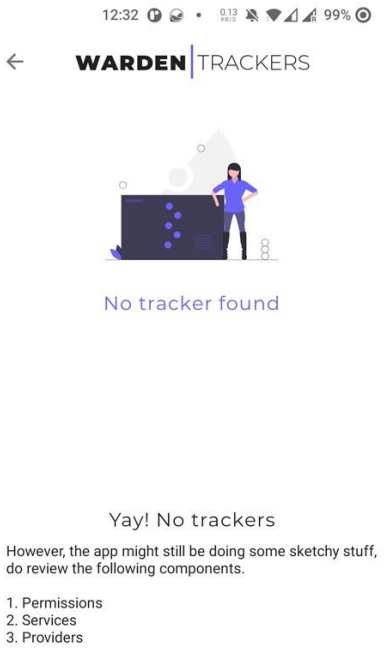
4. WhatsApp Application

WhatsApp DOES provide secure end-to-end encryption for your communication and that is important, however despite WhatsApp saying that it takes your privacy seriously, you can see from the data below, that as an application, it poses a ***large*** privacy risk. It does harvest a large amount of data and the new T&C when agreed, allows this to be transmitted to Facebook to be sold to companies for advertising.



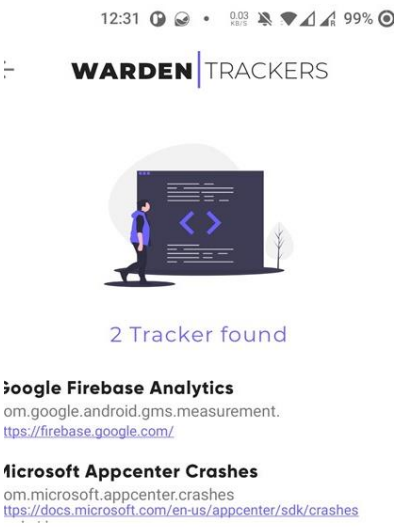
5. Signal Application

Signal was built by the same founders who created WhatsApp and not only does it have the same features as WhatsApp and end-to-end encryption for all messages and calls by default, you will see from the data below, that it takes its privacy seriously. It is inherently safer than WhatsApp!



6. Telegram Application

Telegram collects less information in its use when compared to Signal, HOWEVER, remember chats are not encrypted end-to-end by default and group chat messages are ***not*** encrypted at all! Messages are also stored on the Telegram servers (unless you use personal encrypted messages). When deleting, remember to tick 'Delete for Telegram'



To Summarise

It is clear, that a consumer's reliance in using these popular communication applications, poses a threat ***not*** to the ***security*** of that data, but ***to*** the ***privacy*** of the data. I wanted to provide the detailed information on the amount a data/information that is harvested and then provided to the creators of the application. This allows for an informed decision as to whether to continue to use these apps and the privacy threat created by using them.

When using WhatsApp for example, you automatically give permission to the WhatsApp application to regularly access ***ALL*** the contacts in your phone book and the complete personal details attached for ***every*** contact within (if they too have and Facebook company accounts; Facebook, WhatsApp & Instagram) & the basic personal details of ***all*** other contacts in your phonebook (who do not have Facebook company accounts). This allows Facebook as a company, to drill down and build a bigger picture of you and your contacts personal connections and interests etc.

You also automatically give WhatsApp information on how you are accessing their platform, i.e. what device and software version you are using (and that of all your Facebook group contacts) and where you are accessing their platform (even if you have turned off GPS location services on your device, it will collect information on IP addresses and mobile cell towers to gain an approximate location).

WhatsApp, in their attempt to defend the application in the media, have played on the strength of the application security (end-to-end encrypted calls and messages) but have not been as transparent on the data privacy aspect of the use of the application.

This lack of transparency means that there ***is an unknown risk*** that can easily affect the privacy of personal, company and government data (if it used in a professional capacity, or any contact has a personal account &/or linked to a professional contact with Facebook business accounts).

Facebooks new Terms & Conditions being rolled out across their group platforms various applications, are being challenged by different privacy groups and several Governments. In a nutshell, all the information being harvested by the various applications (including WhatsApp) can be sold for marketing/advertising purposes to ***ANY*** company that Facebook does business with.

How do we, a company, or even more importantly governments and their departments, know ***WHAT*** information is being sold by Facebook, to ***WHO***, ***WHERE*** and ***WHY*** they want to purchase the information (is it for a company to provide advertising to us personally on items of interest to us, or is there a more nefarious unknown intent)??

How do we as a consumer and more importantly, businesses, Governments and their departments ***mitigate the risks*** involved in using secure messaging apps.

I would not recommend using Telegram for businesses or Governments, as individual messages are not encrypted end-to-end by default and group chats have NO encryption at all.

More than that, the risk is higher as messages are stored on the Telegram servers, leaving them vulnerable to interception etc.

In Conclusion

Many applications are accessible online using a web browser and using a mobile web browser would allow you to connect to their services without the collection of all the data. You need to remember however, that the user experience on a mobile browser, may not be as good or as convenient as an app; there is always a compromise in experience, if you want to maintain data privacy… Food for thought!!

The most private messaging application to use currently ***IS Signal***. Signal is the most scalable encryption tool on the market. It is free and being open-sourced, is peer reviewed. It allows users to share without insecurity; saying anything, speaking freely, whether personally or in groups.

No ads. No trackers. No kidding.

Why, you may ask, are more people not using it over WhatsApp, perhaps it is due to the dominance of WhatsApp in many markets across the world due to the length of time it has been available.

I have moved to Signal and I would recommend that you do!

---- Remember ----

"When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else."

David Brin