Council of the European Union
General Secretariat
Digital Services - SMART
The Deputy Director-General

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (09.06.2022)

GSC INTERNAL NOTE
Brussels, 28 January 2021
SMART 21/0021

NOTE FOR DIRECTORS-GENERAL

Copy: DELETED, DELETED, IT correspondents
Subject: **Use of commercial messaging apps**

1. Following requests to SMART for clarification on the use of commercial messaging apps, this note gives background information and guidance for you and your staff on using such apps.

Background

2. Most people are used in their private lives to using apps such as WhatsApp, Signal, Telegram, etc. and are familiar with the functionalities they offer. It is understandable that people naturally also wish to use these functionalities in certain professional situations. Messaging apps are very convenient, but they carry security and privacy risks. In our information-driven environment where GSC staff handle significant quantities of sensitive information, we have a responsibility as civil servants to manage such information in compliance with security and data protection rules.

3. As the provision of such services involve a cost to the operators, they are always looking for new revenue streams so they can continue offering their service at no direct cost for users. Remember the old adage about social media: if there is no cost for using the product, assume that your information is the product.

4. It is very hard to establish the security status and trustworthiness of such apps. The encryption mechanisms they offer are not sufficient to guarantee confidentiality of your conversation and of the files you share (including pictures, videos, links, metadata, see below), as an app may have other flaws allowing information leakage. Also, the encryption used does not protect against potential access by capable state actors. Having said this, encryption provides an initial layer of protection, so make sure any apps you use **support end-to-end encryption**. This is the case with both WhatsApp and Signal.

5. There are also substantial data protection concerns regarding the use of such apps, especially the metadata related to use of the apps (user name / telephone number / email address / device information / location data / address book / chat group names / etc.). You will find further information on two more commonly used apps below.

JL 20-10-AC-76
Tel. +32 (0)2 281 61 94 - david.galloway@consilium.europa.eu

WhatsApp

6. As regards WhatsApp, you should be aware that your user data, any personal data and files you share through WhatsApp will end up in the US or other third countries outside the EEA, this means that it can be accessible by public authorities of those third countries under applicable legislation.

7. You may also have seen press reports about WhatsApp forcing users to agree to sharing information with Facebook if they want to keep using the service. Facebook, which owns WhatsApp, has indicated that European users would not see the same data-sharing changes.

8. It has also stated that WhatsApp does not share European region WhatsApp user data with Facebook for the purpose of Facebook using this data to improve its products or advertisements. The problem is that the terms and conditions that will apply to users in the EEA are still not clear at the moment. European data protection authorities are looking into the issue.

Signal

9. You may be aware that the Commission has advocated the use of Signal as a messaging tool. Signal is operated by a US tax-exempt foundation funded by donations. It offers end-to-end encryption and by default encrypts metadata (unlike WhatsApp) as well as all local files. It supports encrypted group calls. However, it offers fewer features compared to WhatsApp and it is subject to similar security concerns.

10. However, from a privacy perspective Signal is currently less intrusive than WhatsApp: it does not collect user data in the same way as WhatsApp and it only stores your phone number.

Guidance for GSC staff

11. Please note that commercial messaging apps **are not corporate information sharing tools** in the GSC's IT portfolio, i.e. they are not services for which SMART can provide any support, backup or assurance. If you do use any, please consider your privacy carefully.

12. The following guidance on using any messaging app in a professional context is strongly advised for GSC staff:
    - **Only use** messaging apps **for short-lived, ephemeral chat** about public or non-sensitive content; they are **not** to be used for sharing substantive content on sensitive matters;
    - **Make sure** that you know who is a member of any chat group you are in, and that this membership is regularly reviewed;
    - **Respect** the privacy and integrity of individuals at all times, as well as the information provided by them.

    In short, use common sense concerning the content you post in chat messages.

13. As a reminder, for internal communication with GSC colleagues, email (on your laptop/hybrid or your mobile device) is much safer than any messaging app, as the messages are encrypted and do not leave the Council's IT environment, which is well protected. Similarly, chat messages in the Avaya IX Workplace app remain on our servers. Emails sent to the Commission, EEAS and European Parliament are also encrypted.

14. However, emails sent externally (e.g. to the Presidency, member states, or other external partners) are **not** encrypted by default, and are therefore not more secure than using a messaging app.

GALLOWAY David

Digitally signed by GALLOWAY David
Date: 2021.01.29 08:14:20 +01'00'