Where Are Your Online Messages Truly Private?

John Wolfe
Academic Support Engineer
University of Dayton

University *of* Dayton
Center for Cybersecurity & Data Intelligence

OHIO CYBER RANGE INSTITUTE

Overview

Privacy options vary across internet messaging tools, making it difficult to know how to keep your data and communications secure. This paper explains how encryption protocols work to protect your data and reviews the encryption options available in several popular communication services and apps.

About the Author

John Wolfe is an Academic Support Engineer in the University of Dayton's Center for Cybersecurity and Data Intelligence.

University of Dayton
Center for Cybersecurity and Data Intelligence
937-229-1929
udaytoncyber@udayton.edu

Find more tools at **go.udayton.edu/cybersecurity**

Where Are Your Online Messages Truly Private?

John Wolfe
Academic Support Engineer
University of Dayton

Privacy options vary across popular communication services and apps. Here's what you need to know about how to keep your data and communications secure.

What is Encryption?
In the early days of the internet, data was sent over networks with little regard to who saw the contents. In these early days, information was largely non-sensitive academic or novelty data. As internet use increased, computers connected to this worldwide network begin to handle payment networks, banking and medical records, personal communications, and other information not traditionally available publicly. To maintain the integrity of these systems access to this data needed to be limited to authorized parties. This is where encryption came into play.

Encryption in simplest terms works by obfuscating data with a secret key that the intended recipient uses to decrypt the data back to its original form. We can think of encryption like a lockbox: you take your sensitive item, place it in the box, lock it with your key, then you send the box to your friend Bob who has the same key. Nobody can open the box but you and Bob. Encryption that uses the same key to encrypt and decrypt data is called "symmetric encryption."

Another variety is "symmetric encryption," which is particularly useful for internet communication since there's not an easy way to securely exchange a secret key over the internet. In this method, the sender and recipient each have two keys, one public and one secret. To send you a private message, Bob encrypts your message with your public key, at which point even Bob can't decrypt this message - only your secret private key can do so. Likewise, to send a private message back to Bob, you would encrypt your message with Bob's public key, and only his private key could decrypt it.

In this scenario, it's important to know where the keys to your data are stored (and who can access them); anyone with the keys to your data can decrypt it.

How is End-to-End (E2E) Encryption Different?
Most encryption is between your device and the service you are using. After the data arrives at the service they have the keys to decrypt your data. Many large companies, such as Google, Facebook, or Snapchat will encrypt your data while it's stored on their systems, but still hold the keys to decrypt it.

With E2E encryption, the secret keys for your data remain on your own device, not with the service the data passes through. Since the service itself does not hold the decryption keys, your data remains private.

Why Does Encryption Matter?
In the wrong hands, the information about you available through your online data (like medical conditions, payment, and banking information) could be stolen and used by criminals to blackmail or scam you. Also, employees of your online services have the potential to misuse your data; there have been recent cases of Roomba sending pictures of

people's homes and an internal Snapchat tool once allowed employees to see users' private snaps. The services you use could also experience a data breach, in which case non-E2E encrypted data could become compromised and made public.

ENCRYPTION OPTIONS IN POPULAR COMMUNICATION APPS AND SERVICES

Below you'll find information about the privacy and security options in some popular applications that use direct messaging features - in particular, do they offer E2E encryption?

Dating Apps: Bumble, Hinge & Tinder

Parents: Bumble Group, Match Group

Bumble, Hinge and Tinder are popular dating apps used by millions of people. None of these applications offer E2E encryption. Conversations within this app are visible to the parent companies. Even basic security on these apps has been lax in the past, such as in 2018 when Tinder wasn't using basic HTTPS communications within its app, allowing for communication to be intercepted in plain text by bad actors.[1] [2]

Discord

Parent: Discord Inc.

Discord is a popular application for group communication. Users can create and join public and private Discord Servers, consisting of multiple voice and text-based communication channels. Discord channels, both voice and text, are not E2E encrypted and can be accessed by Discord at any time.[3]

Facebook Messenger

Parent: Meta (Facebook)

Facebook Messenger is one of the world's most popular messaging platforms. Messenger is similar to (and, in some cases, integrated with) Instagram Direct Messages. By default, Messenger is not E2E encrypted and, like Instagram, it offers the option to launch an E2E encrypted conversation. This optional E2E encryption only works on Messenger for iOS and Android; the Facebook web interface is not capable of E2E Encryption.[4]

Google Chat

Parent: Alphabet Inc.

Google Chat is Google's primary messaging app. It's available on most platforms and via web browser. Google Chat is not E2E encrypted, but offers E2E encrypted conversations if both parties are using the Android App and Rich Communication Services (RCS) messaging, a successor to SMS not supported on iPhone. E2E encryption is indicated by a lock icon in the conversation. All other messages, such as messages sent through a web browser or non-Android platforms, are not E2E encrypted and can be seen by Google.[5]

GroupMe

Parent: Microsoft

GroupMe is used for group messaging on devices across multiple platforms. GroupMe does not offer E2E encryption. Avoid sharing sensitive information though this application.

---

[1] https://foundation.mozilla.org/en/privacynotincluded/tinder/

[2] https://www.nbcnews.com/tech/security/dating-apps-grindr-could-pose-national-security-risk-experts-warn-n1115321

[3] https://stealthoptional.com/gaming/is-discord-encrypted-2021-how-private-and-secure-is-discord/

[4] https://www.facebook.com/help/messenger-app/78661322198978

[5] https://support.google.com/messages/answer/10262381?hl=en

iMessage
Parent: Apple Inc.
Apple's iMessage is included on every iOS device and Mac since its launch on iOS 5 in 2011. Since its inception, iMessage has been designed with privacy in mind -- iMessage has always been E2E encrypted. When you register a new Apple device with iMessage, a key pair is generated. The public key is sent to Apple so other people can contact you and the private key stays on your device. Messages you send, text or media, are E2E encrypted so that only the recipient can view them. Not even Apple could view your message.[6]

Instagram Direct Messages
Parent: Meta (Facebook)
Instagram Direct Messages let you privately share content with your friends through Instagram. Direct Messages are not E2E Encrypted by default, however Instagram offers a E2E Encrypted chat feature that can be activated when beginning a new conversation. Encrypted messaging is available on Instagram's mobile application only, not its web interface. [7]

Microsoft Teams
Parent: Microsoft
Microsoft Teams is a business application for team collaboration. Teams was not designed with privacy at the forefront. Like most enterprise applications, it's focus is on compliance and IT administration. By default, Teams is not E2E encrypted, however your organization's system administrators can choose to activate E2E encryption for video and audio calls.[8]

Signal
Parent: Signal
Signal, a privacy focused app, is currently the gold standard for E2E encrypted messaging. Signal is an open source product based on its custom Signal Protocol, which is used for E2E encryption in many other chat applications. By default all Signal conversations are E2E encrypted, including group messages, DMs, voice and video. Signal also promises that there are no ads or trackers on its service.[9] [10]

Skype
Parent: Microsoft
Skype was one of the first video chat applications to gain widespread traction. Skype isn't E2E encrypted by default, however it offers a private chat feature that allows users to initiate an E2E encrypted text, video, or audio conversation. Private Chats in Skype use the Signal protocol for E2E encryption.[11]

Slack
Parent: SalesForce
Slack is an enterprise application built for collaboration, compliance, and ease of administration. As such, Slack does not offer E2E encryption options for its services. Slack messages, even DMs and private channels, can be viewed by organization administrators, as well as Slack itself.[12]

SMS & MMS

---

[6] https://support.apple.com/guide/security/imessage-security-overview-secd9764312f/web
[7] https://help.instagram.com/491565145294150
[8] https://learn.microsoft.com/en-us/MicrosoftTeams/teams-end-to-end-encryption
[9] https://signal.org/#signal
[10] https://github.com/signalapp
[11] https://support.skype.com/en/faq/FA34824/what-are-skype-private-conversations?q=end+to+end
[12] https://a.slack-edge.com/964df/marketing/downloads/security/Security_White_Paper_2020.pdf

SMS is a legacy technology and should not be used for any communications that you deem sensitive or secure. Short Messaging Service (SMS) and Multimedia Messaging Service (MMS) have been around since the 1990s. The first SMS message was sent in 1992. At that time, encrypting these short communications wasn't a priority and would have been technologically difficult. SMS & MMS are not encrypted; your phone carrier can see and store any messages you send through these standards. On iPhone, SMS messages appear as green bubbles, compared to iMessage's blue bubbles. On Android, the Messages app sends SMS messages, but you can adjust chat settings to use Google Chat features instead (although, as texts to iPhone users still use SMS, due to Apple's lack of RCS support).

Snapchat
Parent: Snap Inc
Snapchat is a popular mobile application for communicating with friends and family using photos, short videos, and text messages. Snapchat's distinctive feature is its ability limit the amount of time recipients can access images, videos, and texts. When sending a snap, you can specify how long the recipient can view the item. So, naturally, privacy is a primary tenet of the Snapchat experience. Snapchat has implemented E2E encryption on snaps sent as photos or videos. Snaps that appear as red or purple icons have been E2E encrypted and can't be viewed by Snapchat. However, snaps sent as messages, which appear as blue icons, are not E2E encrypted and can be seen by Snapchat.[13]

Telegram
Parent: Telegram
Telegram is a privacy focused messaging apps. Telegram's regular conversations are not E2E encrypted, but it offers a "Secret Chat" with E2E encryption.[14] [15]

TikTok Direct Messages
Parent: ByteDance
TikTok doesn't publish anything about the security of their direct messages, but they are not likely E2E encrypted. There are significant privacy concerns with TikTok; it has close ties with the People's Republic of China, a nation-state with strict surveillance laws. Many states have banned installation of TikTok on state-owned devices.[16] [17]

Twitter Direct Messages
Parent: X Corp.
Twitter Direct Messages (DMs), allows users to send private messages to anyone on the platform. These messages are not E2E encrypted, and can be viewed by Twitter. Elon Musk, the new owner of Twitter, said he was going to investigate the addition of E2E encrypted messages, but (as of this time) they have not yet been implemented. [18]

WhatsApp
Parent: Meta (Facebook)
WhatsApp, an internationally popular messaging application, is fully E2E encrypted by default when chatting with other WhatsApp users. All text, voice, and video chats done through WhatsApp is E2E encrypted. WhatsApp also supports SMS messaging; this method of communication is not E2E Encrypted in the application. While the contents of

[13] https://www.digitalinformationworld.com/2019/01/snapchat-end-to-end-encryption-users-media-messages.html
[14] https://core.telegram.org/techfaq
[15] https://telegram.org/faq#security
[16] https://www.trustedreviews.com/news/is-tiktok-safe-4172063
[17] https://www.yahoo.com/entertainment/can-tiktok-convince-the-us-its-not-a-national-security-threat-173030115.html
[18] https://www.theverge.com/2022/11/21/23472174/twitter-dms-encrypted-elon-musk-voice-video-calling

your WhatsApp chats and can't be seen by Meta, the company heavily track your metadata (usage, timestamps, etc.).[19]

YikYak Direct Messages
Parent: YikYak Inc.
YikYak added a Direct Messaging feature in 2022. The geo-location based, anonymous sharing application allows you to message users without an ID. YikYak doesn't provide much documentation about the platform, and an information request regarding DMs went answered. While we don't know for certain if YikYak messages are E2E encrypted, it's best to assume they aren't and that YikYak can see your communications.

Zoom
Parent: Zoom Video Communications
Zoom rose to prominence during the COVID-19 pandemic. Effective remote work and socialization required video conferencing software and Zoom was there to fill the void. As a primarily enterprise application, Zoom's primary focus is productivity, not. Zoom doesn't employ E2E encryption by default, but includes an option for systems administrators to enable E2E encryption.[20] Zoom also has had multiple allegations of ties to the People's Republic of China.[21]

Conclusion
Clearly, messaging applications have wildly different standards for privacy and data protection. In an ideal world, we'd want to use the applications that keep our data in our own hands. Of the options we reviewed, Signal, iMessage, Telegram, and WhatsApp offer the best privacy and personal data protection measures.

Signal is currently the gold standard for messaging privacy, as their protocol is used widely, even on competing platforms such as Skype, to facilitate E2E encryption. Additionally, Signal is a non-profit organization committed to keeping information private, rather than a for-profit company beholden to business needs and goals that may be at odds with consumer data protections.

If you choose to use applications with less secure data management protocols, be mindful about the content that you're sharing through each platform. For example, it would be unwise to share bank or social security details over Slack, Zoom or GroupMe. A thoughtful approach to the communication tools you use will help keep your data secure.

[19] https://www.whatsapp.com/security/advisories
[20] https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings
[21] https://www.reuters.com/article/us-zoom-video-commn-privacy/u-s-lawmakers-ask-zoom-to-clarify-china-ties-after-it-suspends-accounts-idUSKBN23I3GP