



# RCP-2021

**Recommendation for Communication Platform 2021**






**Prepared by Hassan Khan**

Commenced January 2019

Completed Jan 2021

Email: [contact@hksltd.net](mailto:contact@hksltd.net) || Website: [www.hksltd.net](http://www.hksltd.net)

# Table of Contents

	Page #
	
<b>Opening</b>	
<b>1:</b> Intro	2
<b>2:</b> WhatsApp and your data after Feb/2021	3
<b>3:</b> List of Industry Best	5
<b>4:</b> Recommendations	6
<b>5:</b> Comparison Tables	8
	
<b>Technical Details</b>	
<b>6:</b> Real World Limits for WhatsApp	11
<b>7:</b> Recommendations Illustrated	14
<b>8:</b> Application Architectures	18
<b>9:</b> Fully Rendered Images	23
<b>10:</b> Video Link	35
	
<b>Closing</b>	
<b>11:</b> Closing Remarks	36
<b>12:</b> Source and References used during Research	37

All hypertext links are active and point to their respective locations.

All images are fully rendered in Part 19.

# -PART 1-

## Intro

This research started in 2019 to find a solution for companies operating in CARICOM to communicate daily and maintain their employee's personal barrier while performing their corporate duties with acceptable security in place. The scope was updated due to global influences and now includes the above and paid for applications.

There is an unsettling trend of businesses and government entities using WhatsApp as their daily communication tool when it was never fully developed for that purpose. WhatsApp was easy to use and employers and employees became increasingly complacent in allowing this application's prevalence in the work environment. The application's architecture should be scrutinized further in 2021, and the reader should seek a more "tailored designed" application with better data and user management including security built in.

WhatsApp and other similar **Mobile-number Centric Messaging Applications (MCMAs)** were designed for social groups and connectivity of friends/ family and scalable on a small group dynamic. They are primarily free, which in most cases the owner of the application shares/ sells the meta data to increase funding to continue the application's development. This is unacceptable for high level businesses and government use.

I hope this document explains the pros and cons of WhatsApp and leaves the reader understanding more about MCMAs and their use when compared to ERPs and other tailored (paid for) messaging applications. However, when sales revenue, security needs and complexity increase for government needs, WhatsApp is a far cry from a recommended and safe platform to use.

*Security analysis and investigative processes to gather intelligence (signals) from user devices will not be listed in this document as that information can be used to further mask any nefarious operations the reader may bare. That information will be given voluntarily once my concerns are negated and due diligence is satisfied.*

## -PART 2-

### WhatsApp and your data after February 2021

WhatsApp does not offer industry standard features as seen in other enterprise applications, such as auditing, media storage options, mass broadcast (one-way communication), and protection of the user's information. I created a YouTube video to explain this and the scannable QR code is at the end of this document. WhatsApp does offer robust encryption developed for user-to-user, but due to WhatsApp's meteoric rise in the messaging application domain, many simply ignored their reservations of using their own mobile numbers to usher in this more accepted communication platform by "ease of use" and market share. **WhatsApp uses the same encryption as Signal, but unlike Signal it allows more meta data to be leaked into their servers for monetization via Facebook.**

Operational Security is a field of thought that has been overlooked and my goal is to offer OPSEC framework and methodology to help government and professionals alike to secure their information.

**Operations security (OPSEC)** is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if that information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

My use of Operational Security for this purpose is *"internal actions being observed by outside parties and acted on"*.

OPSEC helps to identify why having a purpose-built platform and application can be not only secure, but highly efficient when needing to scale and handle complex layers of a team's or company's communication channels. It also provides auditing and accountability for matters not yet perceived inclusive of integration with other ERPs for seamless workflows and tracking user data sent, and only visible if needed.

Currently many CARICOM businesses and peer groups use WhatsApp as their primary messaging and media sharing platform for day-to-day operation, this includes doctors and lawyers. WhatsApp is a private and personal messaging platform that was never designed for businesses and governments to share critical data, and Facebook owns WhatsApp and has started adding features that are useful for personal users such as Stories and Statuses which have no real-world application for high level uses.

## -PART 2-

### WhatsApp and your data after February 2021

#### (Continued)

As I said there are cases where some businesses can use WhatsApp throughout their entire operation with no lost value, and then there are governments and large companies that need a better solution than WhatsApp.

Since WhatsApp authenticates users by mobile numbers alone, it is not well suited for separating work and personal lives. Lead generation and complex team management are also not well represented with-in WhatsApp's architecture when compared to established Enterprise Resource Planning applications (ERPs). Small businesses and sole traders alike can benefit from the free platform WhatsApp provides but cannot scale holistically unless pairing with other applications.

When medium to large businesses, government, healthcare, or complex team organization is needed, the limits of WhatsApp are too obvious and cumbersome to allow its further use, and nothing has been mentioned of audits or security at this point.

- I recommend Signal as a free solution for any company or government entity.
- I recommend MS Teams, Slack or Threema as a paid solution for any company or government entity.
- I recommend Signal over Telegram over WhatsApp for general everyday use.  
*(using telegram secret chats function)*

Telegram has a "hide contact" feature which WhatsApp and Signal do not offer, and that is why I recommend it for light business to customer use to lower the chance of the employee number being shared unwillingly, however, a full table listing a comparison chart of the three messaging applications is available on page:

I have reviewed many platforms/ services from various suppliers and there are several that classify by two groups: paid and non-paid, but all were subjected to the same criteria of testing "to find an alternative that had 95% of Whats App's feature set but allows for better business and secure data use". I ended with 5 different messaging application; [MS Teams](#), [SLACK](#), [Telegram](#), [Signal](#) and [Threema Work](#). *(not in any specific order)*.

## -PART 3-

### List of Industry Best

#### A list of industry bests as of April/2020

- Most secure: Signal (Global)
- Most downloaded: Whats App (Western Hemisphere)
- Most Active users: Facebook Messenger (USA)
- Most cross-platform: Telegram (Central and Eastern Hemisphere)
- Most used service for users <25 yrs. of age: Instagram (Western Hemisphere)
- Most used service for users <35 yrs. of age: Facebook Messenger and Whats App (USA)
- Most used service East of Greenwich Mean Time: WeChat, Telegram, Weibo
- Most used service West of Greenwich Mean Time: Whats App, Facebook Messenger, Instagram, Twitter, Kik
- Top 3 most used Social Media Platforms: Facebook (2.3B), YouTube (2B) and Instagram (1B)

Information sourced via [SLANT](#)

There is no single best option for messaging and each service on a specific platform has pros and cons towards its demographic and its requirements for personal, business and government use.

## -PART 4-

### Recommendations

*I have based the options presented below from >22 months of work and subscriptions purchased, and applications tested in the real world. The listed options below are alternatives to WhatsApp and account for any unforeseen restrictions/ updates at time of writing this document.*

Current model of communication for most parties is to operate WhatsApp due to its market share and its user ability in conjunction with Facebook Messenger. These applications, (WA and FB) cannot scale adequately for projects that require clear communication, auditing, security of data, and file history indexing. WhatsApp is privy to meta data of the conversations on its platform, and WhatsApp Business was tested and offers nothing more in the way of better data and audit policies needed from its sister application, general WhatsApp, other than better management of chats by use of labels.

#### **Option 1 – PAID and not Microsoft centric for companies and government use.**

Based on my testing, SLACK and Threema are the better options for all parties and maintain the ability to bring outside users onto the platform for communication when needed. All the features listed in WhatsApp are available in both the applications and more. Signal can be used for personal communication and the paid for application can be used for work and government needs. Please review their respected websites and what they offer in the way of team management, auditing, and security. They both offer an extensive feature set built around document management digitally, which complements projects with heavy use of photos as “documented forms” such as healthcare and service-based entities. [SLACK \(USA\)](#), [Threema](#)

#### **Option 2 – FREE and not Microsoft centric for companies and government use.**

If there is no option to move to a paid for application at this time, then the only recommendation I can provide is to use Signal. Signal will store all the media shared between users on the device. It is best to set encryption on the device and the memory card to ensure if the physical device is stolen, the data is not accessible. Purchase large storage removable memory cards to supplement the limited storage of a mobile device. My only concern is confidentiality as proprietary data is stored pertaining to a corporate or government entity should not be left for anyone to use other than the intended user. This is a possible vulnerability and Operational Security should not be taken lightly. Encrypt all media to ensure security.

## -PART 4-

### Recommendations (Continued)

**Option 3 – FREE and PAID in conjunction with MS Teams for all parties.**

Most medium to large business and government entities have access to Office 365 and as such should use MS Teams for their internal communication.

Signal in conjunction with MS Teams (Microsoft) is the best solution currently.

When needing to send files and images/video over a messenger application that is not MS Teams, Signal is the next best thing currently. There are more secure applications, but they are cumbersome given their heightened security protocols.

Using Microsoft for productivity, calendar, email, teams, video chat and more is beneficial since most large entities have a Office 365 account in place. This will cover all the necessary security needs of virtually all parties and when communicating with customers or friends and family, Signal will be used.

All the recommendations above are illustrated from page 15.



# -PART 5-

## Comparison Table

<b>Table 1.1</b>	<b>Whats App</b>	<b>Telegram</b>	<b>Signal</b>
Back Up	Device + Google Drive	Device + Cloud Based	Device
Block User(s)	yes	yes	yes
Broadcast(s)	yes	yes	no
One Way Communication Broadcast(s)	no	yes	no
Send Files	<160MB	<1.5GB	<200MB
Delivery Receipt	First check means sent	1st check means sent	First check means sent
	2nd check means the message been delivered	2nd check means read	2nd check means the message been delivered
	blue checks mean message has been read	(one less step than Whats App)	both circles filled in message has been read
Desktop Client	yes	yes	yes
Web Client	yes	yes	no
Format Text	yes	yes	no
Group Chat	yes	yes	yes
Group Chat Limits	256 participants	5000 participants	150 participants
Hold to Talk (Voice Note)	yes	yes	yes
Multi-Device	Only one device at a time, plus access on desktop	yes	Only one device at a time, plus access on desktop
Device Limits?	telephone number centric	telephone number centric	only on GSM devices
Online Status	yes	yes	yes
Phone Calls (VoIP)	yes	yes	yes
Platforms	iOS, Android, Windows Phone, Blackberry, Symbian	iOS, Android, Windows OS, OS X, Blackberry, Symbian, Windows Phone, Linux	iOS, Android, Windows Phone, OS X, Linus

## -PART 5-

### Comparison Table (Continued)

<b>Table 1.2</b>	<b>Whats App</b>	<b>Telegram</b>	<b>Signal</b>
Number of Platforms	6	8	6
Photo Editor (in app)	no	yes	no
Price	Free	Free	Free
Registration Type	Phone Number	Phone number and Email	Phone Number
Can hide mobile number	no	yes	no
Screen Shots	yes	yes, in general chats, no in secrete chat	no
Screen Sharing	no	no	no
Share Contact	yes	yes	no
User Base (April 2020)	2 Billion	350 Million	1.2 Million (estimated)
User Base (January 2021)	1.5 Billion	525 Million	525 million (estimated)
Video Calls	yes	no	yes

## -PART 5-

### Comparison Table (Continued)

<b>Table 1.3</b>	<b>Whats App</b>	<b>Telegram</b>	<b>Signal</b>
Encryption	Signal Foundation (Open Whisper Systems) (US) With clear back-end access to user data. Meta Data	MTPROTO	Open-Source Signal Foundation (Open Whisper Systems) (US)
Security keys	Company holds the keys	Company holds the keys	User holds the keys
What is collected by parent company during normal operation of application	Device ID, User ID, Advertising Data, Purchase History, Coarse Location, Contacts, Email, Telephone, Product Information, Crash Data, Performance Data, "other Diagnostic Data", Payment Info, Customer Support, IP Address, Browser Links, App Version, Operating System Version, URL meta data	Contacts, Telephone Number, Email, User ID	Contacts, Telephone Number, User ID

## -PART 6-

### Real World Limits for WhatsApp

#### **Data Protection Concerns:**

- 1) Fact: Though WhatsApp uses end-to-end encryption, it was ranked almost last by the [Electronic Frontier Foundation](#) when it came to data privacy.
- 2) Consequence: WhatsApp is connected to employee/ customer phone numbers and can access contact lists allowing it (Facebook) to create a complex relationship map. Chats which might contain confidential customer data are also under the . Their device with the app is listed as personal and cannot be wiped remotely if compromised. This puts your company at risk for outside interference. The media shared on Whats App is stored on the device and/or Google Drive of the user.

#### **New Whats App Policy Feb/2021:**

- 1) WhatsApp recently posted their newest policy regarding data sharing and Facebook which has been met with global push back from the user base. It is recommended to remove all critical communication from the platform immediately and use it only for light conversation and inter-personal matters.
- 2) All devices that have WhatsApp installed should delete the application and move the data on the device to secure it better.

#### **Lacking audit features:**

- 1) Fact: German automotive company Continental AG [banned WhatsApp from an estimated 36,000 company devices in](#) June 2018 after information security concerns were repeatedly raised in the courts and by data protection authorities.
- 2) Consequence: WhatsApp has no audit log feature, meaning there is no way to track and record documents, images, and videos sent via the app. The lack of an audit log makes it difficult for you (employer) to foster user accountability, detect intrusions, or reconstruct events to remediate a security/ disputed problem.

## -PART 6-

### Real World Limits for WhatsApp (Continued)

#### Limited admin controls:

- 1) Fact 1: WhatsApp only allows you to control who can send messages to a group chat and change group description, icon, and details.
- 2) Consequence: With unclear company-wide communication policies and complex user management with no access control features in place makes WhatsApp susceptible to misuse to steal information by employees no longer a part of the organization if they go unnoticed.
- 3) Fact 2: WhatsApp cannot have any other user control a group if that user does not already have admin privileges.
- 4) Consequence: If the sole admin in charge of that group is no longer active then there is nothing that can be done in way of adding new members and the data in the group cannot be migrated to another.

#### May cause higher employee turnover:

- 1) Fact: A study by the [Chartered Institute of Personnel and Development](#) surveyed practitioners on the use of WhatsApp at work: 40% said the app undermined corporate culture.
- 2) Consequence: WhatsApp is a great tool to communicate with friends and family, but successful workplace environment requires a level of professionalism, especially during business-related communications. You cannot supervise communications within the app, anyone can privately message anyone, create unauthorized sub-groups that breach policies, or use the app as a tool for bullying/ harassment, prompting targeted employees to leave the company or retaliate in an undesired manner.

## -PART 6-

### Real World Limits for WhatsApp (Continued)

#### **May cause inefficient communication and reduce productivity:**

- 1) Fact: Inefficient communication channels lead to decreased effectiveness when applying changes to policy or services. WhatsApp offers a clear single line thread for communication, but couple that with various projects or subjects for a team of 5+ to manage, and the platform becomes a hinderance. A work around is to have one employee dedicated 24/7 monitoring WhatsApp and alerting other team members, acting as a “administrative aid”. This is an expensive work-around for a problem that can be fixed by using a different platform for team management/ communication.
- 2) Consequence: WhatsApp group chats only allow for 250 users at a time and do not allow you to create threaded chats to structure your communication, causing you to create multiple side groups for different aspects of a project, each with different members maybe. An increasing number of groups and messages makes it difficult to keep track of details, progress, and updates. Unstructured communication also results in missed deadlines, incorrect work, and unhappy clients, and leads to employee frustration.

#### **May cause employee apprehension to raise:**

- 1) Fact: Employees use WhatsApp already for personal engagement which the service was already built for. Personal touches such as display picture and stories added are for the consumption of that users’ personal peers.
- 2) Consequence: When employees must use it for business, they find it difficult to express themselves freely because their information is no longer seen by their chosen peers, but by the work environment also. The employee can choose to not share certain details such as display picture, when last seen or status, but then they are now also limited in what they can express to their personal peer groups and family. Separating Work from personal is important to the employee’s ability to perform better and increase their comfort levels.

## -PART 7-

### Recommendations Illustrated

**Note:**

Using MS teams internally will boost the tracking of subjects discussed, increase coordination and management, and reduce the data storage needs of devices since MS Teams stores on their cloud (Azure) primarily, and on device when needed.

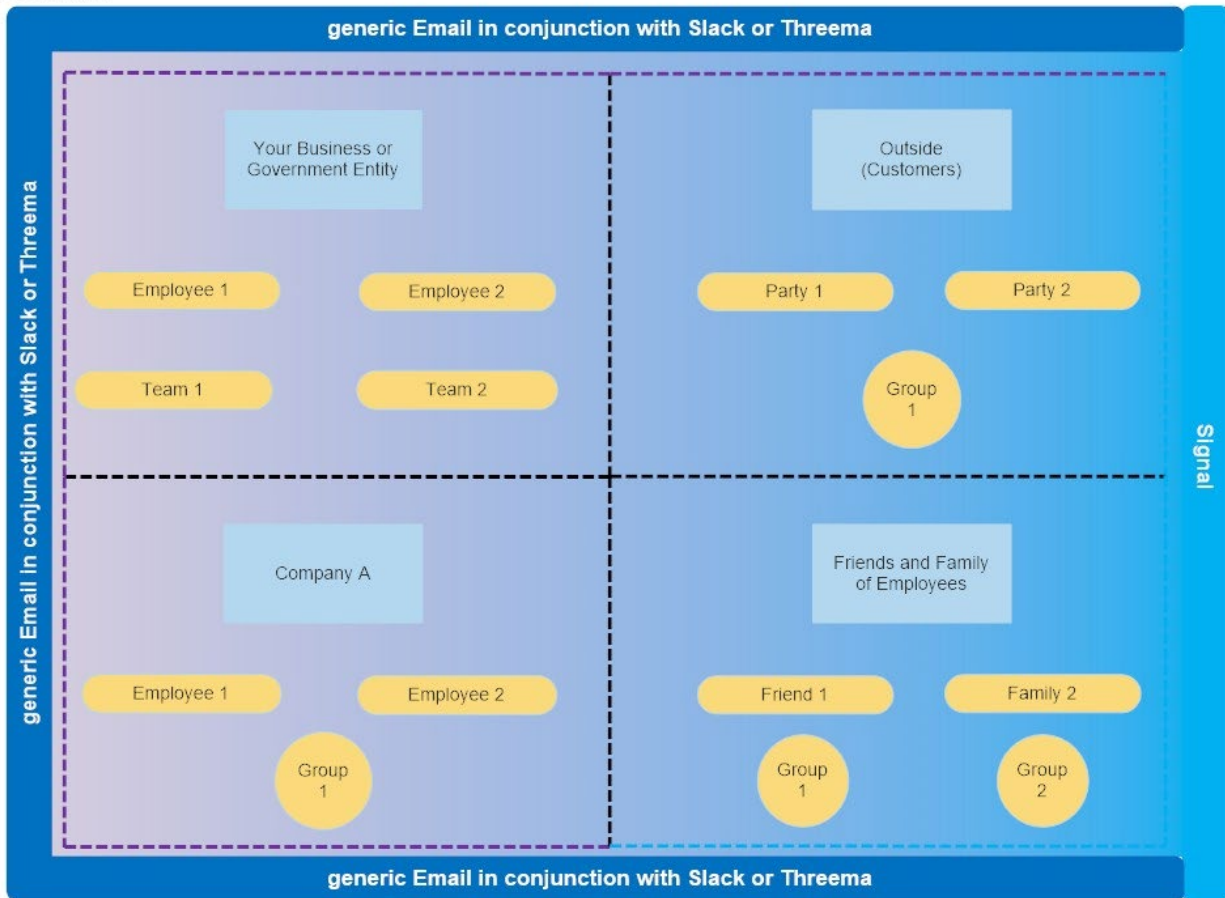
Many businesses have not addressed the growing social changes associated with free speech and movements online to help bring to light other's plights. Having a separate communication application leaves the employee to freely express their personal views of global matters and not include their work relationships directly. They can use other applications outside of the work model.

The options illustrated are not fully detailed because the user will have different needs for specific aspect of the model.

# -PART 7-

## Recommendation 1 Illustrated

### Option 1



[Full page render on](#)

### **Option 1 – PAID and not Microsoft centric for companies and government use:**

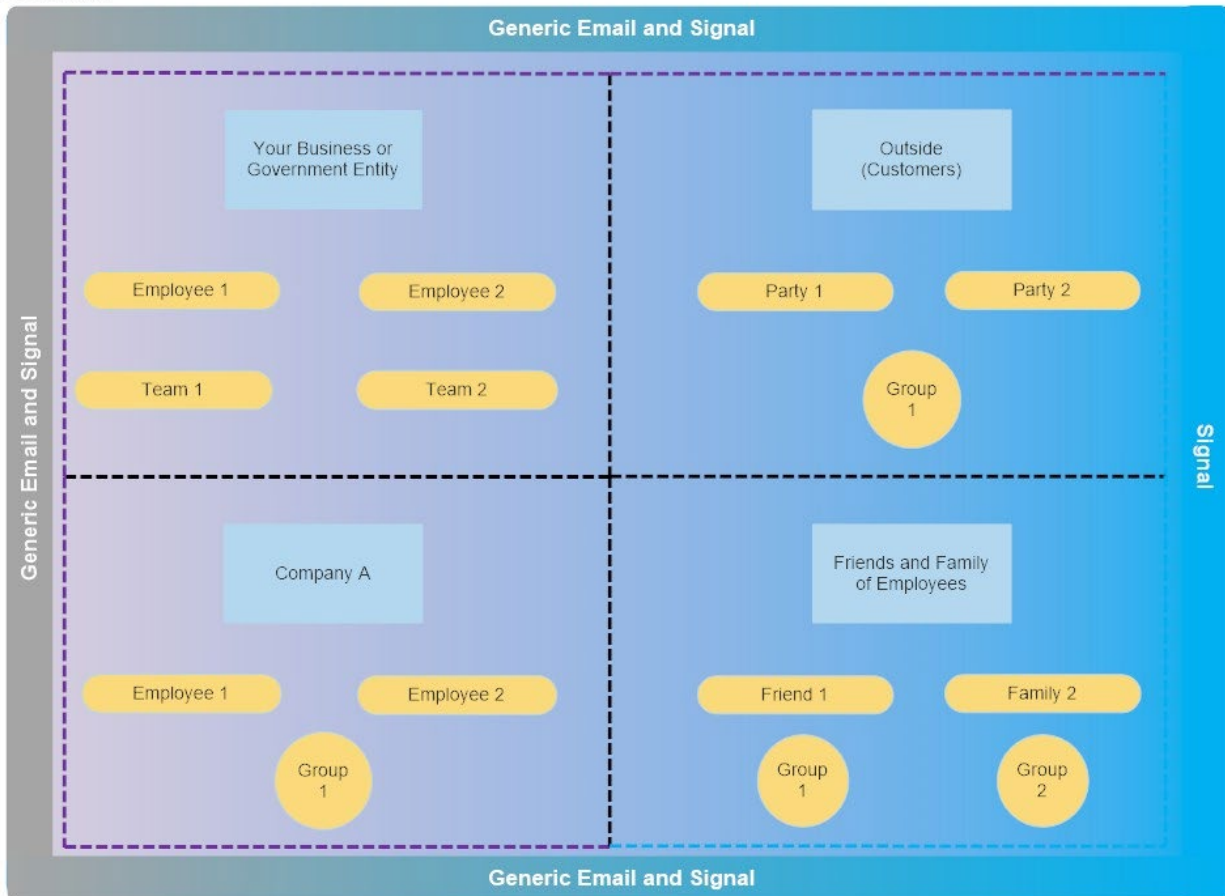
As seen above a generic Email client and one of the two paid for applications, Slack or Threema, can be used for inter-company communications and customer relations, with Signal moving into a personal use.



# -PART 7-

## Recommendation 2 Illustrated

### Option 2



[Full page render on](#)

### **Option 2 – FREE and not Microsoft centric for companies and government use:**

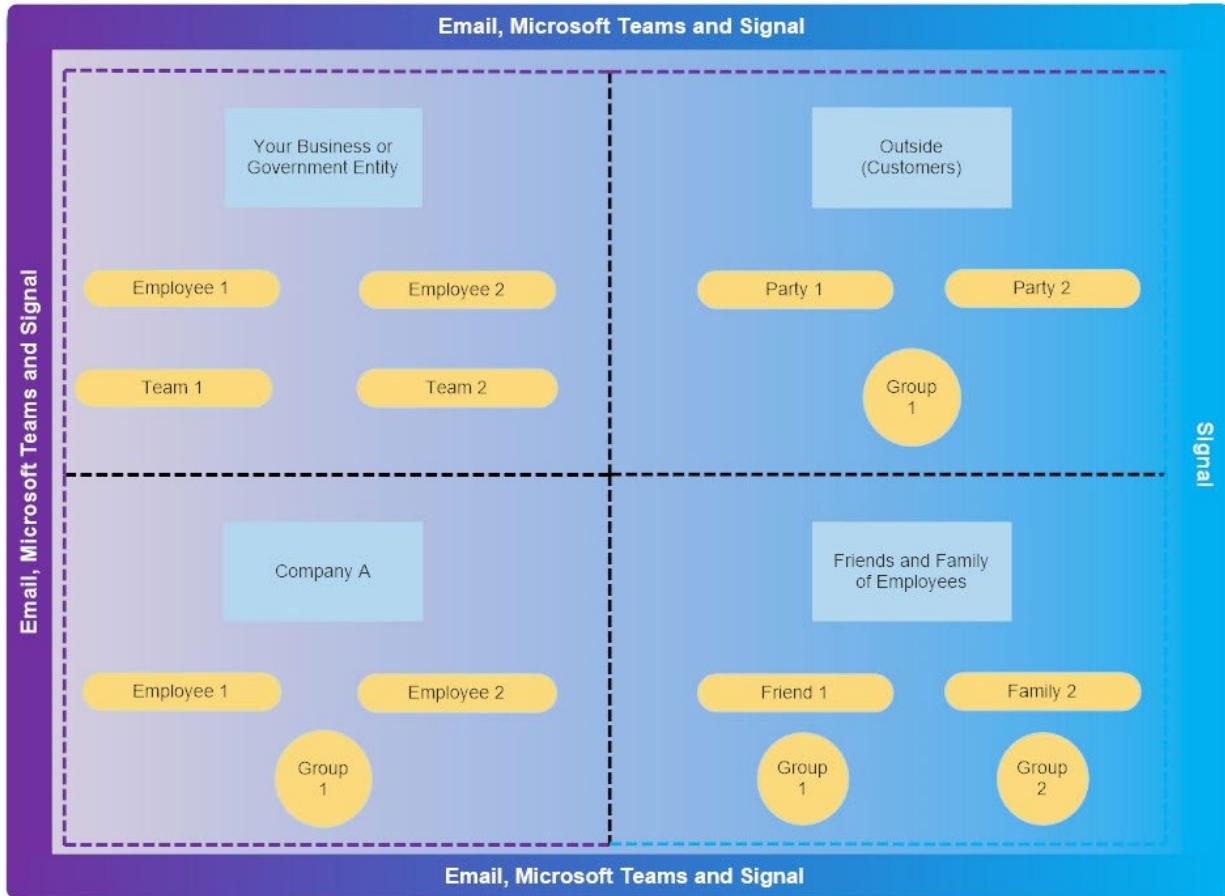
As seen above a generic Email client and Signal can be used for all communications provided the device is encrypted. This is the completely “free” option.

Government and healthcare may also use this model if needed, but the data management framework does not exist as it will in Option 3. OpSec is a major concern, but Signal does help in place of WhatsApp.

# -PART 7-

## Recommendation 3 Illustrated

### Option 3



[Full page render on](#)

### **Option 3 – FREE and PAID in conjunction with Microsoft for all parties.**

As seen above Email and Signal can be used for inter-company communications and customer relations, and Signal can also be used for personal needs as seen on the bottom right of the image. Internal communication and data/user management can be easily provided via MS Teams from Microsoft.

There can be clear policies implemented and storage is both cloud and device. Microsoft has a good track record providing solutions for all types of business and government needs, and virtually all companies and government bodies today already use a Microsoft suit for their productivity, and they can have it further configured to meet the needs listed. Slack and Threema can be brought into the model to replace MS Teams but is not recommended unless your situation demands it.

# -PART 8-

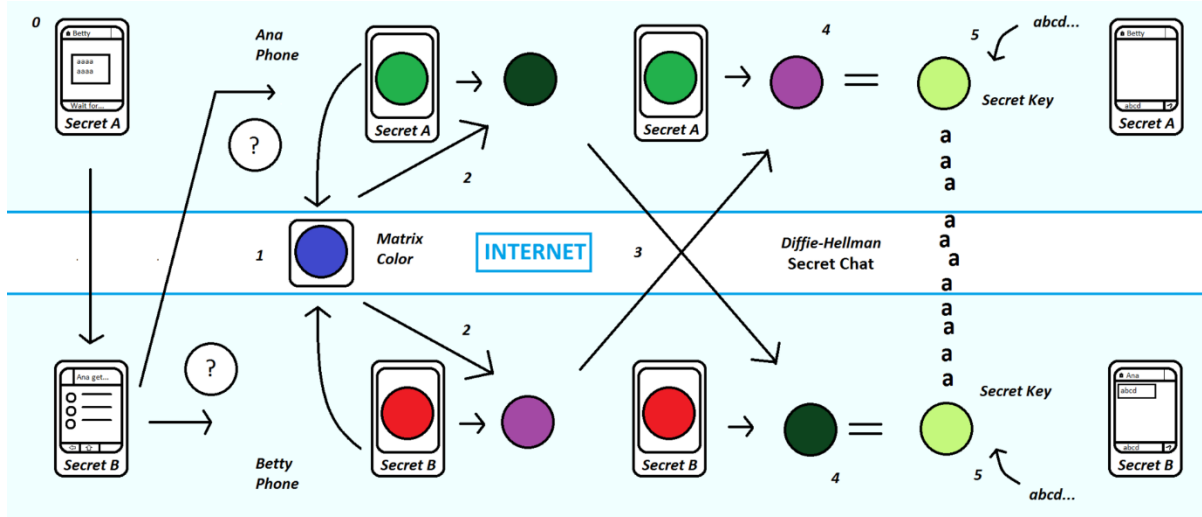
## Application Architecture

### Telegram

- a) General chats are [client -> server] to [server -> client] encrypted
- b) Secret chats are [client-> client] encrypted
- c) Cloud storage of media is encrypted in multiple locations by Telegram, but is stored on the device also

Telegram stores all the user's data on its cloud which is met with industry standard encryption and it is noted that it does not fully comply with presenting data to law enforcement or under court order. The data stored in its cloud service for your chats has the added effect of not worrying about accessing any files sent previously. On Whats App if you send a picture and the sender deletes it or move to another device, then you cannot retrieve it fully, but on Telegram, it is stored until deleted.

*Full renders of images later in document*



## -PART 8-

### Application Architecture (Continued)

#### Telegram

##### Encryption Scheme:

Telegram uses a symmetric encryption scheme called MTProto. The protocol was developed by Nikolai Durov and other developers at Telegram and is based on 256-bit symmetric AES encryption, 2048-bit RSA encryption and Diffie–Hellman key exchange.

##### Servers

Telegram Messenger LLP has servers in several countries throughout the world to improve the response time of their service. Telegram's server-side software is closed-source and proprietary. Pavel Durov has said that it would require a major architectural redesign of the server-side software to connect independent servers to the Telegram cloud.

# -PART 8-

## Application Architecture (Continued)

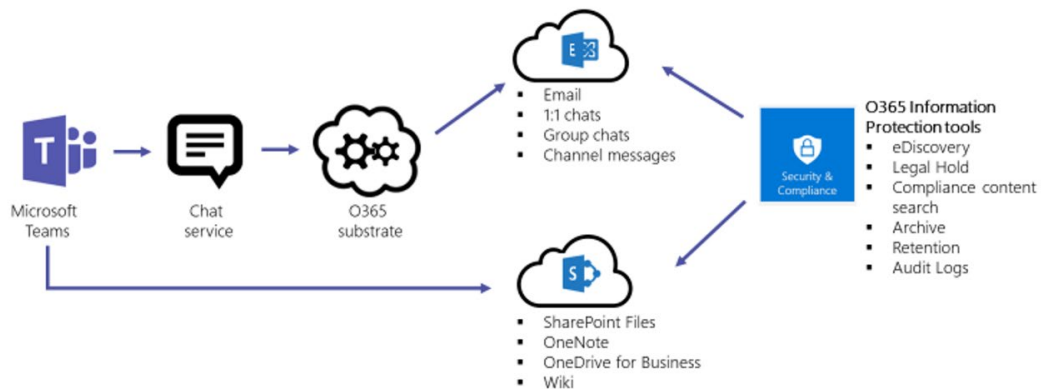
### MS Teams

MS Teams has done a wonderful job of bringing the logical architecture of productivity services in Microsoft 365 - including data governance, security, and compliance capabilities, all into a seamless mesh of services and applications. Below provides a view into the logical architecture of productivity services for enterprise architects and general users.

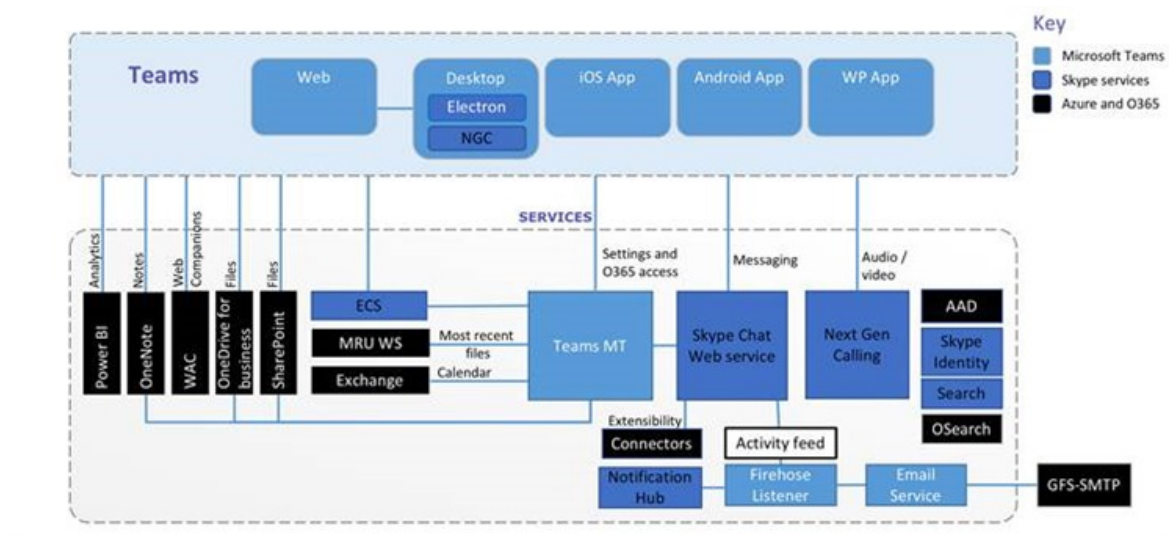
[MS Teams architecture further detailed](#)

## Information Protection Architecture

Chat data and channel messages are journaled to Exchange storage (known as the Office 365 Substrate) to enable integrated management tools for information protection that work across all Office 365 workloads, including Microsoft Teams.



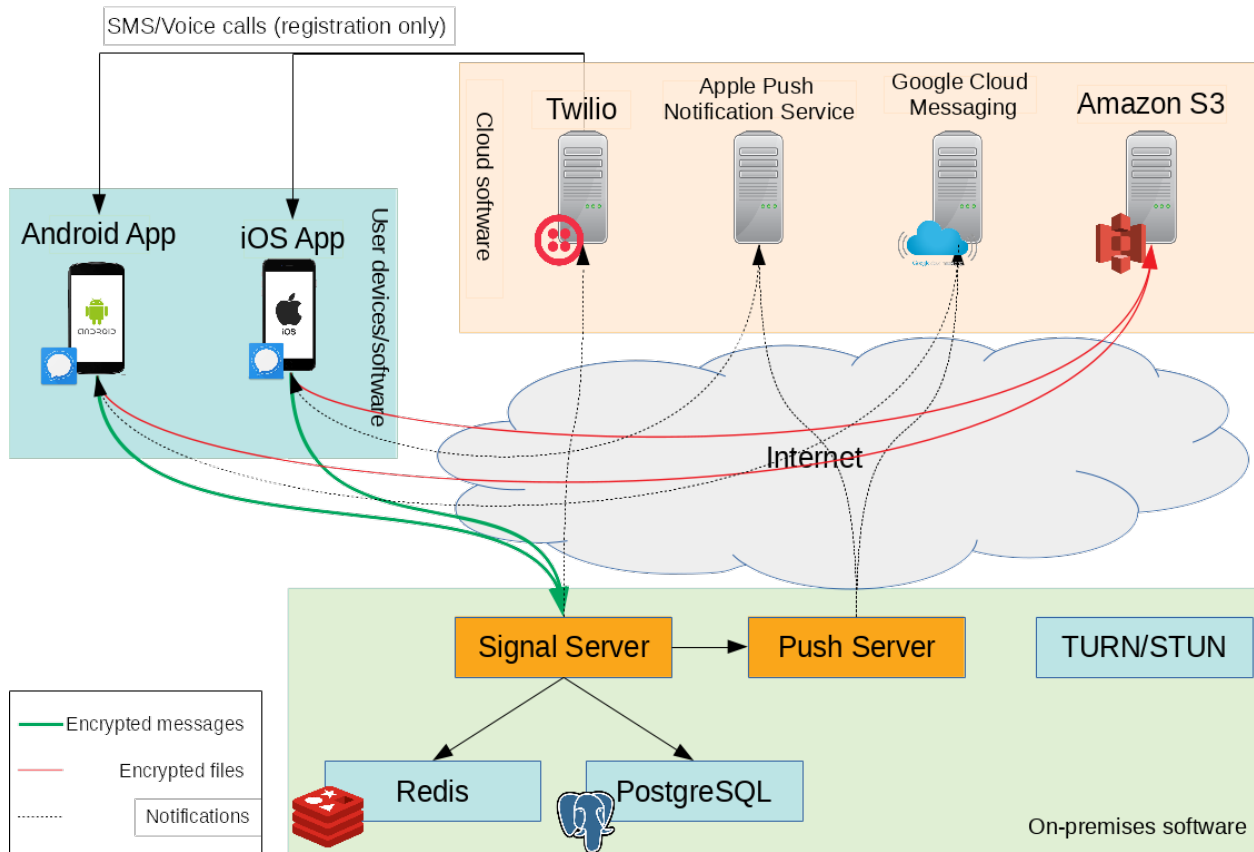
Microsoft Teams



# -PART 8-

## Application Architecture (Continued)

### Signal



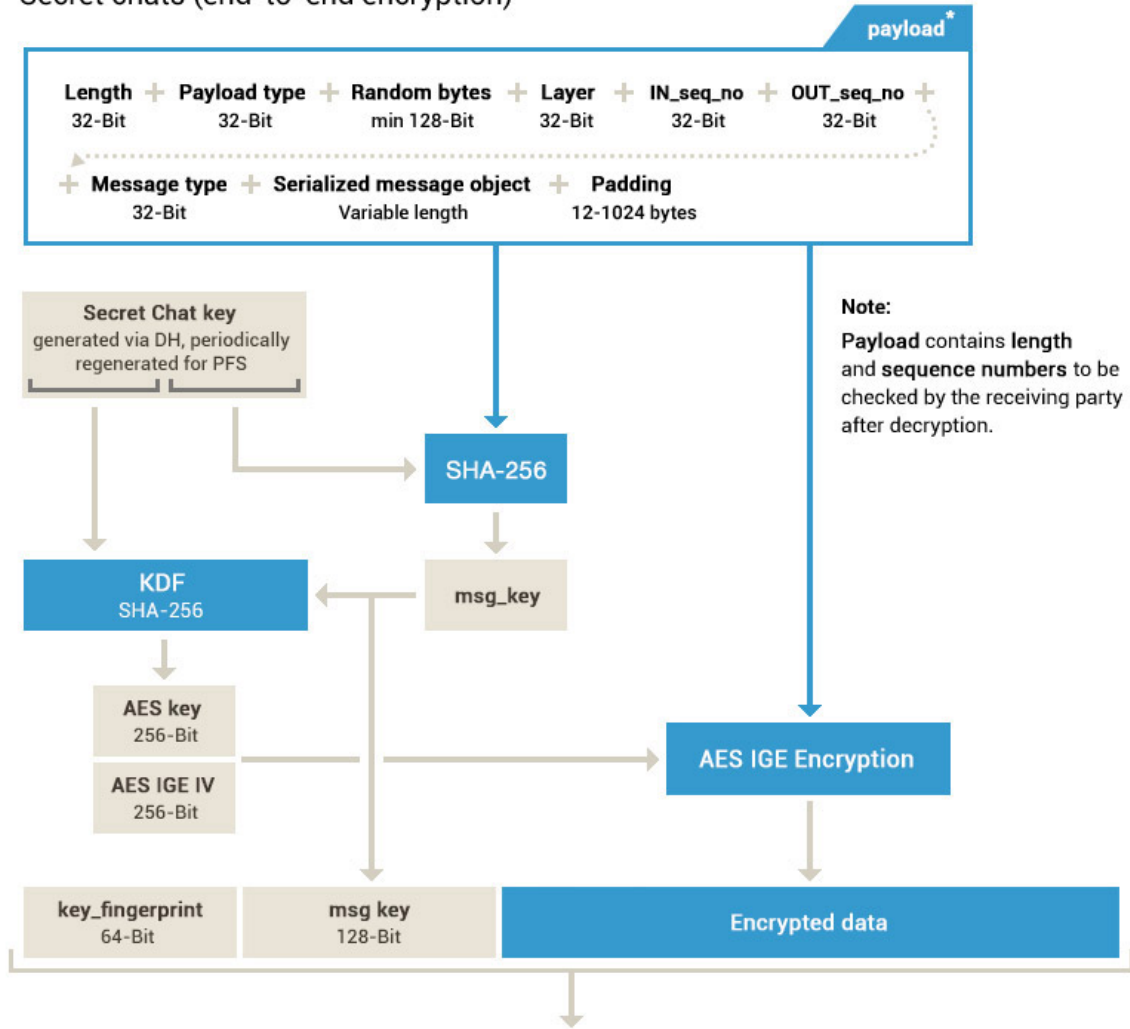
# -PART 8-

## Application Architecture (Continued)

### Signal

#### MTProto 2.0, part II

Secret chats (end-to-end encryption)



embedded into an outer layer of client-server (cloud) MTProto encryption, then into the transport protocol (TCP, HTTP, ..)

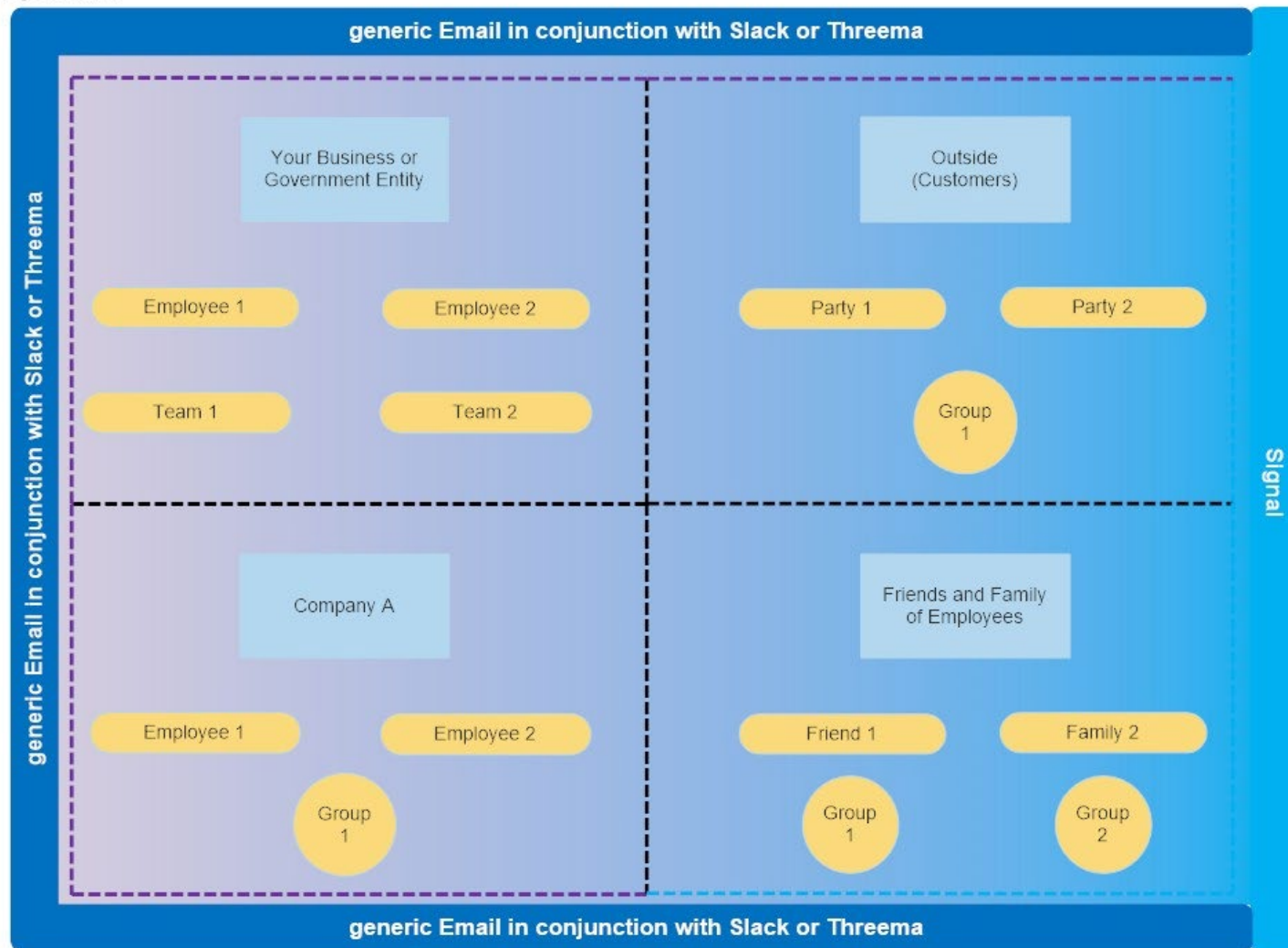
**Important:** After decryption, the receiver **must** check that  $\text{msg\_key} = \text{SHA-256}(\text{fragment of the secret chat key} + \text{decrypted data})$



# -PART 9-

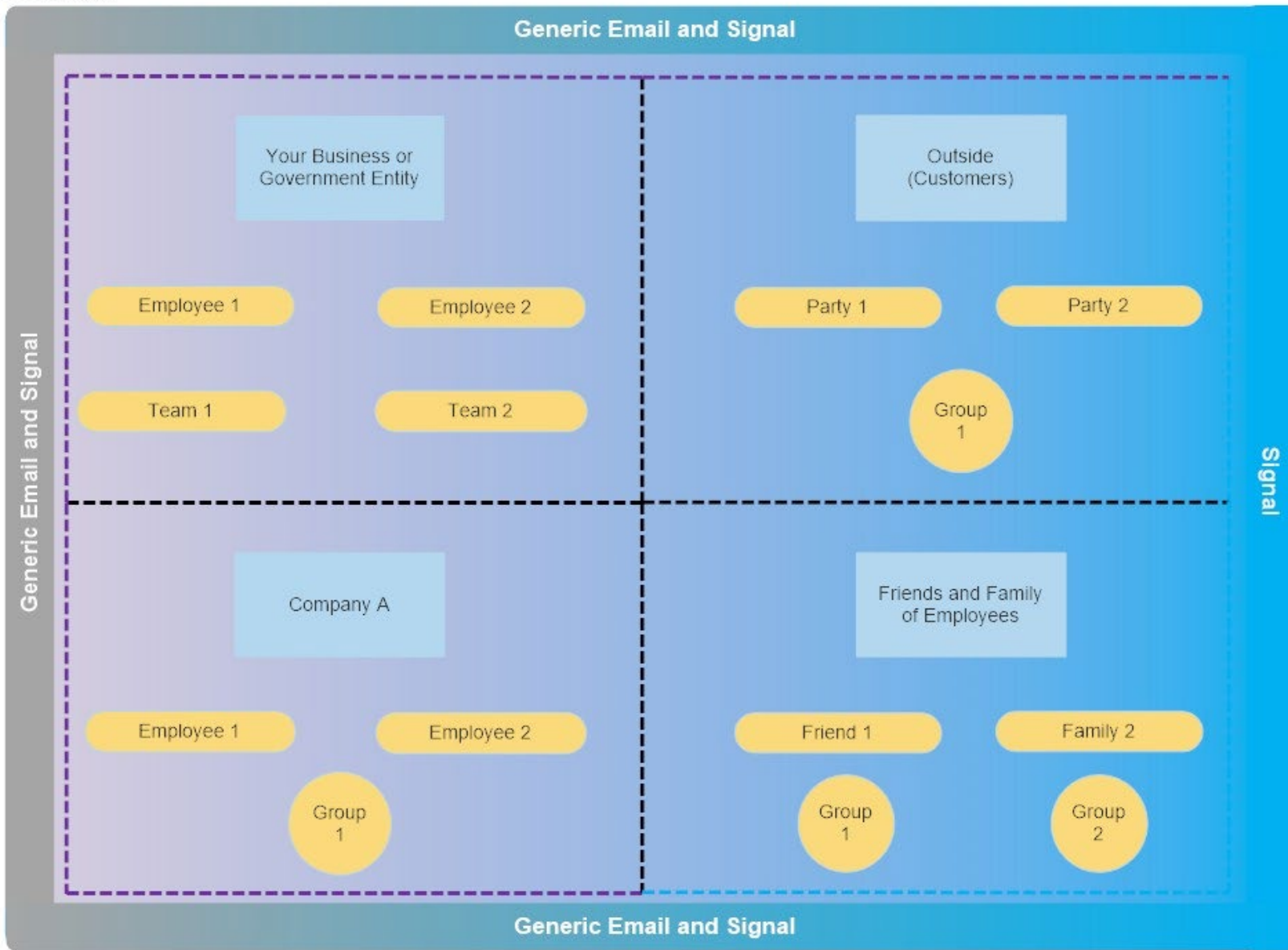
## Fully Rendered Images

Option 1

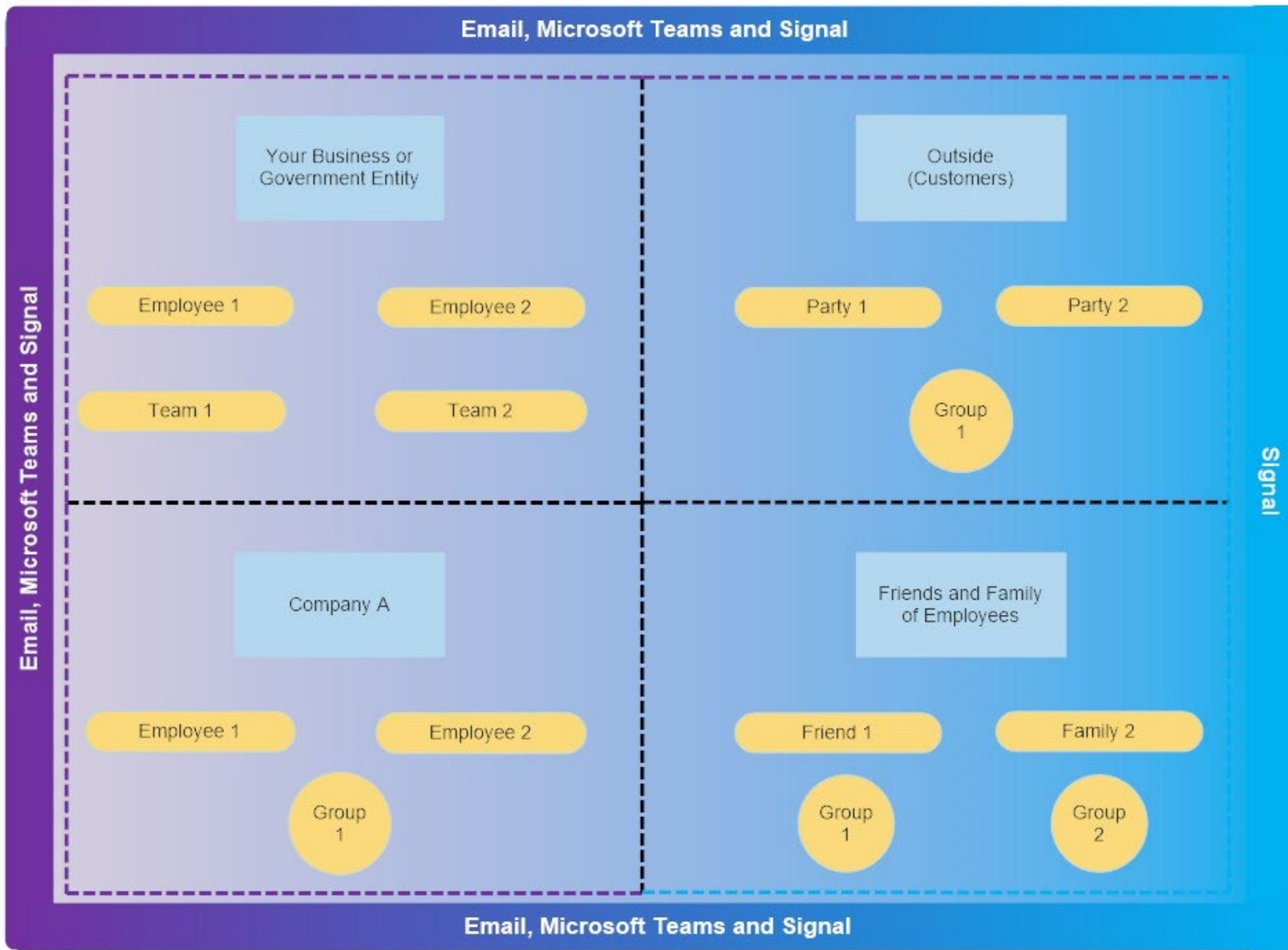


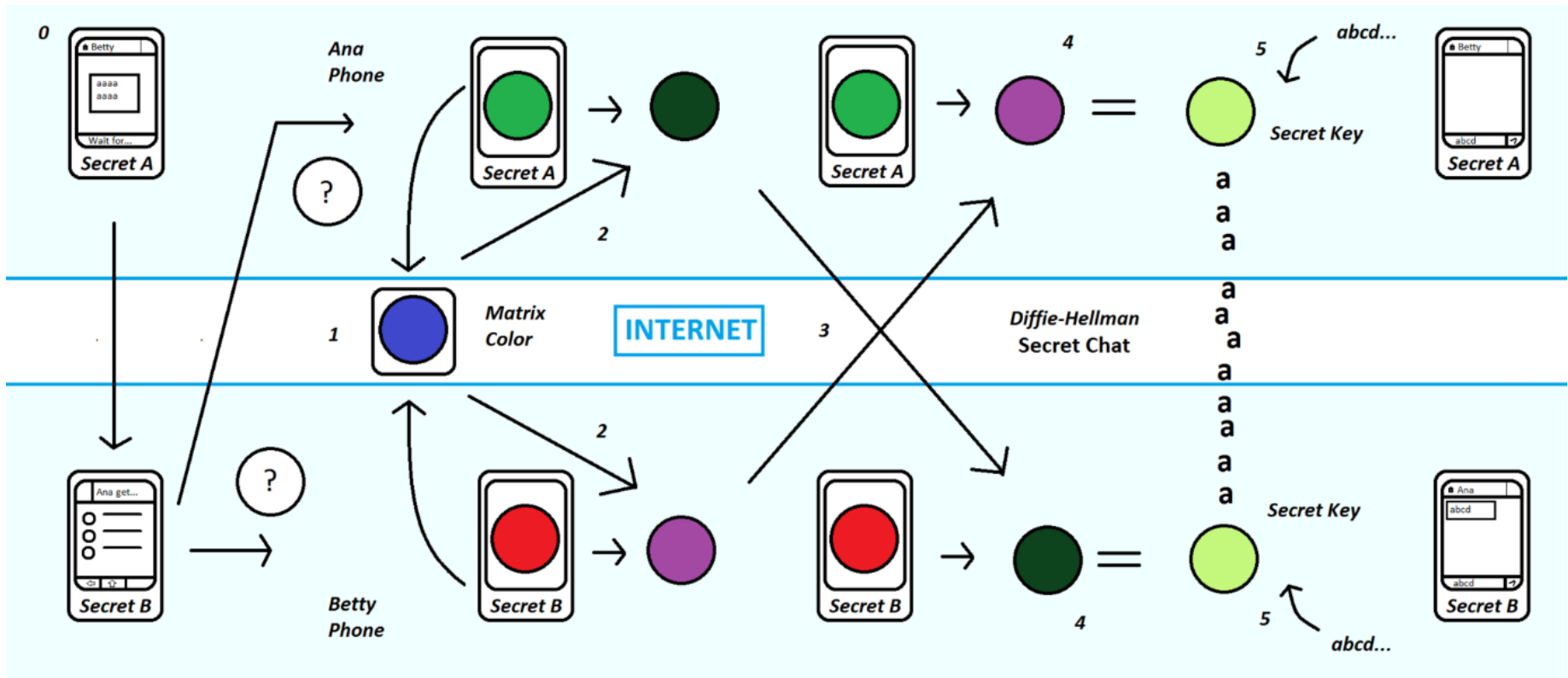


## Option 2



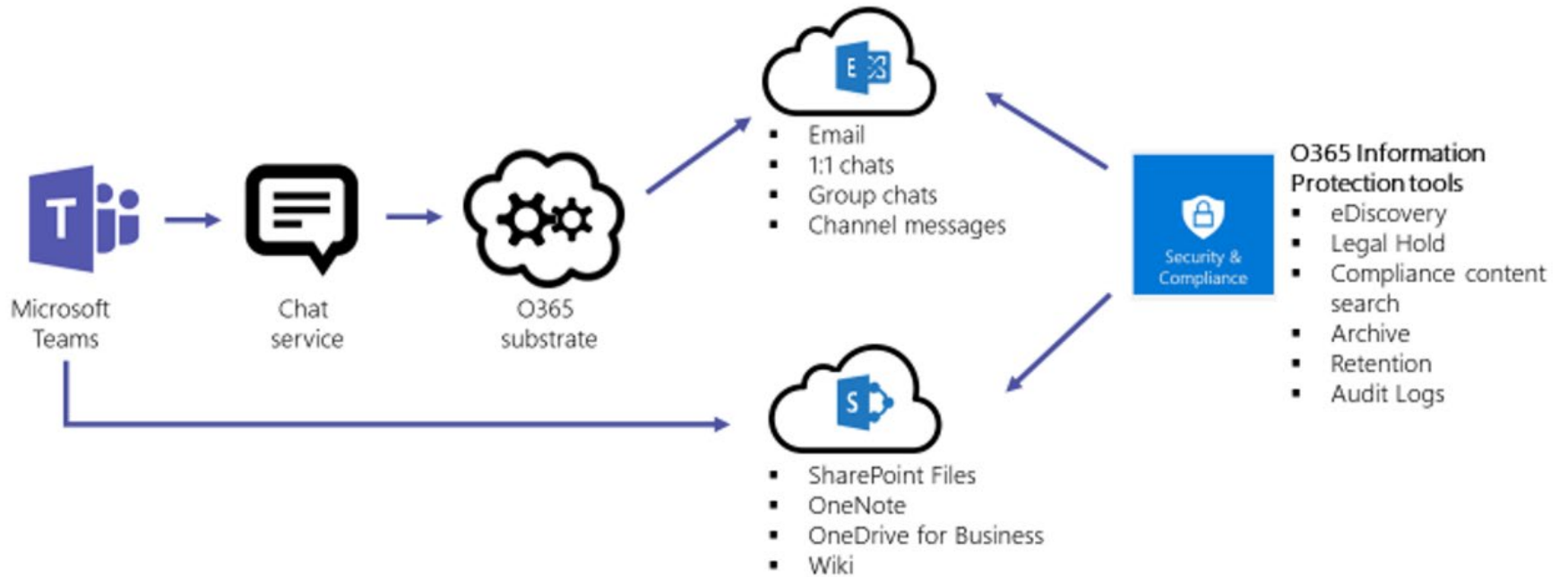
### Option 3



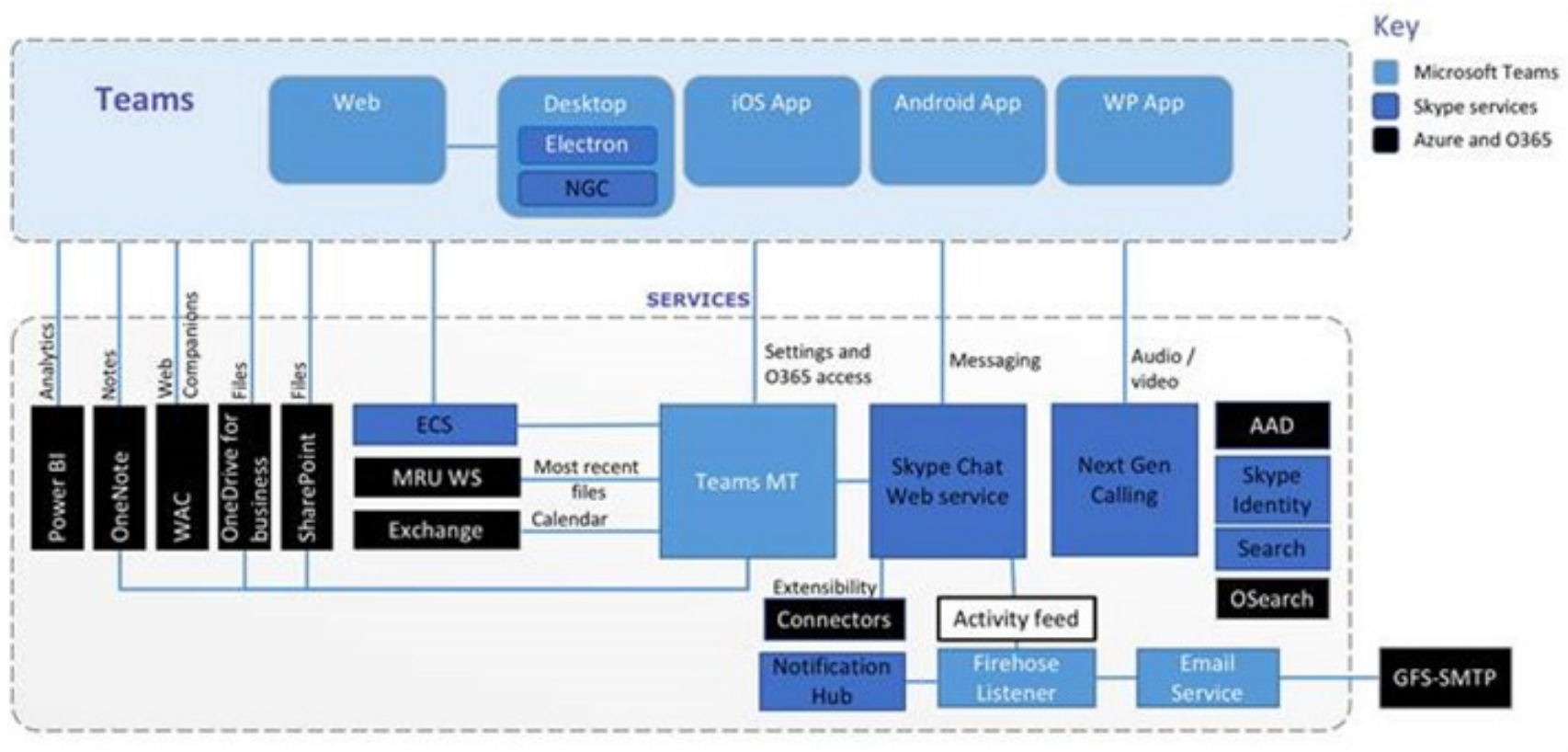


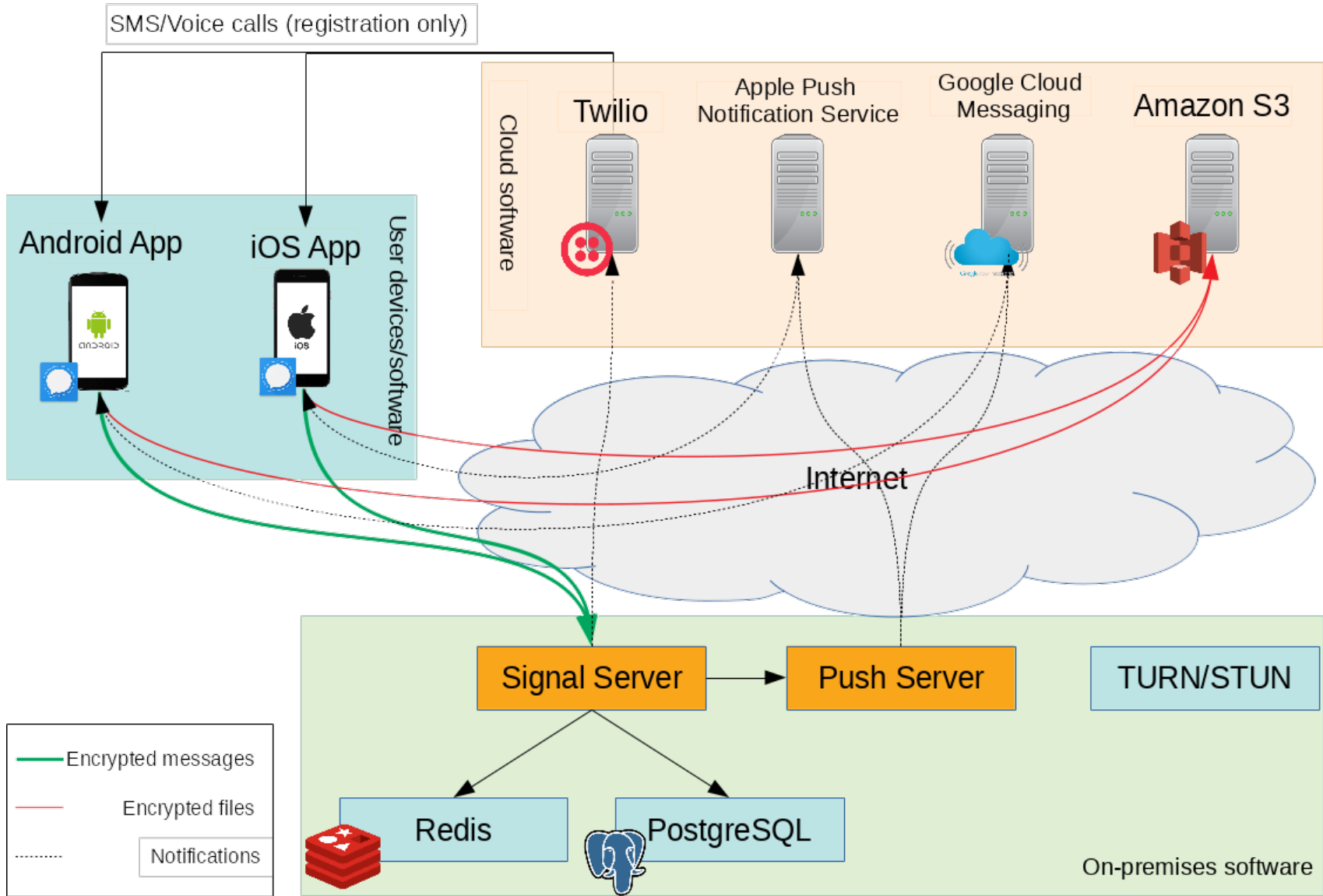
# Information Protection Architecture

Chat data and channel messages are journaled to Exchange storage (known as the Office 365 Substrate) to enable integrated management tools for information protection that work across all Office 365 workloads, including Microsoft Teams.



Microsoft Teams



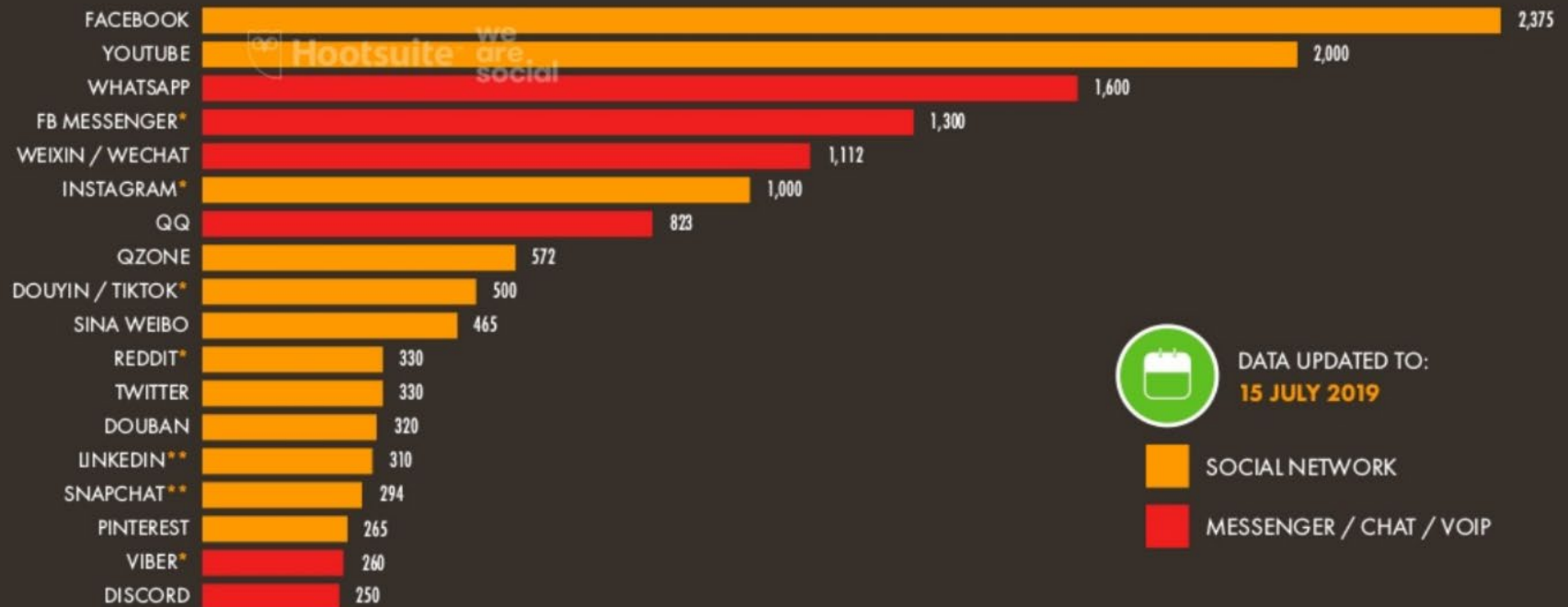




JUL  
2019

## ACTIVE USERS OF TOP SOCIAL PLATFORMS

BASED ON MONTHLY ACTIVE USERS, ACTIVE USER ACCOUNTS, OR UNIQUE MONTHLY VISITORS TO EACH PLATFORM, IN MILLIONS



DATA UPDATED TO:  
15 JULY 2019



SOCIAL NETWORK



MESSENGER / CHAT / VOIP

46

**SOURCES:** KEPIO'S ANALYSIS, LATEST COMPANY EARNINGS RELEASES, PRESS RELEASES OR MEDIA STATEMENTS; REPORTS IN REPUTABLE MEDIA (ALL TO JULY 2019). **\*ADVISORY:** PLATFORMS IDENTIFIED BY (\*) HAVE NOT PUBLISHED UPDATED USER FIGURES IN THE PAST 12 MONTHS, SO FIGURES MAY BE LESS RELIABLE. **\*\*NOTES:** THESE PLATFORMS DO NOT PUBLISH MAU DATA. LINKEDIN FIGURE IS BASED ON MONTHLY UNIQUE WEBSITE VISITORS IN DEC 2018, VIA SIMILARWEB. SNAPCHAT FIGURE EXTRAPOLATED FROM DATA REPORTED IN TECHCRUNCH (JUN 2017).



# Top Messenger Apps by Country [September 2018]

[Based on the Apple App Store Rank for each country in September 2018]

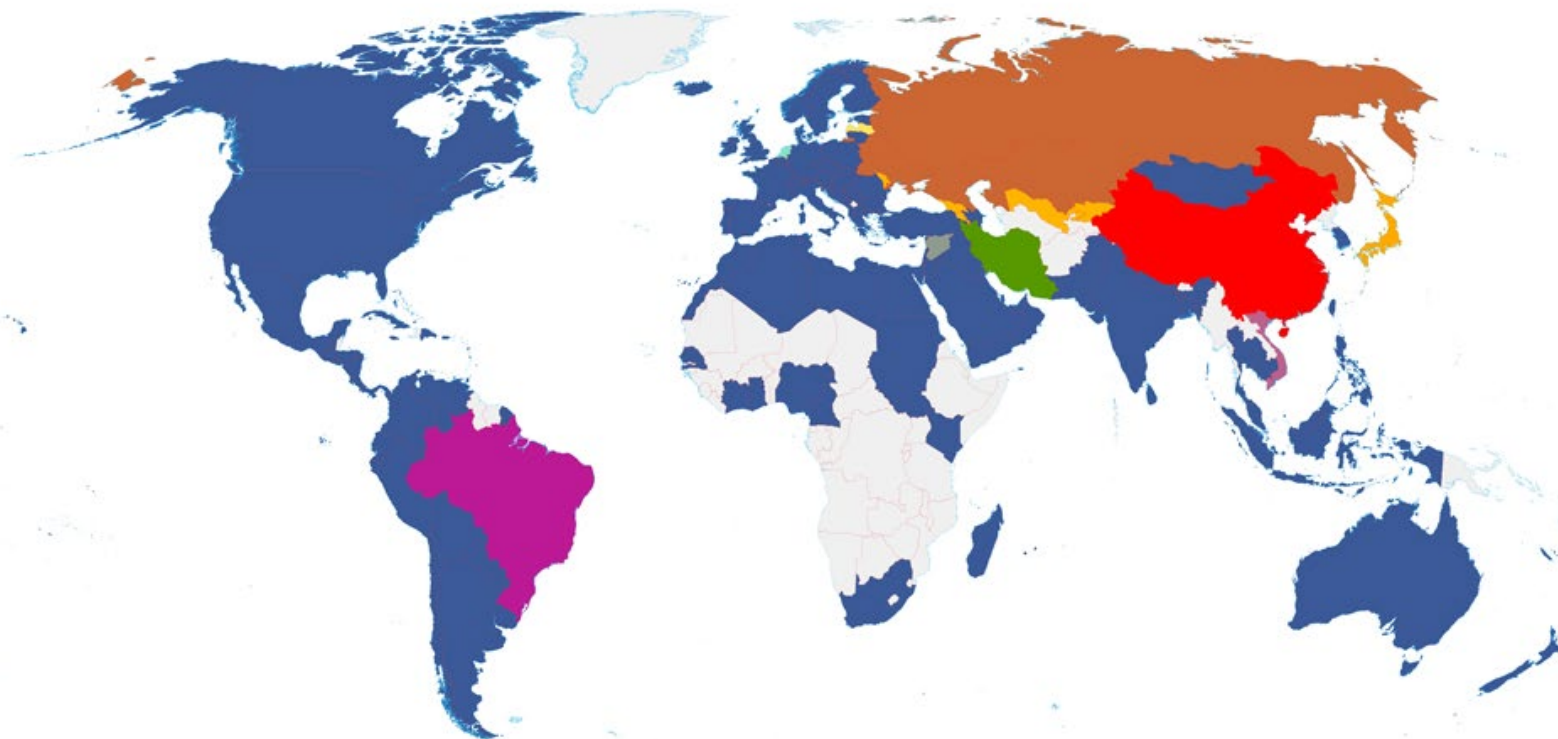


Source: Similarweb.com | September 2018 | Based on the Apple App Store Rank for each country  
Illustrated by Larry Kim | MobileMonkey.com



# WORLD MAP OF SOCIAL NETWORKS

December 2010



- |          |            |               |          |       |      |      |
|----------|------------|---------------|----------|-------|------|------|
| Facebook | V Kontakte | Odnoklassniki | Draugiem | Hyves | Zing | Mixi |
| Orkut    | QZone      | Maktoob       | Cloob    |       |      |      |

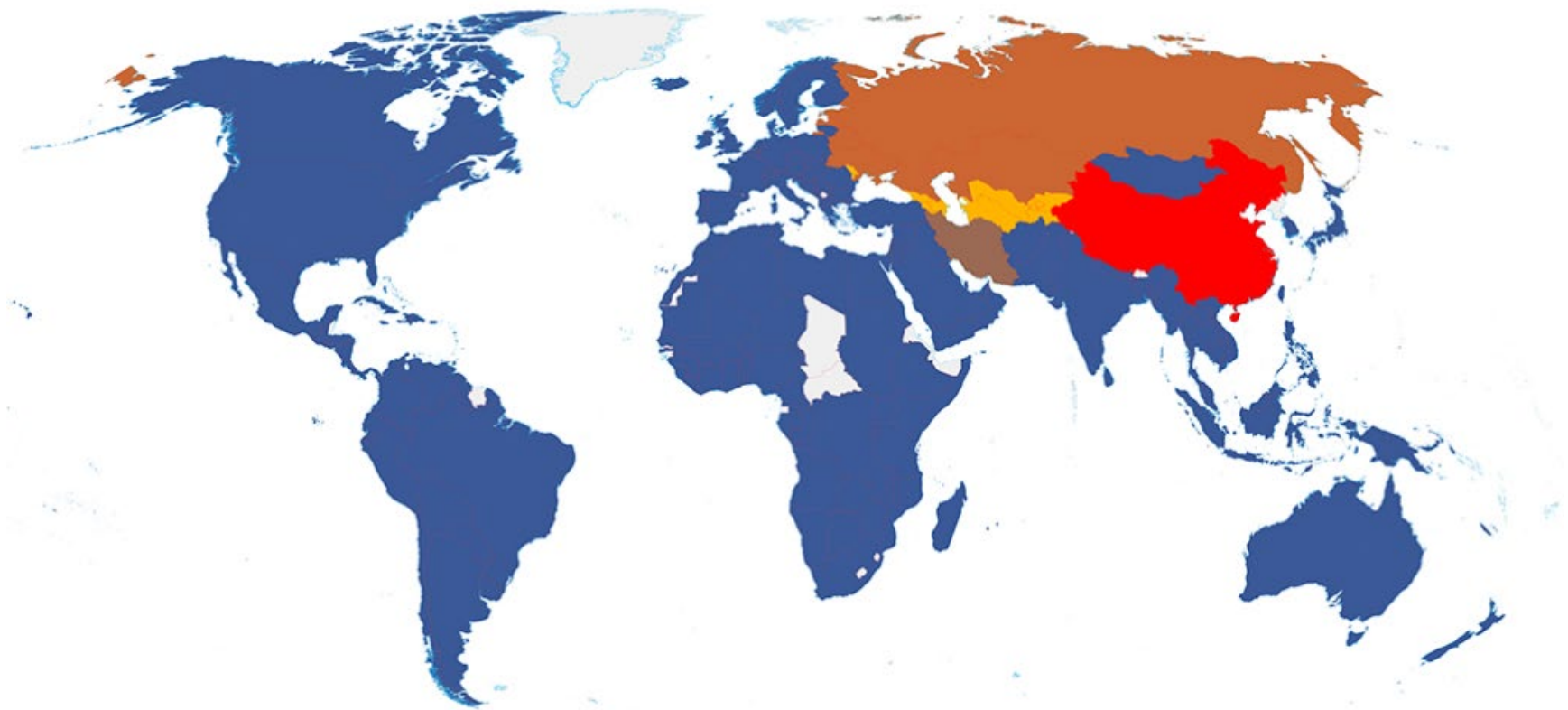
credits: Vincenzo Cosenza [www.vincos.it](http://www.vincos.it)

license: CC-BY-NC

source: Google Trends for Websites /Alexa

# WORLD MAP OF SOCIAL NETWORKS

January 2020

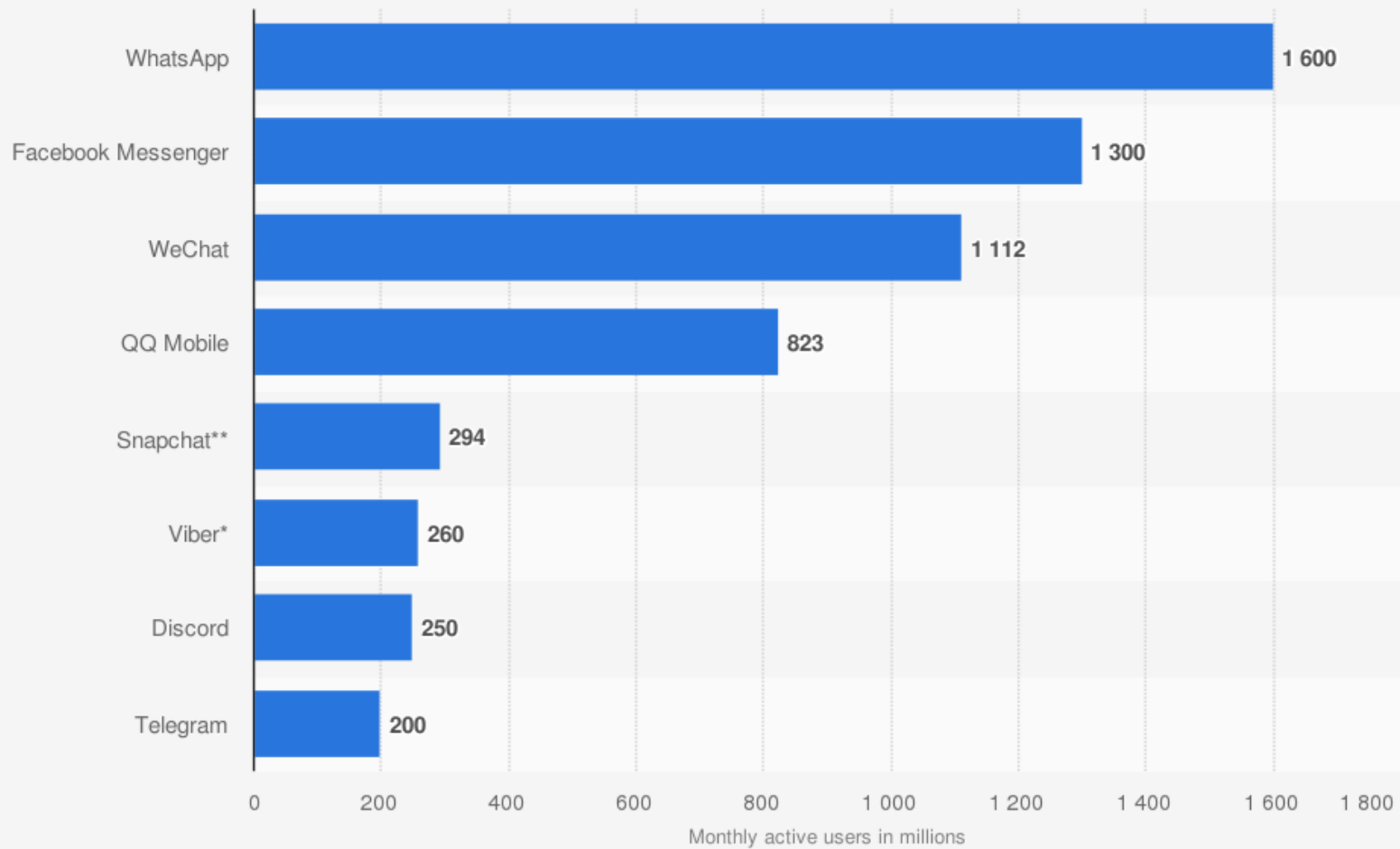


credits: Vincenzo Cosenza vincos.it

license: CC-BY-NC

source: Alexa/SimilarWeb

### Most popular global mobile messenger apps as of July 2019, based on number of monthly active users (in millions)



**Sources**

We Are Social; Various sources (Company data); Hootsuite; DataReportal © Statista 2019

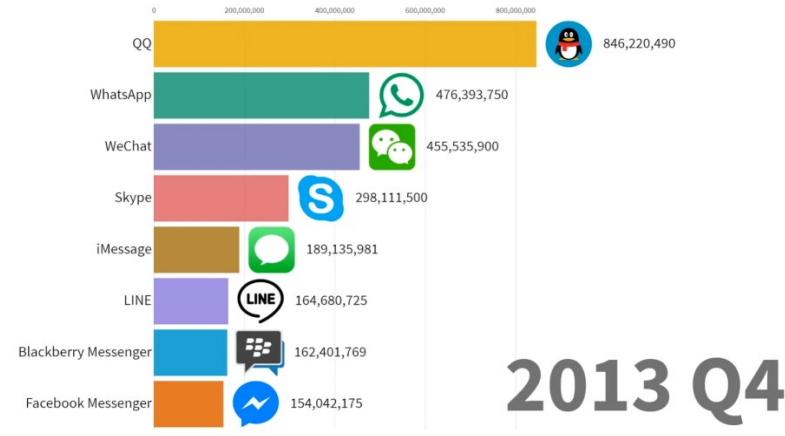
**Additional Information:**

Worldwide; Various sources (Company data); DataReportal; as of July 15, 2019

# -PART 10-

## Online Video Link

1997 to 2019 of Social Media App



[LINK](#)

## -PART 11-

### Closing Remarks

Many of us find it difficult to use multiple devices and multiple applications to facilitate the communication and data sharing we have grown accustomed to in the last 10 years. It is easier to use one application on one device and one or two accounts for it all, which has been part of the problem. Trying to “squeeze” all types of communications into one holder leads to the “eggs in one basket” issue and that is safety of your device, data, and freedom of expression.

Android offers the ability to install two instances of some applications for those with an additional SIM card, and other providers offer multi tray options of their mobile devices also. To recommend a paradigm shifting idea and implement it are difficult endeavors when faced with the likability and market share of Whats App. However, their new policy has made a global shift in the user base and it is best to act now while “change” is in the air than later.

I believe it is about time companies realize their employees also need their freedom and it is important to separate the corporate from the personal to protect all parties involved. I am not recommending structure your entire life around several applications but at the very least to use Microsoft Teams for inside company communication and external can be any combination of Email and Signal. Telegram is MCMA but it offers the ability to hide your contact number, which Whats App or Signal do not offer currently. If you have to communicate with a customer and be able to send uncompressed files, Telegram is the solution.

The proliferation of Chat Bots is no trend to ignore and many businesses and governments should seek professional services to build those Chat Bots to help ease their customer service expenses.

To determine what is the best path forward for you is to quantify what applications are available to you and how they intersect with the number of primary users you interact with daily for formal and informal groups. Try to separate work from personal to enjoy the full freedoms of each of those applications. If you do not use MS Teams or only use Google Docs, then maybe a Signal centric model will suit your needs.

Ideally a Microsoft architecture for the company and users will be best, coupled with Signal as seen on page 17, “Recommendation 3”.

## -PART 12-

### Sources & References used during Research

[Electronic Frontier Foundation \(USA\)](#)

[Slant \(USA\)](#)

[GDPR \(EU\)](#)

Various News Reports (Global)

[Why change?](#)

[CIPD \(UK\)](#)

[Wikipedia](#)

[Telegram Features](#)

[Market Research \(UK\)](#)

[Versus](#)

[Chat Bots being used for COVID 19 relief](#)

[Creating Whats App Chat Bot](#)

[Mobile App Development in 2020](#)

[Microsoft](#)

**Apps Researched:**

[Slack \(USA\)](#)

[Signal \(USA\)](#)

[Telegram \(RU\)](#)

[EKO \(UK\)](#)

[BBMe \(CAN\)](#)

[Whats App \(USA\)](#)

[Google Hang Out \(USA\)](#)

[Facebook Messenger \(USA\)](#)

[Kik \(CAN\)](#)

[Line \(JAP\)](#)

[Telegram \(GER\)](#)

[Threema \(CHE\)](#)

[WeChat \(CHN\)](#)

[Microsoft Skype \(USA\)](#)

[Wire \(USA\)](#)

[Microsoft Teams \(USA\)](#)

[Microsoft Yammer \(USA\)](#)

[Viber \(LUX\)](#)

[Twitter \(USA\)](#)

[Band \(KOR\) – South Korea](#)

[Signal \(USA\)](#)

[Group Me \(USA\)](#)

[Discord \(USA\)](#)

[Snap Chat \(USA\)](#)

[Voxer \(USA\)](#)

[Textra \(LBN\)](#)

[Weibo \(CHN\)](#)

[Ozone \(CHN\)](#)

[Riot](#)



Download this  
White Paper



Hassan Khan  
Contact Card



Website  
Link



WhatsApp  
YouTube video



Hassan I. Khan

Date: 24/January/2021

Email: [contact@hksltd.net](mailto:contact@hksltd.net) || Website: [www.hksltd.net](http://www.hksltd.net)