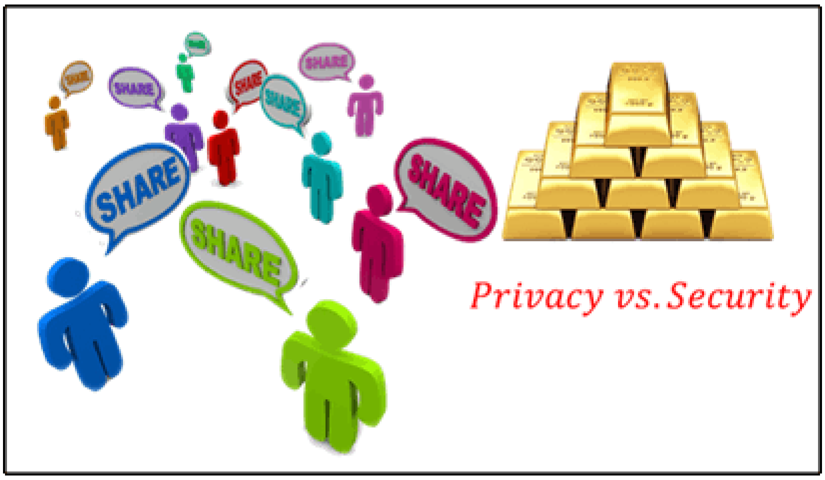
Examrace

New Privacy Policy of WhatsApp vs Other Apps YouTube Lecture Handouts

New Privacy Policy of WhatsApp vs Other Apps (Signal/Telegram) Your Data is the New Gold: Understand How to Protect It!



©Examrace. Report ©violations @https://tips.fbi.gov/

- Data privacy has always been important. It’s why people put locks on filing cabinets and rent safety deposit boxes at their banks. However, as more of our data becomes digitized, and we share more information online, data privacy is taking on greater importance.

- For instance, you likely wouldn’t mind sharing your name with a stranger in the process of introducing yourself, but there’s other information you wouldn’t share, at least not until you become more acquainted with that person. Open a new bank account, though, and you will probably be asked to share a tremendous amount of personal information, well beyond your name.

- In the digital age, we typically apply the concept of data privacy to critical personal information, also known as personally identifiable information (PII) and personal health information (PHI) . This can include Social Security numbers, health and medical records, financial data, including bank account and credit card numbers, and even basic, but still sensitive, information, such as full names, addresses and birthdates.

- Whether or how data is shared with third parties.
- How data is legally collected or stored.
- Regulatory restrictions such as GDPR, HIPAA, GLBA, or CCPA. The law grants citizens a number of rights, including the right to data portability (which allows people to move their data between platforms) , and the right not to be subject to decisions based on automated data processing (prohibiting, for example, the use of an algorithm to reject applicants for jobs or loans) .
- 1st party - First party data is the information you collect directly from your audience or customers (subscription data, social data)
- 2nd party - Second party data is essentially someone else's first party data. The seller collects data straight from their audience, and it all comes from one source (web activities, social media, mobile app usage)
- 3rd party - Third party data is data that you buy from outside sources that are not the original collectors of that data. Instead, you buy it from large data aggregators that pull it from various other platforms and websites where it was generated.

"Unless" Tracking Cookies Disabled

- Companies such as Google, Facebook, and Amazon have all built empires atop the data economy. Transparency in how businesses request consent, abide by their privacy policies, and manage the data that they have collected is vital to building trust and accountability with customers and partners who expect privacy.
- Privacy is the right of an individual to be free from uninvited surveillance
- Privacy is governing how data is collected, shared, and used
- Security is protecting data from internal and external hackers

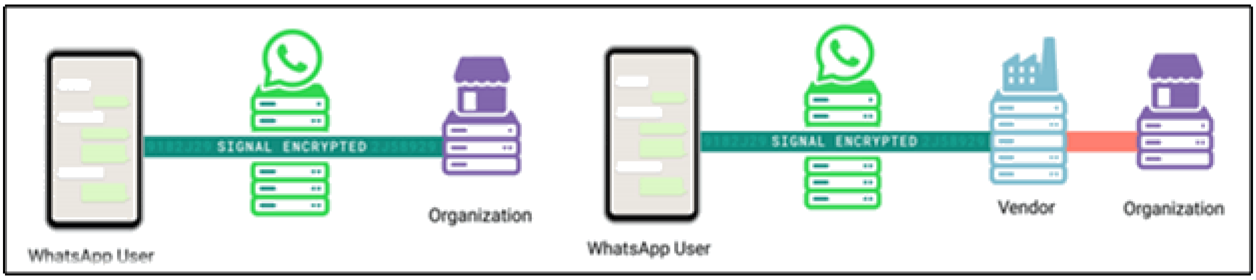
Open Source Code

Open-source software is a type of computer software in which source code is released under a license in which the copyright holder grants users the rights to use, study, change, and distribute the software to anyone and for any purpose. Open-source software may be developed in a collaborative public manner.

E2EE End-To-End Encryption

End-to-end encryption (E2EE) is a method of secure communication that prevents third parties from accessing data while it's transferred from one **end** system or device to another. In E2EE, the data is **encrypted** on the sender's system or device and only the recipient is able to decrypt it.

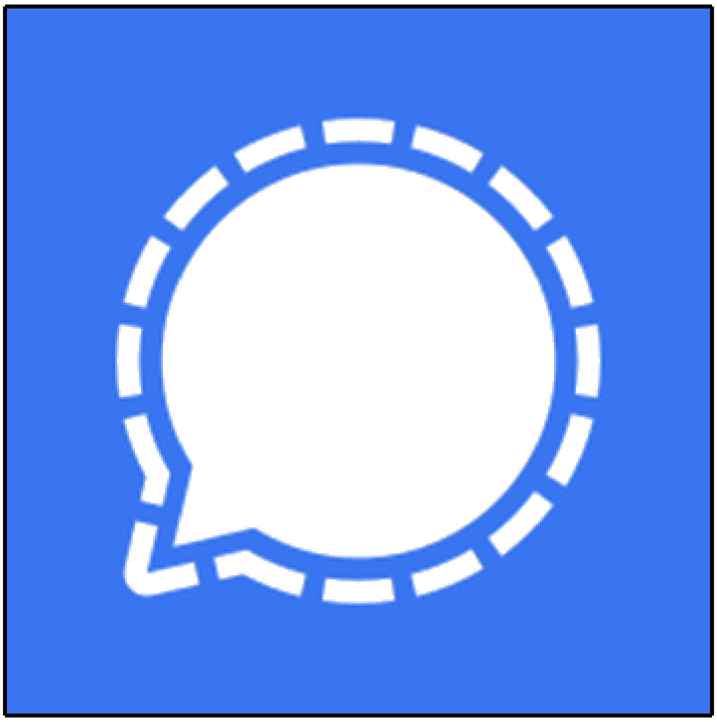
From White Paper of WhatsApp



©Examrace. Report ©violations @https://tips.fbi.gov/

- WhatsApp considers communications with Business API users who manage the API endpoint on servers they control to be end-to-end encrypted since there is no third-party access to content between endpoints.
- Some organizations may choose to delegate management of their **WhatsApp Business API endpoint to a vendor**. In these instances, communication still uses the same Signal protocol encryption and clients on or after version v2.31 are configured to generate private keys within the vendor-controlled API endpoint. However, because the WhatsApp Business API user has chosen a third party to manage their endpoint, WhatsApp does not consider the messages end-to-end encrypted.

About "Signal"



- Signal's software is free and open-source. Its clients are published under the GPLv3 license, while the server code is published under the AGPLv3 license. The official Android app generally uses the proprietary Google Play Services (installed on most Android devices) for functions such as push notifications. Signal also has an official client app for iOS and a web app on desktops.
- The non-profit Signal Foundation was launched in February 2018 with initial funding of $ 50 million from Brian Acton
- The end-to-end encrypted messaging service Signal was launched in 2014, and has become more widely used in 2019 and 2020. Finally as Signal Messenger in 2018.

About "Telegram"

- Telegram is a freeware, cross-platform, cloud-based instant messaging (IM) software and application service. The service also provides end-to-end encrypted video calling, VoIP, file sharing and several other features. It was initially launched for iOS on 14 August 2013 and Android in October 2013.
- Telegram provides end-to-end encrypted calls and optional end-to-end encrypted "secret" chats between two online users on smartphone clients, whereas cloud chats use client-server/server-client encryption.
- Telegram is building its own Ad Platform. Durov stated that advertisements would appear in channels, which are currently serving non-integrated ads, and will be

integrated into the interface. The company intends to generate funds that way and support its services for the foreseeable future.

About “Threema”

- Threema is a paid open-source end-to-end encrypted instant messaging application for iOS and Android.
- The software is based on the privacy by design principles, as it does not require a phone number or any other personally identifiable information. This helps anonymize the users to a degree.
- In addition to text messaging, users can make voice and video calls, send multimedia, locations, voice messages and files. A web app version, Threema Web, can be used on desktop devices.
- The Swiss company Threema GmbH develops Threema. The servers are located in Switzerland and the development is based in Pfaffikon SZ. As of January 2020, Threema had 8 million users.

About “WhatsApp”

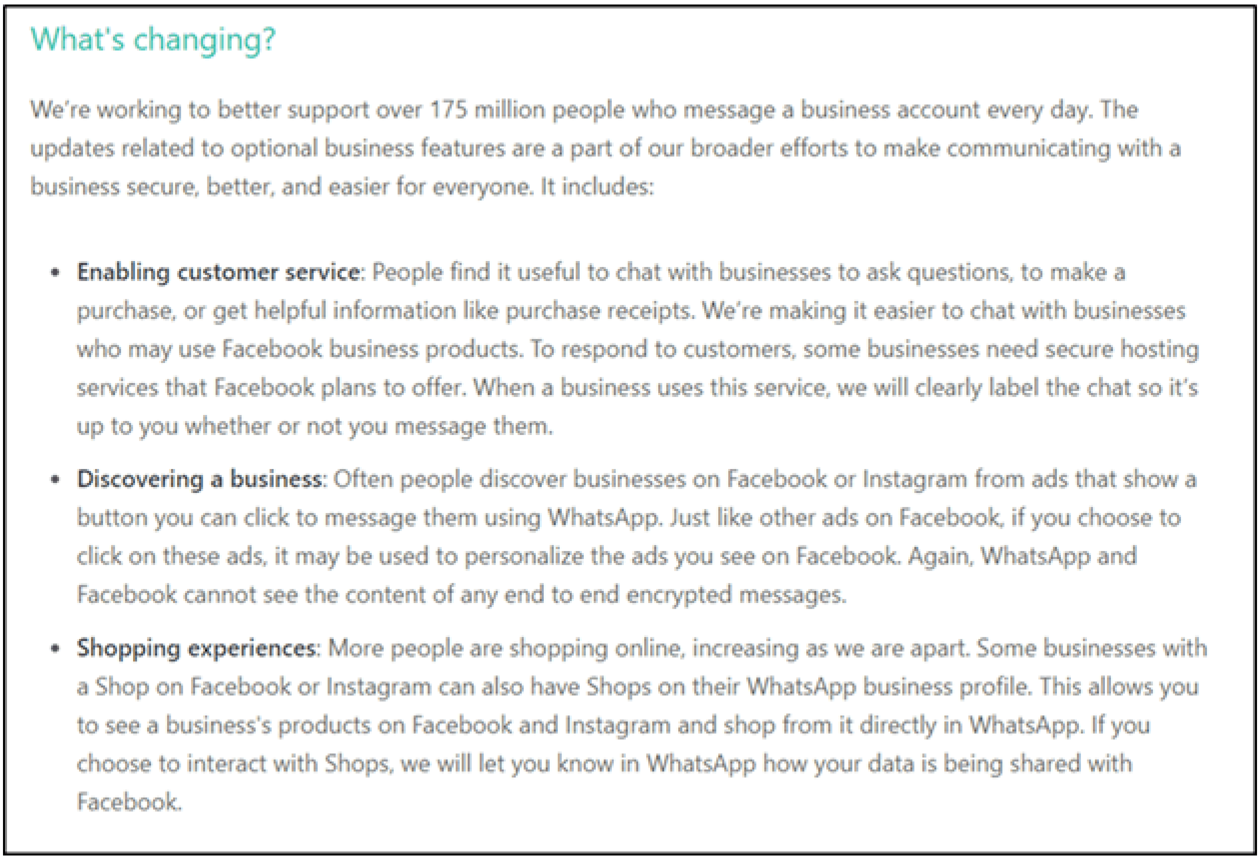
©Examrace. Report ©violations @https://tips.fbi.gov/

- WhatsApp Messenger, or simply WhatsApp, is an American freeware, cross-platform messaging, and Voice over IP (VoIP) service owned by Facebook, Inc. It allows users to send text messages and voice messages, make voice and video calls, and share images, documents, user locations, and other media

- WhatsApp Inc. of Mountain View, California, which was acquired by Facebook in February 2014 for approximately US $ 19.3 billion, created the client application.
- Has over 2 billion users worldwide as of February 2020.

Facebook – Cambridge Analytica Data Scandal

The Facebook – Cambridge Analytica data scandal concerned the obtaining of the personal data of millions of Facebook users without their consent by British consulting firm Cambridge Analytica, predominantly to be used for political advertising. The data were collected through an app called "thisisyourdigitallife," developed by data scientist Aleksandr Kogan and his company Global Science Research. The app consisted of a series of questions to build psychological profiles on users, and collected the personal data of the users' Facebook friends via Facebook's Open Graph platform. The app harvested the data of up to 87 million Facebook profiles. Cambridge Analytica sought to sell the data of American voters to political campaigns and ultimately provided assistance and analytics to the 2016 presidential campaigns of Ted Cruz and Donald Trump



What's changing?

We're working to better support over 175 million people who message a business account every day. The updates related to optional business features are a part of our broader efforts to make communicating with a business secure, better, and easier for everyone. It includes:

- **Enabling customer service**: People find it useful to chat with businesses to ask questions, to make a purchase, or get helpful information like purchase receipts. We're making it easier to chat with businesses who may use Facebook business products. To respond to customers, some businesses need secure hosting services that Facebook plans to offer. When a business uses this service, we will clearly label the chat so it's up to you whether or not you message them.
- **Discovering a business**: Often people discover businesses on Facebook or Instagram from ads that show a button you can click to message them using WhatsApp. Just like other ads on Facebook, if you choose to click on these ads, it may be used to personalize the ads you see on Facebook. Again, WhatsApp and Facebook cannot see the content of any end to end encrypted messages.
- **Shopping experiences**: More people are shopping online, increasing as we are apart. Some businesses with a Shop on Facebook or Instagram can also have Shops on their WhatsApp business profile. This allows you to see a business's products on Facebook and Instagram and shop from it directly in WhatsApp. If you choose to interact with Shops, we will let you know in WhatsApp how your data is being shared with Facebook.

©Examrace. Report ©violations @https://tips.fbi.gov/

- Data can be shown to insurance agents, medical agent, products, gaming, and toys
- Different rates can be charged for the same service provided to you and others
- Date of birth information is available – they can target age specific products

- Children are specifically gullible to ads and can be targeted with specific products and services.
- They can identify your location based on your interest and businesses you visit, understand standard of living and tentative amount you are ready to spend.

Snapchat

©Examrace. Report ©violations @https://tips.fbi.gov/

One of the principal features of Snapchat is that pictures and messages are usually only available for a short time before they become inaccessible to their recipients. The app has evolved from originally focusing on person-to-person photo sharing to presently featuring users' "Stories" of 24 hours of chronological content, along with "Discover," letting brands show ad-supported short-form content. It also allows users to keep photos in the "my eyes only" which lets them keep their photos in a password-protected space. It has also reportedly incorporated limited use of end-to-end encryption, with plans to broaden its use in the future.

Snapchat servers are designed to automatically delete all unopened **Chats** after 30 days.

Tips to Protect Your Data

- At home, use a mail slot or locking mailbox, so that thieves can't steal your mail.
- Before discarding, shred documents, including receipts and bank and credit card statements that contain personal information.
- Make sure to secure your home Wi-Fi network and other devices so that criminal's can't "eavesdrop" on your online activity.
- Don't automatically provide your Social Security number just because someone asks for it. Determine if they really need it and, if so, ask how they'll help protect it.
- Use strong, unique passwords for all of your online accounts.

One final recommendation to help you keep your data private: Regularly assess the privacy settings on your social media accounts. If you don't, you may be sharing a lot more than just your name with people you have never met — and a savvy criminal could use that information to steal your identity and a lot more.

- 1974: US Privacy Act of 1974 maintains restrictions on data held by government agencies
- 1996: Health Insurance Portability and Accountability Act (HIPAA) protects health information
- 1999: Gramm-Leach-Bliley Act (GLBA) protects financial nonpublic personal information (NPI)
- 2000: Children ′ s Online Privacy Protection Act (COPPA) protects Childrens ′ data (⩽ 12 yrs.)
- 2000: The Privacy Rule fortifies HIPAA and safeguards individuals'private health information
- 2002: Sarbanes-Oxley Act (SOX) protects the public from fraudulent practices by corporations
- 2002: Federal Information Security Management Act (FISMA) orders agencies to protect data
- 2013: ISO 27001 functions as a framework for an information security management system
- 2018: General Data Privacy Regulation (GDPR) aims to protect EU citizens' personal data
- 2020: California Consumer Privacy Act (CCPA) restricts how companies collect and use data

Global Scenario

- A Supreme Court mention right to privacy is fundamental right.

- But nothing has been there in India Legislation.
- *Right to Privacy - A Fundamental Right*
- The Supreme Court confirmed that the right to privacy is a fundamental right that does not need to be separately articulated but can be derived from Articles 14,19 and 21 of the Constitution of India. It is a natural right that subsists as an integral part to the right to life and liberty. It is a fundamental and inalienable right and attaches to the person covering all information about that person and the choices that he/she makes. It protects an individual from the scrutiny of the State in their home, of their movements and over their reproductive choices, choice of partners, food habits, etc. Therefore, any action by the State that results in an infringement of the right to privacy is subject to judicial review.
- *Not an Absolute Right - Subject to Reasonable Restrictions*
- *Aadhaar data cannot be accessed by private companies in India*

✍ Manishika

Developed by: Mindsprite Solutions