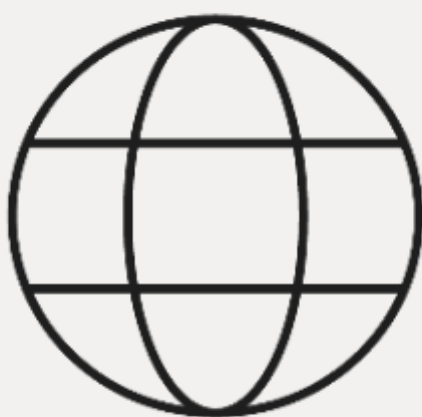
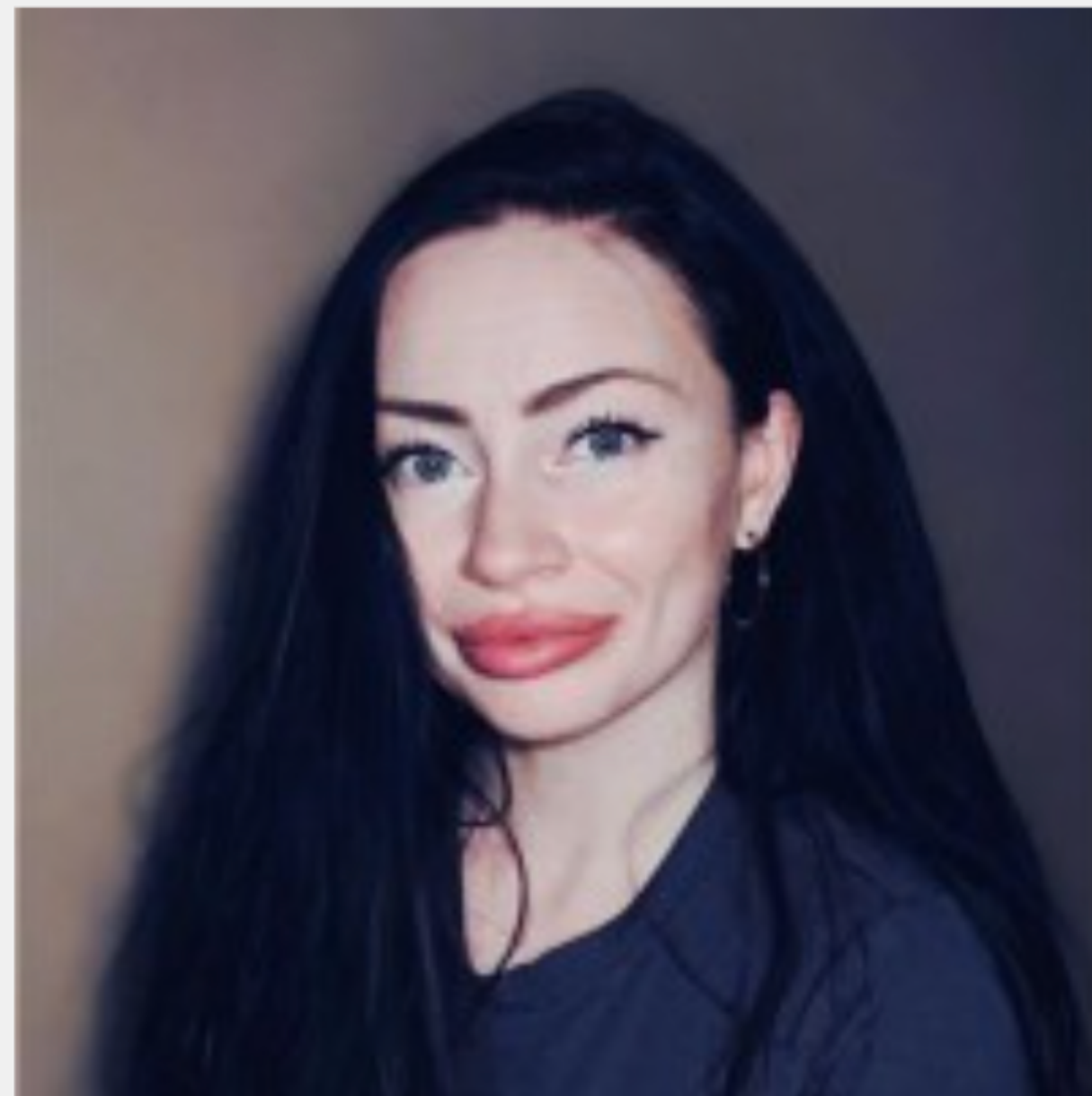




Bezpieczeństwo w świecie komunikatorów czyli czy szyfrowanie danych = prywatność?

Kasia Brzozowska



Google
Developer
Groups



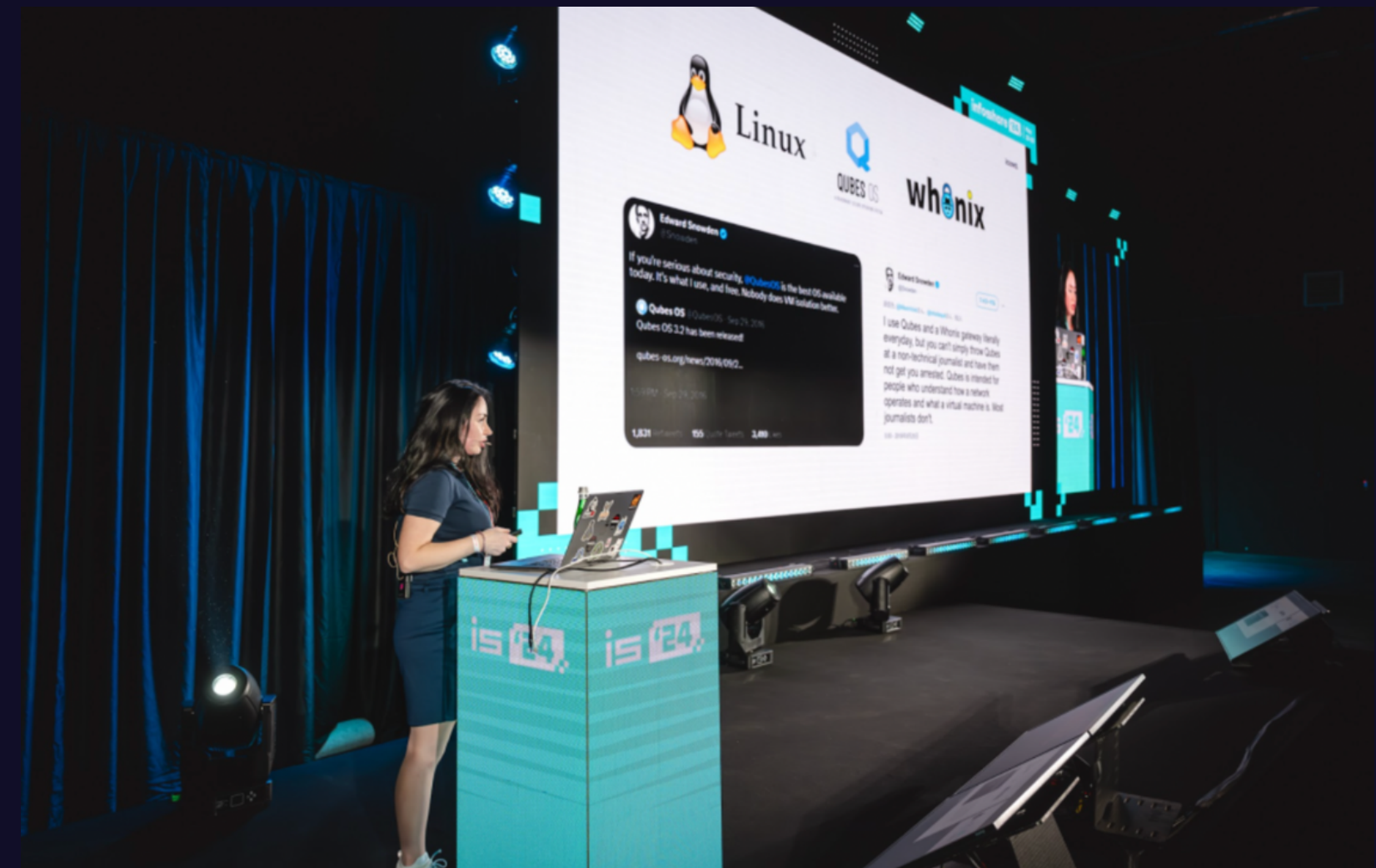
DevSecOps Engineer w **KnowIT**
Właścicielka w **Be Like Neo & Trinity**
Twórca w **Projekt TFMAESTRO**



Cyberbezpieczeństwo | DevOps | Cloud
| Prywatność



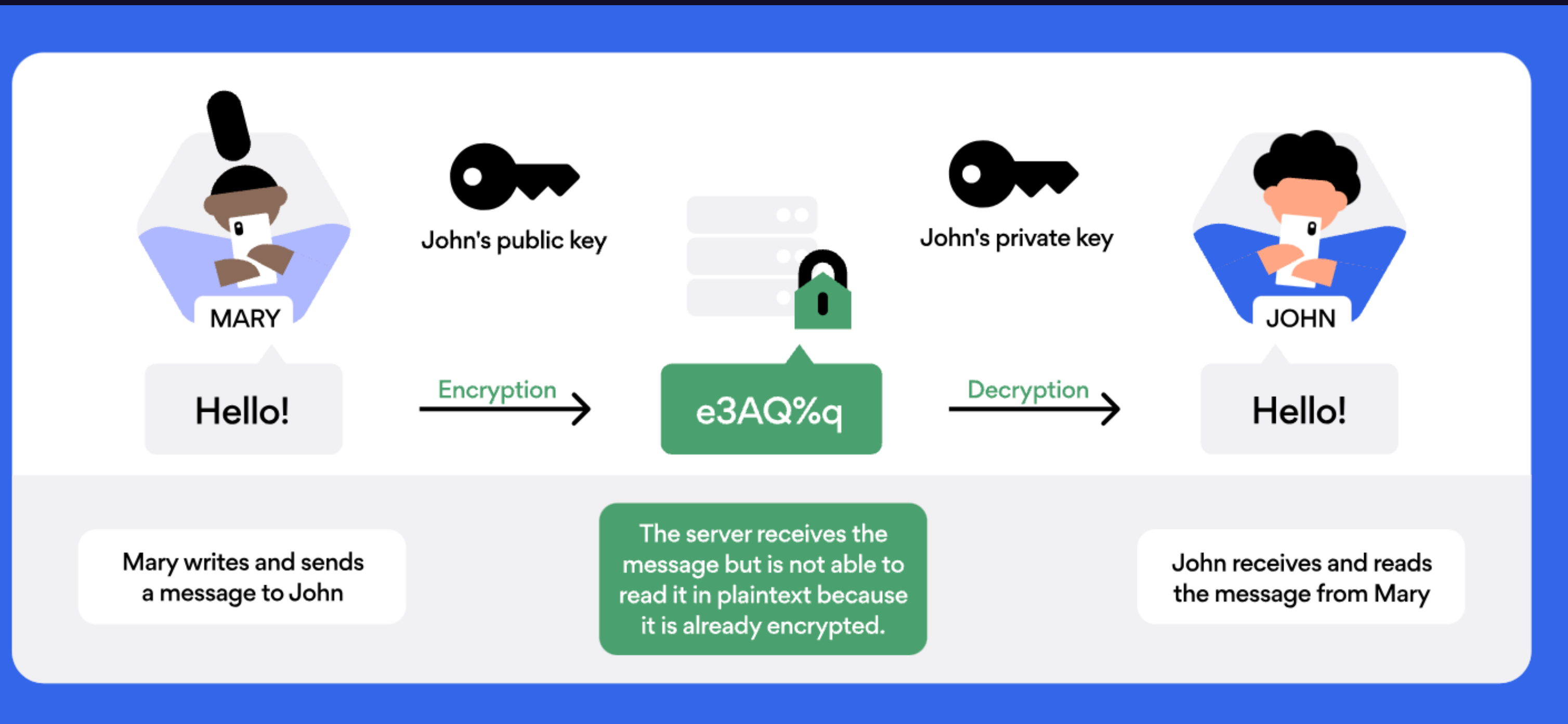
linktr.ee/katarzynabrzozowska



A close-up shot of Leonardo DiCaprio from the movie Inception. He is wearing a dark blue pinstripe suit and a red tie with white polka dots. He is holding a US \$100 bill in front of his face with both hands, looking directly at the camera with a slight, knowing smile. The background is a dimly lit office with a framed picture of a sailboat on the wall and a computer monitor visible on the right.

Informacja jest nową walutą świata

How end-to-end encryption works?



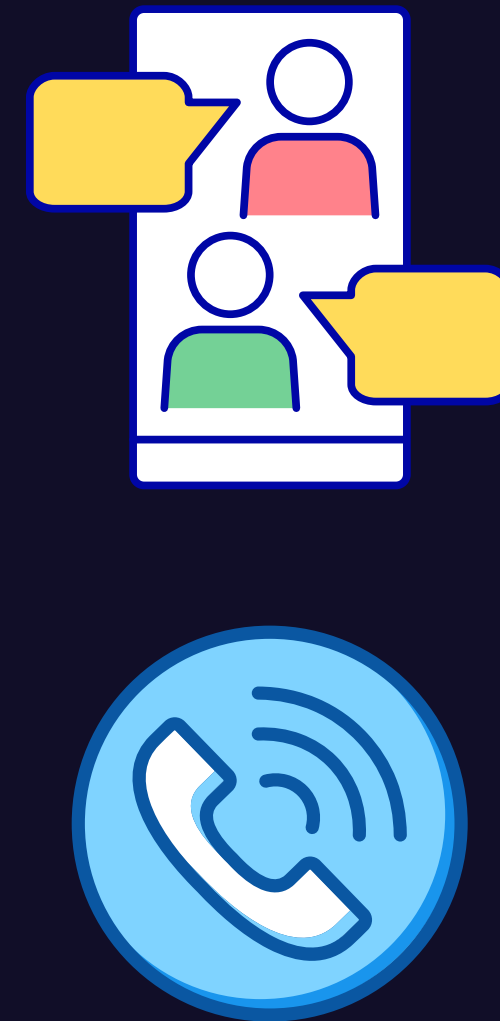


Full E2EE



VS

Partial E2EE



**MY DAD SAYS
YOU'RE SPYING
ON US**

**HE'S NOT
YOUR DAD**

WhatsApp is updating its terms and privacy
policy.



WhatsApp

META PLATFORMS INC.



- **Full E2EE**
- **Signal Protocol**



- **Phone number required**
- **FB + IG data**
- **Not open source**
- **Conversations kept on server permanently**
- **USA jurisdiction**



Messenger

META PLATFORMS INC.



- **Partial E2EE**
- **E2EE not by default (Secret Conversations)**



- **FB account required**
- **Centralized architecture**
- **Not open source**
- **FB + IG data**
- **USA jurisdiction**



Telegram

TELEGRAM FZ LLC



- **Partial E2EE**
- **E2EE not by default (Secret chats)**



- **Phone number required**
- **MTPROTO Mobile Protocol**
- **Partially open source**
- **Conversations kept on server permanently**
- **Unsure jurisdiction**



iMessage

APPLE INC.



- **Full E2EE**



- **Phone number required**
- **Backups are not encrypted**
- **Centralized architecture**
- **Not open source**
- **USA jurisdiction**



Signal

SIGNAL TECHNOLOGY
FOUNDATION



- **Full E2EE**
- **Signal Protocol**
- **Open source**
- **Tiny metadata collection**



- **Phone number required**
- **USA jurisdiction**
- **Located in AWS**

Signal
'Data Linked To You'



iMessage
'Data Linked To You'

Contact Info

- Email Address
- Phone Number

Search History

Identifiers

- Device ID

WhatsApp
'Data Linked To You'

Analytics

- Purchases**
Purchase History
- Location**
Coarse Location
- Contact Info**
Phone Number
- User Content**
Other User Content
- Identifiers**
User ID
Device ID
- Usage Data**
Product Interaction
Advertising Data
- Diagnostics**
Crash Data
Performance Data
Other Diagnostic Data

App Functionality

- Purchases**
Purchase History
- Financial Info**
Payment Info
- Location**
Coarse Location
- Contact Info**
Email Address
Phone Number
- Contacts**
Contacts
- User Content**
Customer Support
Other User Content
- Identifiers**
User ID
Device ID
- Usage Data**
Product Interaction
- Diagnostics**
Crash Data
Performance Data
Other Diagnostic Data

Facebook Messenger
'Data Linked To You'

Third-Party Advertising

- Purchases**
Purchase History
- Financial Info**
Other Financial Info
- Location**
Precise Location
Coarse Location
- Contact Info**
Physical Address
Email Address
Name
Phone Number
Other User Contact Info
- Contacts**
Contacts
- User Content**
Photos or Videos
Gameplay Content
Other User Content
- Search History**
Search History
- Browsing History**
Browsing History
- Identifiers**
User ID
Device ID
- Usage Data**
Product Interaction
Advertising Data
Other Usage Data
- Diagnostics**
Crash Data
Performance Data
Other Diagnostic Data
- Other Data**
Other Data Types

Analytics

- Health & Fitness**
Health
Fitness
- Purchases**
Purchase History
- Financial Info**
Payment Info
Other Financial Info
- Location**
Precise Location
Coarse Location
- Contact Info**
Physical Address
Email Address
Name
Phone Number
Other User Contact Info
- Contacts**
Contacts
- User Content**
Photos or Videos
Gameplay Content
Other User Content
- Search History**
Search History
- Browsing History**
Browsing History
- Identifiers**
User ID
Device ID
- Usage Data**
Product Interaction
Advertising Data
Other Usage Data
- Sensitive Info**
Sensitive Info
- Diagnostics**
Crash Data
Performance Data
Other Diagnostic Data
- Other Data**
Other Data Types

Product Personalisation

- Purchases**
Purchase History
- Financial Info**
Other Financial Info
- Location**
Precise Location
Coarse Location
- Contact Info**
Physical Address
Email Address
Name
Phone Number
Other User Contact Info
- Contacts**
Contacts
- User Content**
Photos or Videos
Gameplay Content
Other User Content
- Search History**
Search History
- Browsing History**
Browsing History
- Identifiers**
User ID
Device ID
- Usage Data**
Product Interaction
Advertising Data
Other Usage Data
- Sensitive Info**
Sensitive Info
- Diagnostics**
Crash Data
Performance Data
Other Diagnostic Data
- Other Data**
Other Data Types

App Functionality

- Health & Fitness**
Health
Fitness
- Purchases**
Purchase History
- Financial Info**
Payment Info
Credit Info
Other Financial Info
- Location**
Precise Location
Coarse Location
- Contact Info**
Physical Address
Email Address
Name
Phone Number
Other User Contact Info
- Contacts**
Contacts
- User Content**
Emails or Text Messages
Photos or Videos
Audio Data
Gameplay Content
Customer Support
Other User Content
- Search History**
Search History
- Browsing History**
Browsing History
- Identifiers**
User ID
Device ID
- Usage Data**
Product Interaction
Advertising Data
Other Usage Data
- Sensitive Info**
Sensitive Info
- Diagnostics**
Crash Data
Performance Data
Other Diagnostic Data
- Other Data**
Other Data Types

Other Purposes

- Purchases**
Purchase History
- Financial Info**
Other Financial Info
- Location**
Precise Location
Coarse Location
- Contact Info**
Physical Address
Email Address
Name
Phone Number
Other User Contact Info
- Contacts**
Contacts
- User Content**
Photos or Videos
Gameplay Content
Customer Support
Other User Content
- Search History**
Search History
- Browsing History**
Browsing History
- Identifiers**
User ID
Device ID
- Usage Data**
Product Interaction
Advertising Data
Other Usage Data
- Diagnostics**
Crash Data
Performance Data
Other Diagnostic Data
- Other Data**
Other Data Types



Threema

THREEMA GMBH



- **Full E2EE**
- **No phone number required**
- **Open source**
- **Swiss jurisdiction**
- **Decentralized architecture**
- **GDPR compliant**
- **NaCl cryptography library**



- **Not free (but still cheap!)**

	 Threema	 WhatsApp	 Signal	 Telegram
Privacy by Design: No phone number or email address required	✓	✗	✗	✗
End-to-end encryption of transmitted messages	✓	✓	✓	✗ ¹
Open source	✓	✗	✓	✓
GDPR compliance	✓	✗	✗ ²	✗
Corporate solution available	✓	✗ ³	✗	✗
Transparency report	✓	(✓) ⁴	✗ ⁵	✗ ⁶
Funding	App users	Meta/advertising	Donation / Brian Acton	Pavel Durov / subscriptions / advertising
Jurisdiction	Switzerland	USA ⁷	USA ⁷	n/a

<https://threema.ch/en/messenger-comparison>



Brigar

BRIAR PROJECT



Brigar uses direct, encrypted connections between users to prevent surveillance and censorship.



- **Full E2EE**
- **No phone number required**
- **Open source**
- **Tor network**
- **Decentralized architecture**
- **Swiss jurisdiction**



- **More difficult to use**



Session

THE SESSION TECHNOLOGY
FOUNDATION



- **Full E2EE**
- **No phone number required**
- **Custom onion network**
- **Decentralized architecture**
- **Swiss jurisdiction**



- **Voice & video calls are in beta**

FEDERAL BUREAU OF INVESTIGATION

LAWFUL ACCESS



(U//FOUO) FBI's Ability to Legally Access Secure Messaging App Content and Metadata

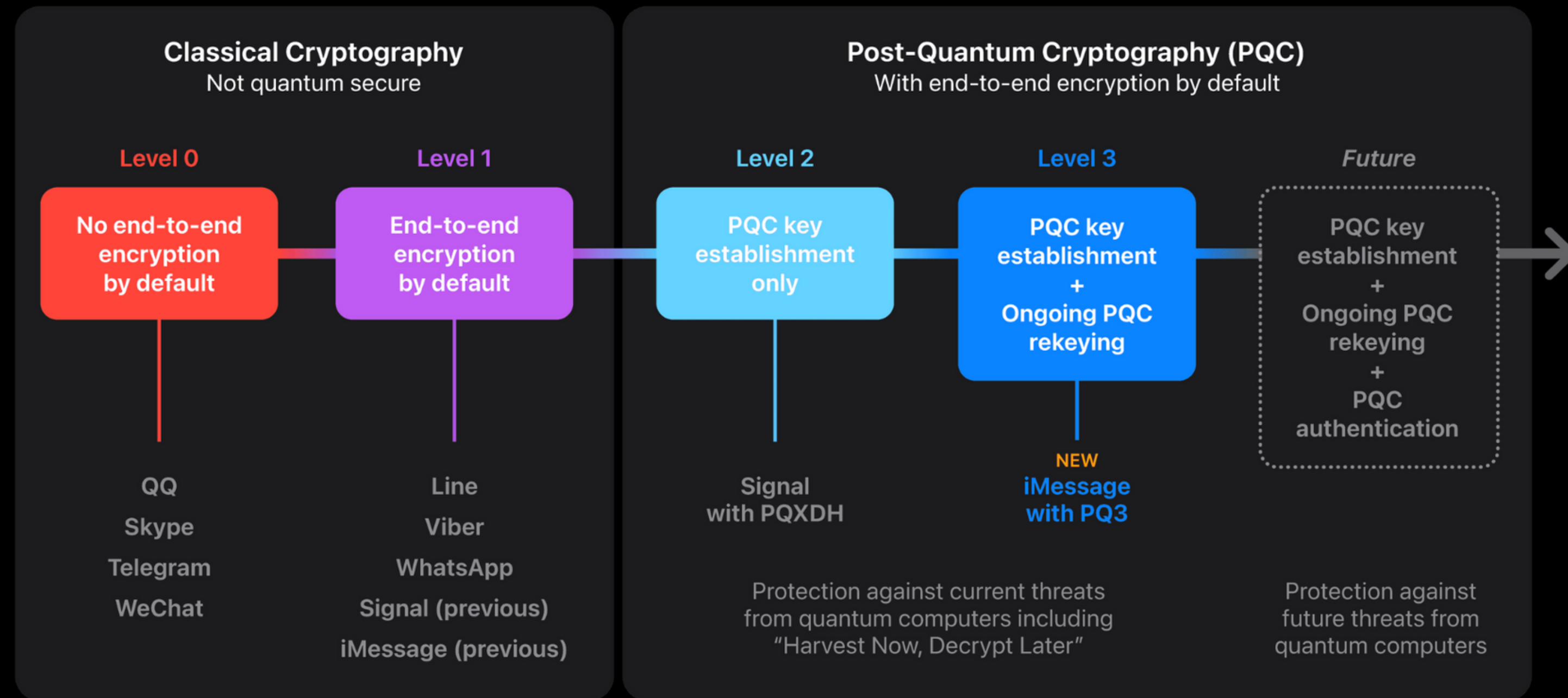
(U//LES) As of November 2020, the FBI's ability to legally access secure content on leading messaging applications is depicted below, including details on accessible information based on the applicable legal process. Return data provided by the companies listed below, with the exception of WhatsApp, are actually logs of latent data that are provided to law enforcement in a non-real-time manner and may impact investigations due to delivery delays.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

App	iMessage	Line	Signal	Telegram	Threema	Viber	WeChat	WhatsApp	Wickr
Information Accessed									
Legal Process & Additional Details	• Message Content: Limited • Subpoena: can render basic subscriber information • 18 U.S.C. §2703(d): can render 25 days of iMessage lookups to and from a target number² • Pen Register: no capability⁴ • Search Warrant: can render backups of a target device; if target uses iCloud backup, the encryption keys should also be provided with content return; can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud	• Message Content: Limited⁴ • Suspect's and/or victim's registered information: (profile image, display name, email address, phone number, LINE ID, date of registration, etc.) • Information on usage *Maximum of seven days' worth of specified users' text chats (Only when E2EE has not been elected and applied and only when receiving an effective warrant; however, video, picture, files, location, phone call audio and other such data will not be disclosed)	• No Message Content • Date and time a user registered • Last date of a user's connectivity to the service	• No Message Content • No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram may disclose IP address and phone number to relevant authorities	• No Message Content • Hash of phone number and email address, if provided by user • Push Token, if push service is used • Public Key • Date (no time) of Threema ID creation • Date (no time) of last login	• No Message Content • Provides account (i.e. phone number) registration data and IP address at time of creation • Message History: time, date, source number and destination number	• No Message Content • Accepts preservation letters and subpoenas, but cannot provide records for accounts created in China • For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active	• Message Content: Limited⁴ • Subpoena: can render basic subscriber records • Court Order: Subpoena return as well as information like blocked users • Search Warrant: Provides address book contacts and WhatsApp users who have the target in their address book contacts • Pen Register: Sent every 15 minutes, provides source and destination for each message ⁴If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content	• No Message Content • Date and time account created • Type of device(s) app installed on • Date of last use • Total number of messages • Number of external IDs (email addresses and phone numbers) connected to the account, but not plaintext external IDs themselves • Avatar image • Limited records of recent changes to account setting such as adding or suspending a device (does not include message content or routing and delivery information) • Wickr Version Number
	SUBSCRIBER DATA	MESSAGE SENDER/RECEIVER DATA	DEVICE BACKUP	IP ADDRESS	ENCRYPTION KEY(S)	DATE/TIME INFORMATION	REGISTRATION TIME DATA	USER'S CONTACTS	

Post Quantum Encryption

Quantum-Secure Cryptography in Messaging Apps



How to build privacy focused apps?



Use full E2EE



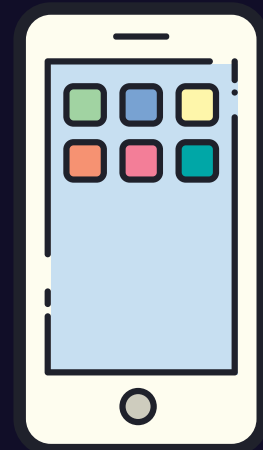
Collect minimum metadata



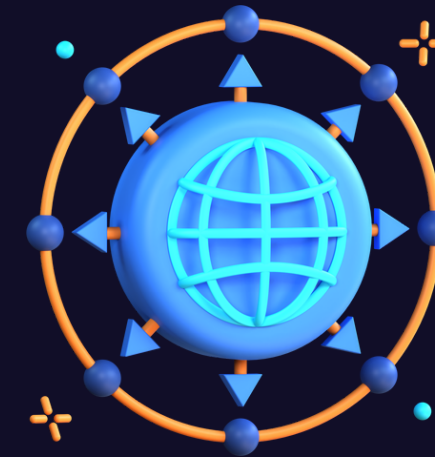
Use secure protocols



**Keep data for a short
period of time**

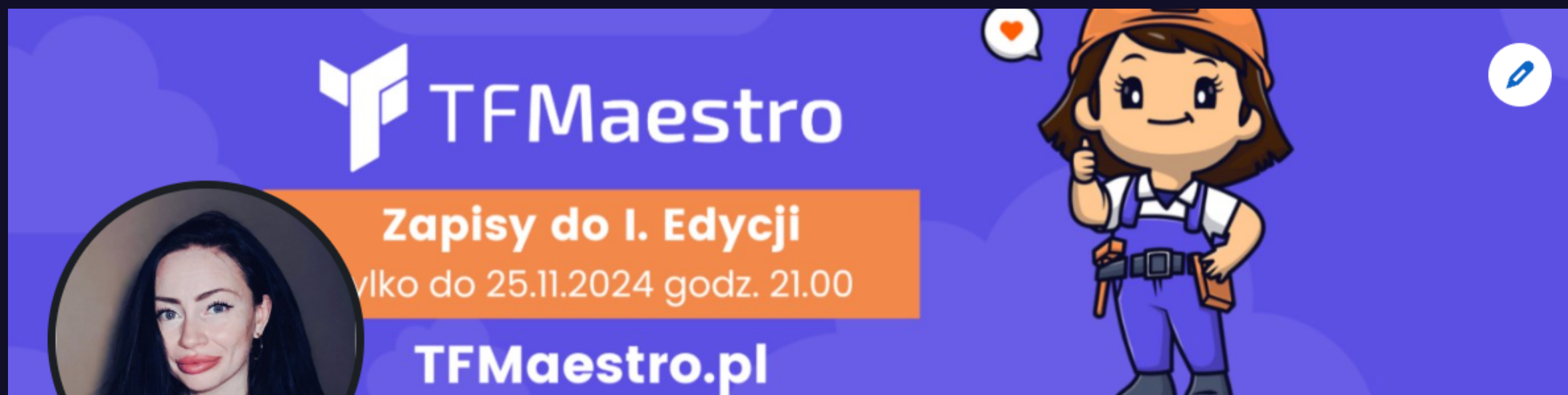


**No phone, email
registration**



**Use decentralized
architecture**

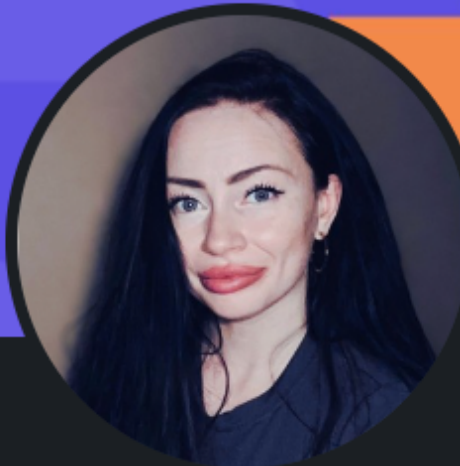
Dziękuję i zapraszam do mojej społeczności!



TFMaestro

Zapisy do I. Edycji
tylko do 25.11.2024 godz. 21.00

TFMaestro.pl

 **Katarzyna Brzozowska** 
Cybersecurity | DevOps | Blockchain | Digital Finances | Privacy
Poznań, Wielkopolskie, Poland • [Contact info](#)

 Be Like Neo & Trinity

Czego nauczysz się z projektu TFMaestro?

Moduł 2
Konfiguracja VPC /
Vnet i dobre
praktyki

Moduł 4
Bezpieczne
przechowywanie
danych na Cloud
Storage

Moduł 5
Bezpieczny dostęp
do maszyn
wirtualnych

Moduł 6
Konfiguracja reguł
firewall

Moduł 9
Tworzenie klastra
K8S i dobre
praktyki

Moduł 12
Wystawienie
aplikacji za load
balancerem

Moduł 14
Zarządzanie
secretami

Moduł 15
Testowanie
bezpieczeństwa
kodu



www.tfmaestro.pl