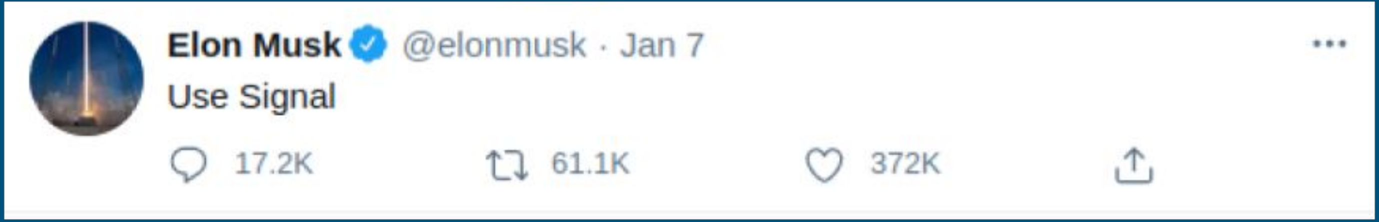
Encrypted Messaging & Society feat. Telegram and Signal

Sabrina Reguyal
INTERFACE 2/7

What's up with Elon's tweet?



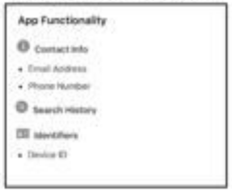
Elon Musk @elonmusk · Jan 7

Use Signal

17.2K 61.1K 372K

Signal
'Data Linked To You'

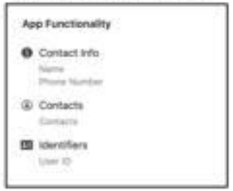
iMessage
'Data Linked To You'



App Functionality

- Contact Info
  - Email Address
  - Phone Number
- Search History
- Identifiers
  - Device ID

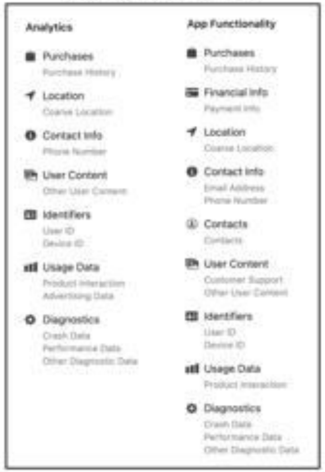
Telegram
'Data Linked To You'



App Functionality

- Contact Info
  - Name
  - Phone Number
- Contacts
  - Contacts
- Identifiers
  - User ID

WhatsApp
'Data Linked To You'



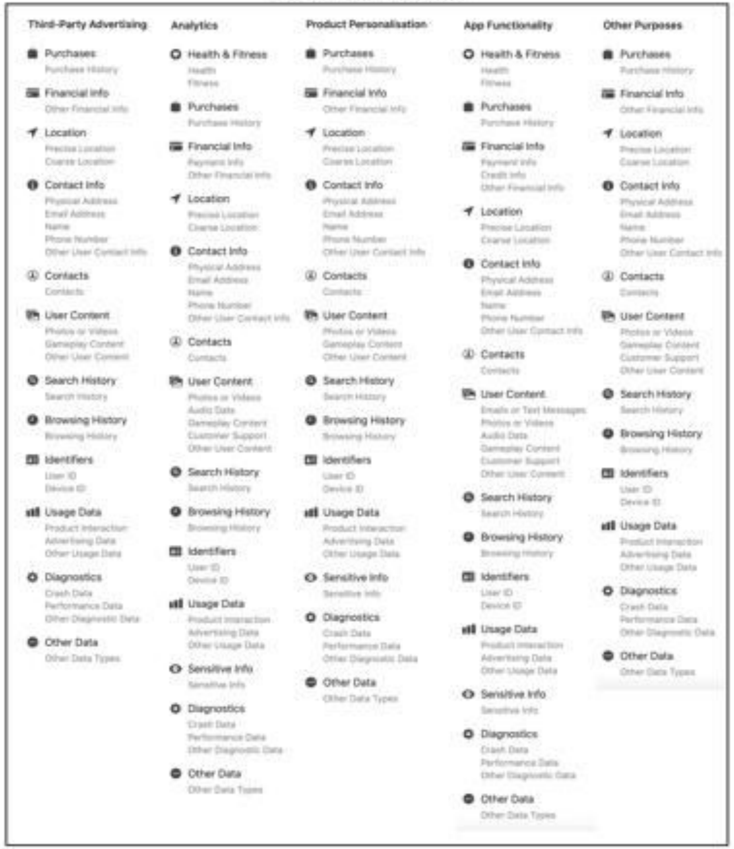
Analytics

- 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
  - 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

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

?%

of people in this meeting believe that complete privacy with respect to personal information and communications is a fundamental(?) human right(?) that must be defended(?).

Areas to investigate

1. What are Telegram and Signal? Who made them? Can we get a sense of their guiding principles?

2. How secure are they?

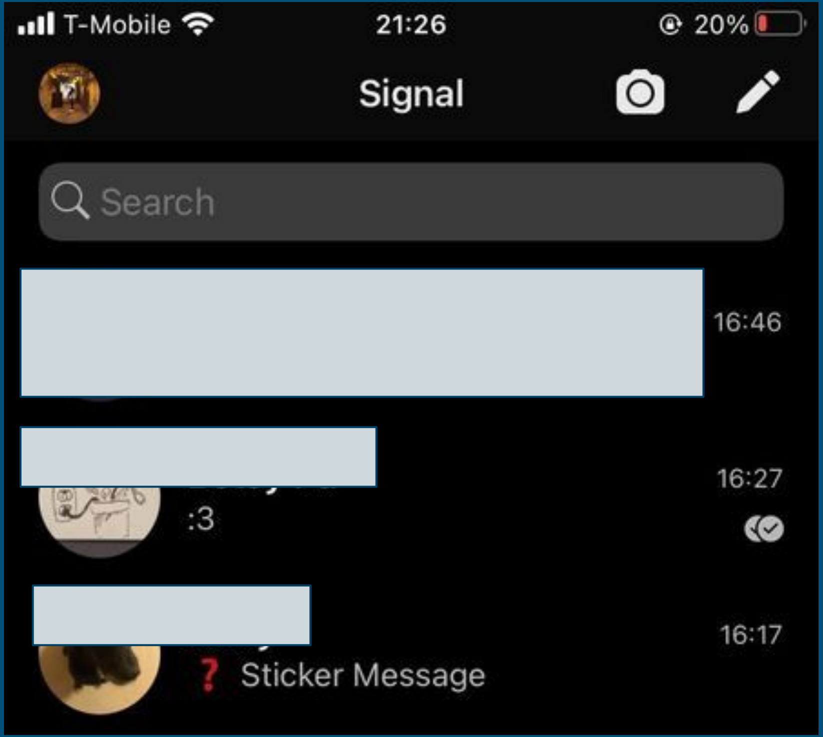
3. Where and how are they used?

4. Vexing questions

Side convos in chat encouraged

Interrupt when you have a question or an important point to add

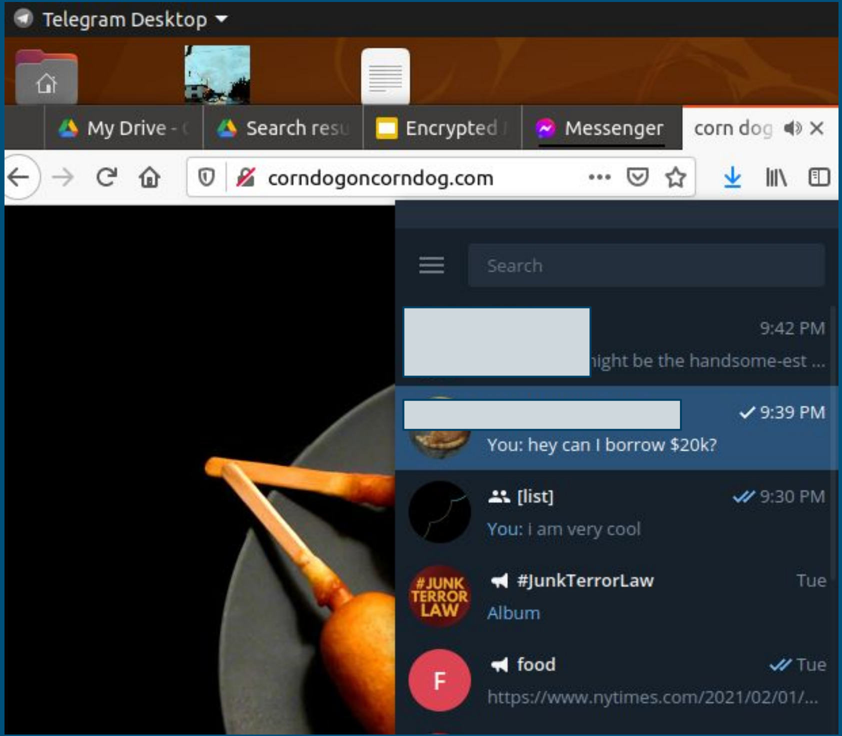
This is what they look like



[redacted] 16:46

[redacted] 16:27
:3

[redacted] 16:17
❓ Sticker Message



[redacted] 9:42 PM
ight be the handsome-est ...

[redacted] ✓ 9:39 PM
You: hey can I borrow $20k?

[list] ✓✓ 9:30 PM
You: i am very cool

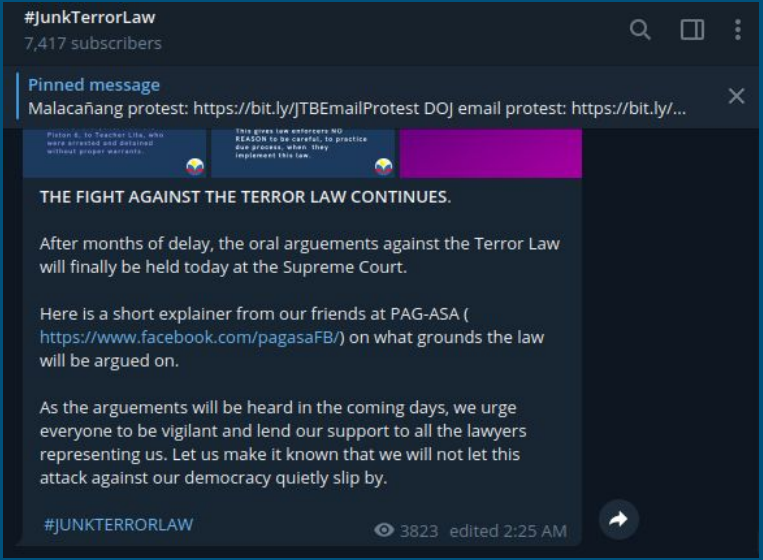
#JunkTerrorLaw Tue
Album

food ✓✓ Tue
https://www.nytimes.com/2021/02/01/...

Telegram

Overview of Features

- Accounts are tied to phone numbers
- Cloud-based messaging with audio, video, photo, and other file-type sharing of up to 2 GB per file
- Secret chats with E2E encryption
- VoIP and videocalls with E2E encryption
- Group chats w/ up to 200,000 members
- Channels: one-way messaging
  - Telegraph: publishing tool
  - view counters
- Reliable on weak internet connections



#JunkTerrorLaw
7,417 subscribers

Pinned message
Malacañang protest: https://bit.ly/JTBEmailProtest DOJ email protest: https://bit.ly/...

Piston 6, to Teacher Lita, who were arrested and detained without proper warrants.
This gives law enforcers NO REASON to be careful, to practice due process, when they implement this law.

THE FIGHT AGAINST THE TERROR LAW CONTINUES.

After months of delay, the oral arguements against the Terror Law will finally be held today at the Supreme Court.

Here is a short explainer from our friends at PAG-ASA (https://www.facebook.com/pagasaFB/) on what grounds the law will be argued on.

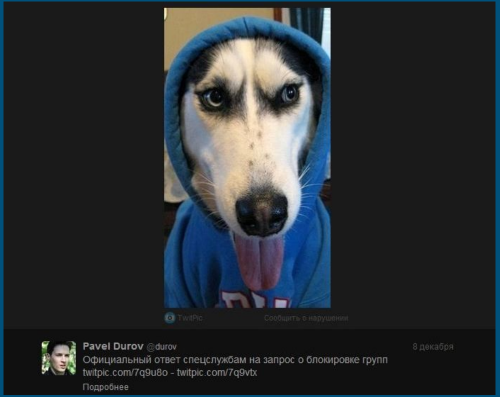
As the arguements will be heard in the coming days, we urge everyone to be vigilant and lend our support to all the lawyers representing us. Let us make it known that we will not let this attack against our democracy quietly slip by.

#JUNKTERRORLAW

3823 edited 2:25 AM

Pavel Durov: One of the guys who made Telegram

Официальный ответ треш-холдингу Mail.ru на его очередные потуги поглотить ВКонтакте



Pavel Durov @durov 8 декабря

Официальный ответ спецслужбам на запрос о блокировке групп twitpic.com/7q9u8o - twitpic.com/7q9vtx

Подробнее

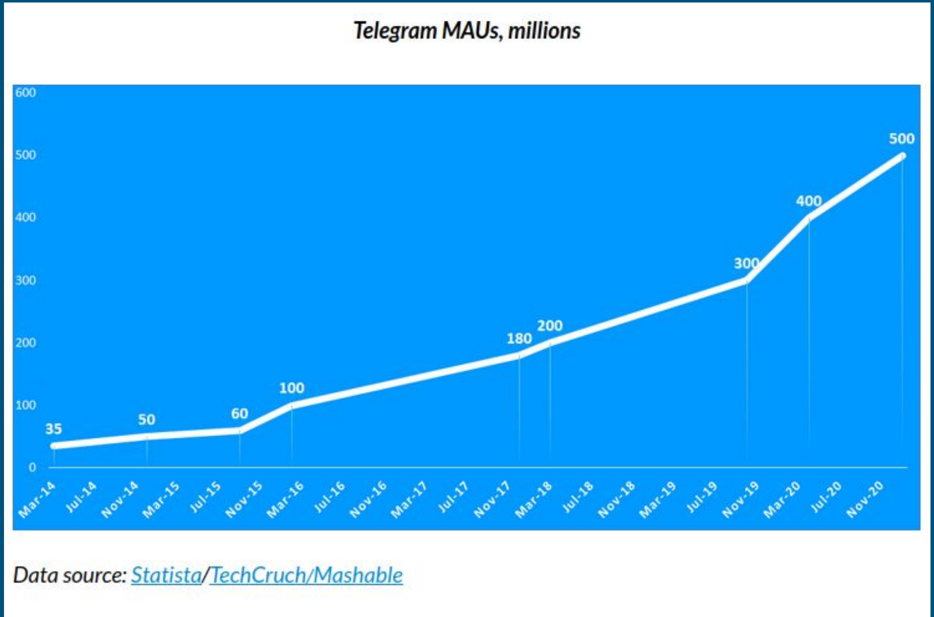
- Founder of VKontakte (aka Russian Facebook, 2006)
  - almost a total rip-off of Facebook
  - refused to delete opposition politician social media pages in 2011; police came to his door
  - was forced to sell VK shares to Mail.ru, removed from position as CEO (2013-14)
- Left Russia; founded Telegram (2013)
- Both of these were done with the help of his brother, Nikolai Durov
- Strong cyber-libertarian vibes

Cyber-Libertarianism

Cyber-libertarianism is “the belief that individuals—acting in whatever capacity they choose (as citizens, consumers, companies, or collectives)—should be at liberty to pursue their own tastes and interests online,” with the goal “to minimize the scope of state coercion in solving social and economic problems and looks instead to voluntary solutions and mutual consent-based arrangements”

- in contrast w/ surveillance capitalism
- Telegram claims to offer freedom through encryption
- Connection to lack of regulation on Russian internet in the early 2000's
- Durov interaction with Zuckerberg: "Mark is an anarchist, but not in terms of denying power and order, but in terms of understanding the outdated nature of the state." The architects agreed that social networks are a superstructure over humanity, allowing information to spread past the centralizing mouthpieces of the state.

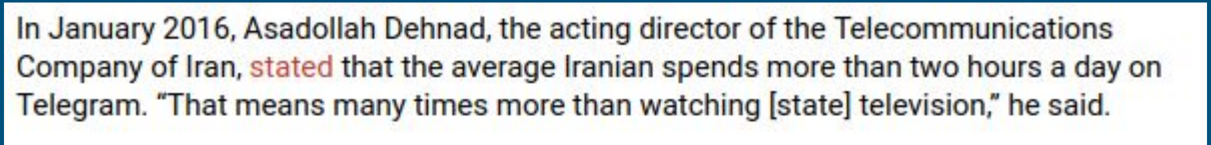
Global Usage of Telegram


Telegram MAUs, millions

Data source: Statista/TechCruch/Mashable

- most popular app in Iran, Uzbekistan, Ethiopia
- significant boosts in Brazil during WhatsApp bans, Hong Kong during protests

The Amad News channel on the Telegram messaging application.

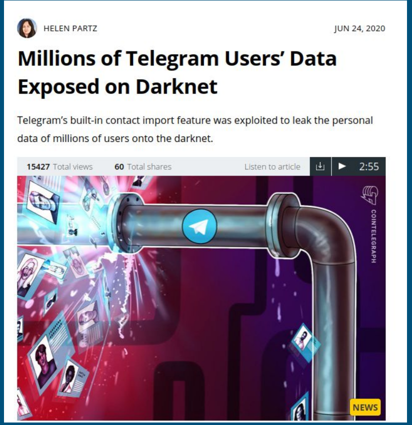

In January 2016, Asadollah Dehnad, the acting director of the Telecommunications Company of Iran, stated that the average Iranian spends more than two hours a day on Telegram. “That means many times more than watching [state] television,” he said.

"Business Model"

- Pavel Durov's wallet
- Telegram cryptocurrency project ended by the SEC
- Possibly shifting in 2021 to Freemium features + advertising channels; Durov claims that all currently free features will remain free
- Registered in several countries; first based in Berlin, now in Dubai

Security Features

- Uses a symmetric-encryption scheme called MTProto, developed by Nikolai Durov
  - based on 256-bit symmetric AES encryption, 2048-bit RSA encryption, and Diffie-Hellman key exchange
  - claim of perfect forward secrecy for secret chats
- Centralized Telegram-specific cloud servers for non-E2E encrypted comms
  - they *say* they've never accessed user chats... but they *could*
- Anti-censorship mechanisms
  - VPN funding
- Roasted by many cryptography experts
  - they ran cracking contests (which are bad) to "demonstrate" security
  - non-trivial number of hacks/vulnerabilities
  - MTProto 2.0, released in December 2017, is better

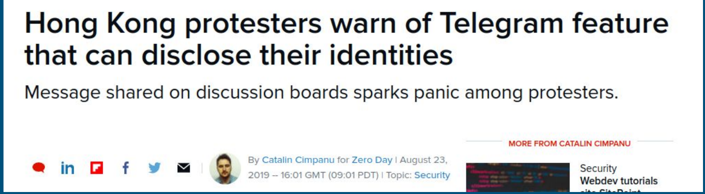


HELEN PARTZ JUN 24, 2020

Millions of Telegram Users' Data Exposed on Darknet

Telegram's built-in contact import feature was exploited to leak the personal data of millions of users onto the darknet.

15427 Total views 60 Total shares Listen to article 2:55



Hong Kong protesters warn of Telegram feature that can disclose their identities

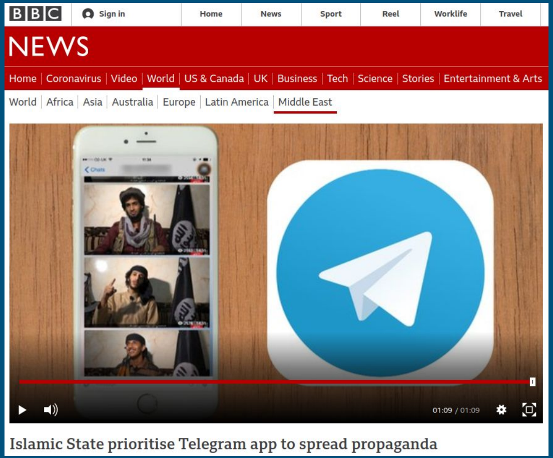
Message shared on discussion boards sparks panic among protesters.

By Catalin Cimpanu for Zero Day | August 23, 2019 -- 16:01 GMT (09:01 PDT) | Topic: Security

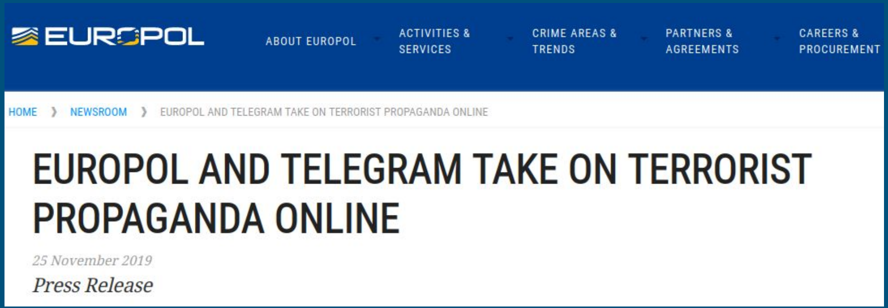
MORE FROM CATALIN CIMPANU

Security
Webdev tutorials

Bad people using Telegram


BBC
Sign in
Home
News
Sport
Reel
Worklife
Travel
NEWS
Home | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Stories | Entertainment & Arts
World | Africa | Asia | Australia | Europe | Latin America | Middle East
01:09 / 01:09

Islamic State prioritise Telegram app to spread propaganda



EUROPOL AND TELEGRAM TAKE ON TERRORIST PROPAGANDA ONLINE

25 November 2019

Press Release

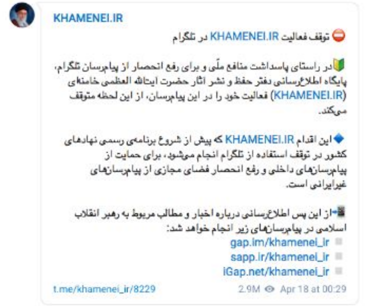
2015: ISIS Telegram channels appear

2019: Europol and Telegram go after ISIS-sponsored channels, deleting up to 200,000 accounts

-other infamous uses of Telegram include distribution of far-right extremist, white supremacist, neo-Nazi content; child and teenage pornography

Iran <3 Telegram except not the Iranian government

- ~40 million Iranians used Telegram as of 2018, penetration of about 58%
  - Replaced many functions of the Internet: email, messaging, discussion forums, blogs, news websites, e-commerce, social networks, television
  - Helped in re-election effort of moderate president Hassan Rouhani in 2017
- April 2018: Iran judiciary announces ban on Telegram
- Internet Service Providers (ISPs) and Telecoms Ministry block access to content
  - extensive disruption to Internet traffic, cloud services
- Mass migration to alternate tools for Telegram
  - Tor, VPNs, Psiphon (resists traffic fingerprinting applied using DPI, emulates common TLS profiles to blend in with ordinary traffic)
- Telegram became the top used app in Iran again on May 27 ^-^
- There was still a chilling effect on speech :<



KHAMENEI.IR

⛔ توقف فعالیت KHAMENEI.IR در تلگرام

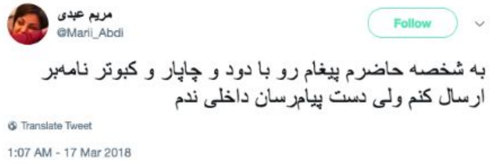
🔰در راستای پاسداشت منافع ملّی و برای رفع انحصار از پیام‌رسان تلگرام، پایگاه اطلاع‌رسانی دفتر حفظ و نشر آثار حضرت آیت‌الله العظمی خامنه‌ای (KHAMENEI.IR) فعالیت خود را در این پیام‌رسان، از این لحظه متوقف می‌کند.

🔹این اقدام KHAMENEI.IR که پیش از شروع برنامه‌ی رسمی نهادهای کشور در توقف استفاده از تلگرام انجام می‌شود، برای حمایت از پیام‌رسان‌های داخلی و رفع انحصار فضای مجازی از پیام‌رسان‌های غیرایرانی است.

📲از این پس اطلاع‌رسانی درباره اخبار و مطالب مربوط به رهبر انقلاب اسلامی در پیام‌رسان‌های زیر انجام خواهد شد:
▫ gap.im/khamenei_ir
▫ sapp.ir/khamenei_ir
▫ iGap.net/khamenei_ir

t.me/khamenei_ir/8229 2.9M 👁 Apr 18 at 00:29

Figure 3. Khamenei's announcement on Telegram that his channel was shutting down and migrating to Soroush instead.



مریم عبدی
@Marii_Abdi

به شخصه حاضرم پیغام رو با دود و چاپار و کبوتر نامه‌بر
ارسال کنم ولی دست پیام‌رسان داخلی ندم

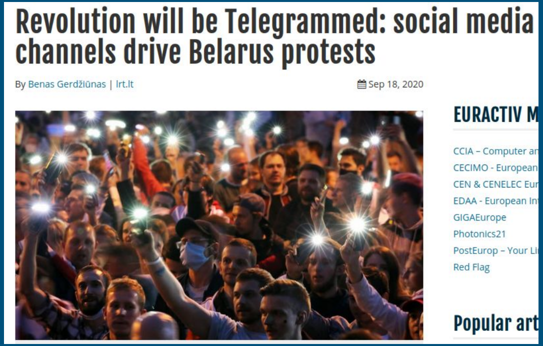
Translate Tweet

1:07 AM - 17 Mar 2018

Figure 4. A tweet by Mariam Abdi, a political activist in Iran reads: "Personally, I would send messages by smoke signals, the pony express, or pigeons before I ever touch domestic messengers."

2020 Belarus Protests

- "Telegram revolution"
- triggered by re-election of President Lukashenko in a highly contested landslide victory on August 9
- August 16: March for Freedom.
    - estimates of over 100,000 attendees



Revolution will be Telegrammed: social media channels drive Belarus protests

By Benas Gerdžiūnas | lrt.lt

Sep 18, 2020

EURACTIV M

CCIA – Computer an

CECIMO - European

CEN & CENELEC Eur

EDAA - European Int

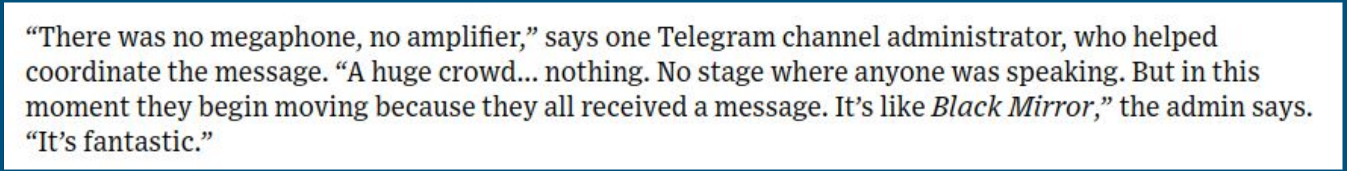
GIGAEurope

Photonics21

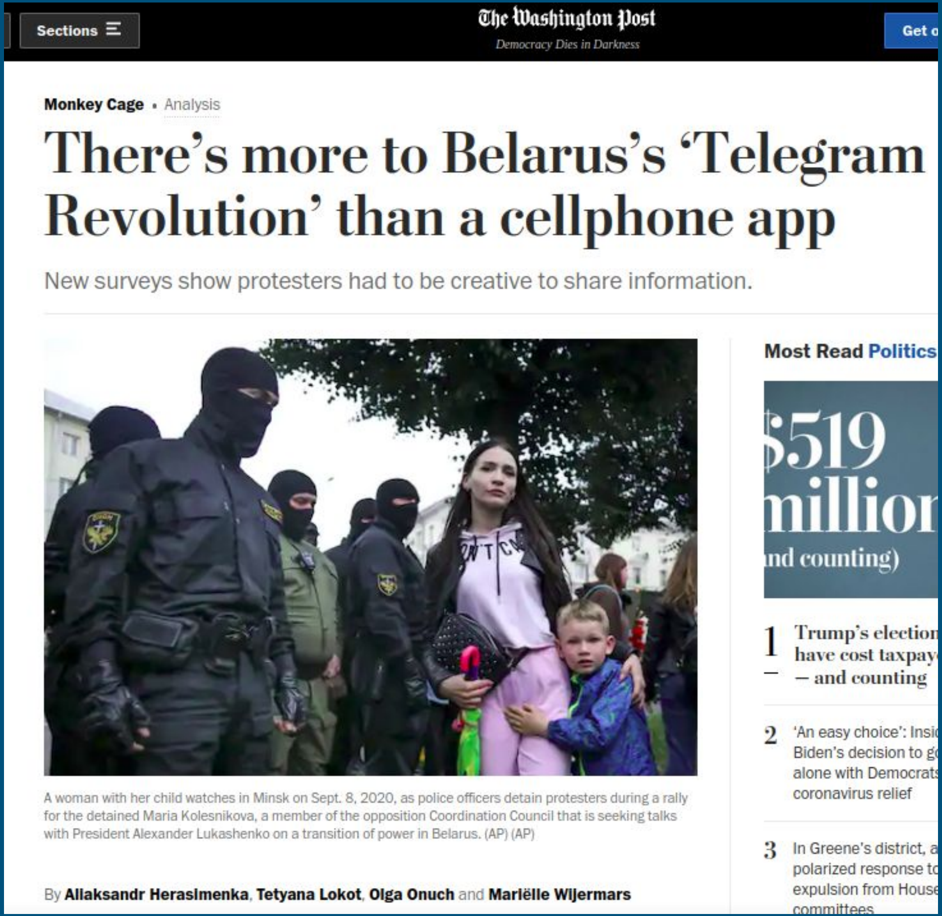
PostEurop – Your Li

Red Flag

Popular art



“There was no megaphone, no amplifier,” says one Telegram channel administrator, who helped coordinate the message. “A huge crowd... nothing. No stage where anyone was speaking. But in this moment they begin moving because they all received a message. It’s like *Black Mirror*,” the admin says. “It’s fantastic.”



Sections ☰

The Washington Post

Democracy Dies in Darkness

Get o

Monkey Cage • Analysis

There's more to Belarus's 'Telegram Revolution' than a cellphone app

New surveys show protesters had to be creative to share information.

A woman with her child watches in Minsk on Sept. 8, 2020, as police officers detain protesters during a rally for the detained Maria Kolesnikova, a member of the opposition Coordination Council that is seeking talks with President Alexander Lukashenko on a transition of power in Belarus. (AP) (AP)

By **Aliaksandr Herasimenka**, **Tetyana Lokot**, **Olga Onuch** and **Mariëlle Wijermars**

Most Read Politics

$519 million
nd counting)

1 Trump's election
have cost taxpay
— and counting

2 'An easy choice': Insi
Biden's decision to g
alone with Democrats
coronavirus relief

3 In Greene's district, a
polarized response to
expulsion from House
committees

Hong Kong Protests + Telegram

- Telegram-based network was cohesive, ensuring efficient spread of information
  - police presence, protest-related events, deliberation
- absence of a single leader
  - more focused on small local communities in contrast to 2014 Umbrella Protests
- cooldown in level of Telegram activity after enactment of National Security Law in July 2020

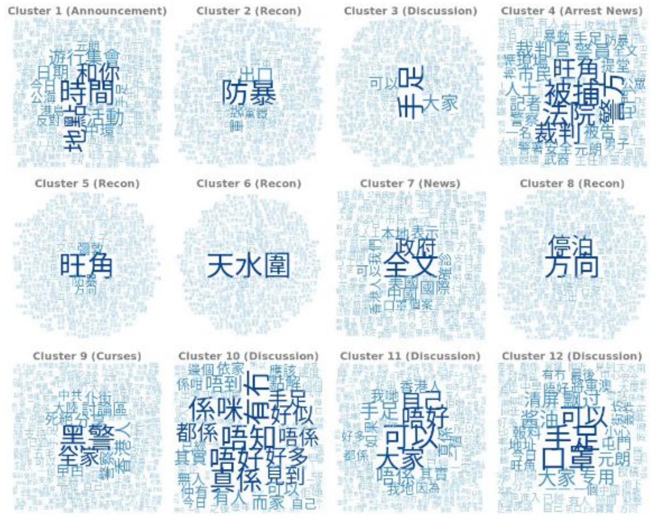


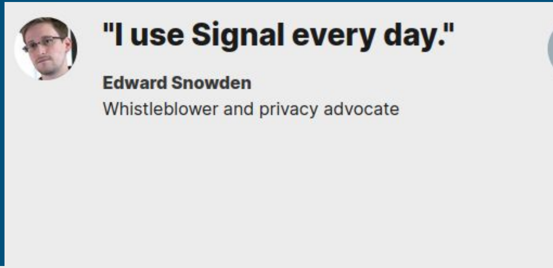
Figure 4. Wordclouds corresponding to 12 topic clusters.

Conclusion

As Joshua Wong and Jason Ng put it in the concluding remarks of their book “Unfree Speech”: “In our case, the night is still young and our journey will get darker and and more perilous before it gets better” (Wong & Ng, 2020).

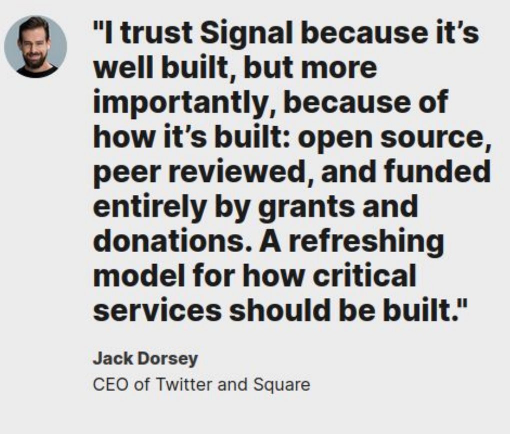
Signal

Other Famous People Besides Elon Like Signal



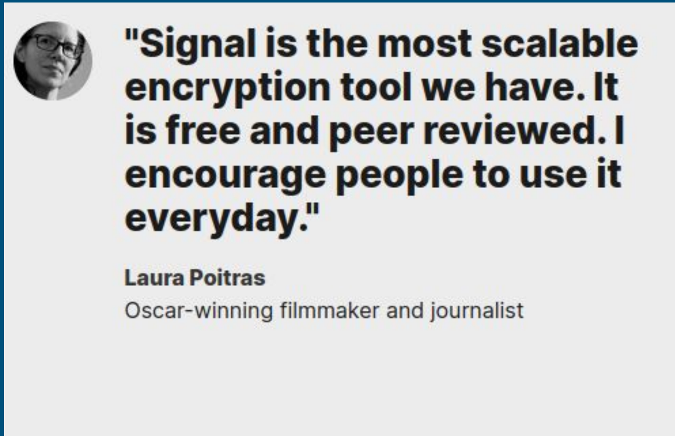
"I use Signal every day."

Edward Snowden
Whistleblower and privacy advocate



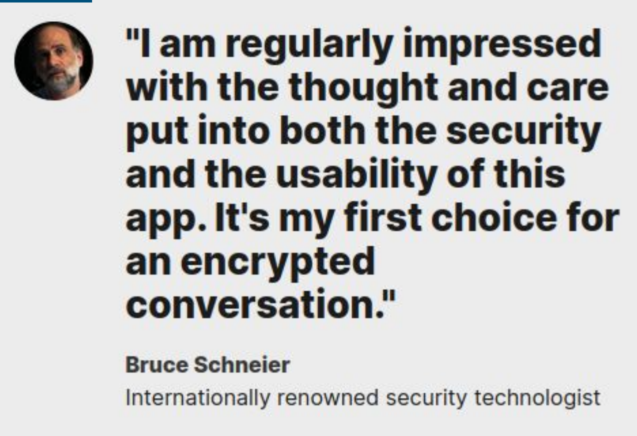
"I trust Signal because it's well built, but more importantly, because of how it's built: open source, peer reviewed, and funded entirely by grants and donations. A refreshing model for how critical services should be built."

Jack Dorsey
CEO of Twitter and Square



"Signal is the most scalable encryption tool we have. It is free and peer reviewed. I encourage people to use it everyday."

Laura Poitras
Oscar-winning filmmaker and journalist

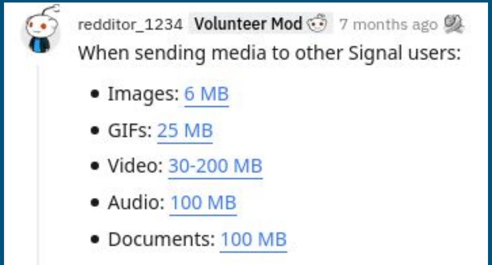


"I am regularly impressed with the thought and care put into both the security and the usability of this app. It's my first choice for an encrypted conversation."

Bruce Schneier
Internationally renowned security technologist

Overview of Features

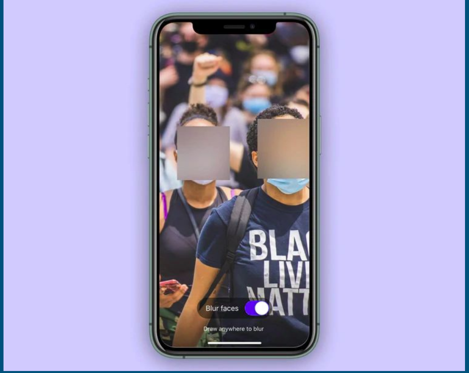
- E2E encrypted individual and group chats (max 8 people).
- Voice and video calls
- File exchange
- Security features: face blur, incognito keyboard, disappearing messages, screen security



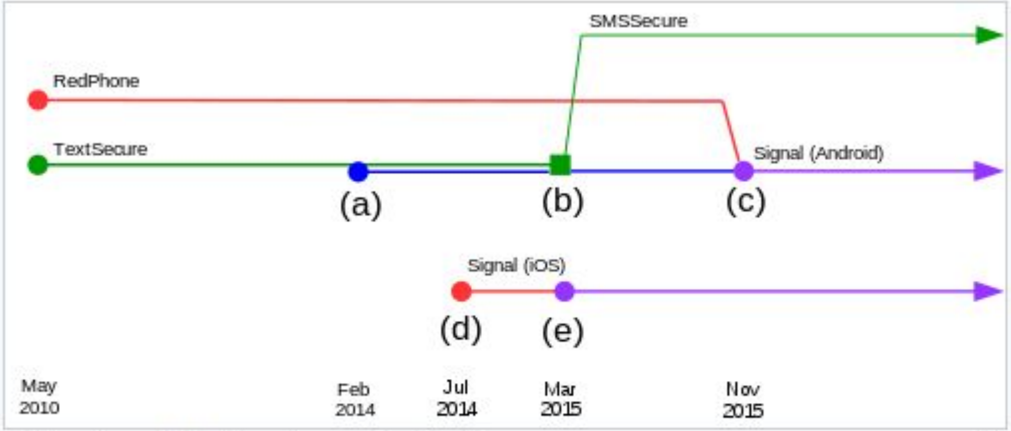
redditor_1234 Volunteer Mod 7 months ago

When sending media to other Signal users:

- Images: 6 MB
- GIFs: 25 MB
- Video: 30-200 MB
- Audio: 100 MB
- Documents: 100 MB



TextSecure (Signal as a baby)



A timeline of the development of TextSecure.
a) Addition of encrypted group chat and instant messaging capabilities.
b) End of encrypted SMS/MMS messaging, which prompted the creation of a fork.
c) RedPhone merged into TextSecure and it was renamed as Signal.
d) Signal as a RedPhone counterpart for iOS.
e) Addition of encrypted group chat and instant messaging capabilities.

- TextSecure born on 25 May 2010 thanks to Moxie Marlinspike and Stuart Anderson
- Feb 2014: new TextSecure protocol = Signal Protocol

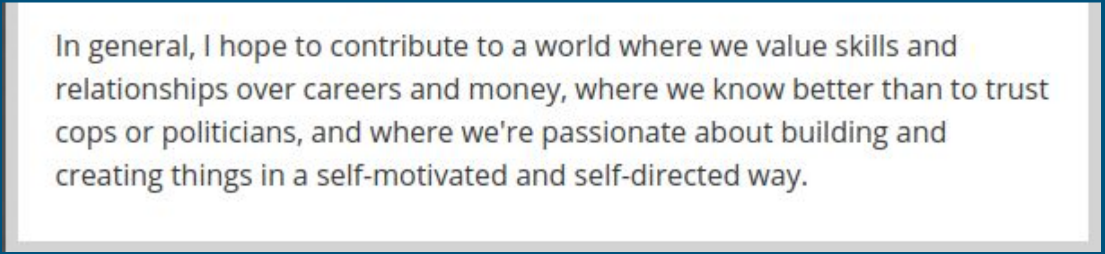
TextSecure's icon from May 2010 to February 2014 and from February 2014 to February 2015.

Signal Foundation

- Founded in February 2018 to "to develop open-source privacy technology that protects free expression and enables secure global communication."
- A 501(c)(3) non-profit organization!
- Signal Messenger LLC: subsidiary dedicated to Signal
- Board of Directors: Brian Acton, Moxie Marlinspike, Meredith Whittaker

Moxie Marlinspike

- Creator of Signal, co-founder of Signal Foundation, CEO of Signal Messenger LLC, co-author of Signal Protocol encryption
- Former head of security team at Twitter
- Avid sailor

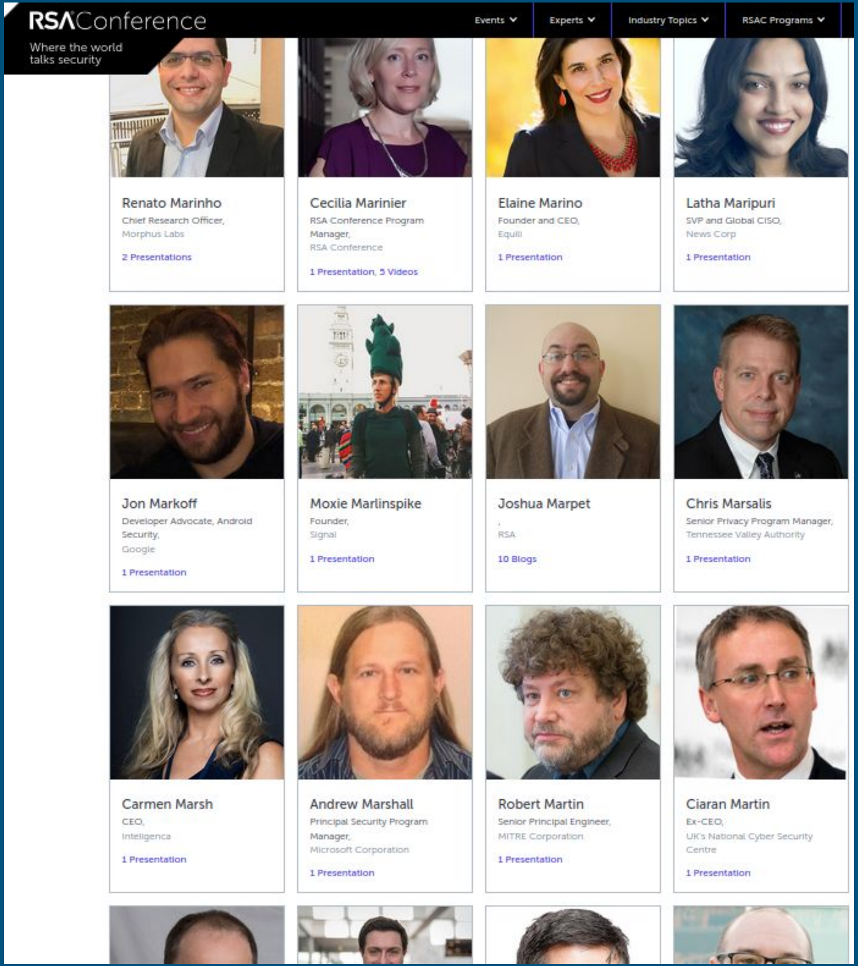


In general, I hope to contribute to a world where we value skills and relationships over careers and money, where we know better than to trust cops or politicians, and where we're passionate about building and creating things in a self-motivated and self-directed way.

from Moxie's personal site ^

Asparagus Dude

@ RSA Conference



Renato Marinho
Chief Research Officer,
Morphus Labs
2 Presentations

Cecilia Marinier
RSA Conference Program Manager,
RSA Conference
1 Presentation, 5 Videos

Elaine Marino
Founder and CEO,
Equili
1 Presentation

Latha Maripuri
SVP and Global CISO,
News Corp
1 Presentation

Jon Markoff
Developer Advocate, Android Security,
Google
1 Presentation

Moxie Marlinspike
Founder,
Signal
1 Presentation

Joshua Marpet
,
RSA
10 Blogs

Chris Marsalis
Senior Privacy Program Manager,
Tennessee Valley Authority
1 Presentation

Carmen Marsh
CEO,
Inteligenca
1 Presentation

Andrew Marshall
Principal Security Program Manager,
Microsoft Corporation
1 Presentation

Robert Martin
Senior Principal Engineer,
MITRE Corporation
1 Presentation

Ciaran Martin
Ex-CEO,
UK's National Cyber Security Centre
1 Presentation

Anarchism

Most people who use social networks and chat services, he argues, assume that their digital communications are private; they want to share their thoughts and photographs with their friends—not with Facebook and Google, not with advertisers, and certainly not on the dark Web. “In a sense, I feel like Signal is just trying to bring normality to the Internet,” he said as we sat on a patch of grass near the beach. “A lot of what we’re trying to do is just square the actual technology with people’s intent.”

He talked about the “diabolical” ways that the Internet has eroded the barrier between our personal and professional identities. “People who aren’t even professional writers have to consider that their communication is being consumed,” he told me. “Anything that I’ve ever written or created, one way or another, about anything is sort of embarrassing to me a month later. Even more so five years later.”

“As people start to tell you who you are, you start to be boxed in by that impression. I think that’s something Moxie has actively resisted, with a lot of energy.”

He spent much of his youth immersed in anarchist literature and communities, and anarchism’s inherent critique of authority is still important to him. This orientation is unusual in the tech world, although its right-wing analogue, libertarianism, is pervasive. “Liberalism basically says that we should all be free to talk about the world we want, and then we have a marketplace of ideas that we can select from,” he said. “I think anarchism’s comment on that is it’s not enough just to talk about things—that you can’t actually know unless you experience or experiment with something.”

Privacy vs. Crime

Enforcing laws, Marlinspike believes, should be difficult. He likes to say that “we should all have something to hide,” a statement that he intends not as a blanket endorsement of criminal activity but as an acknowledgment that the legal system can be manipulated, and that even the most banal activities or text messages can be incriminating. In his view, frequent lawbreaking points to systemic rot. He often cites the legalization of same-sex marriage and, in some states, marijuana as evidence that people sometimes need to challenge laws or engage in nominally criminal activity for years before progress can be made. “Before, it was inconceivable,” he said. “After, it was inconceivable that it was ever inconceivable.”

Privacy, he says, is a necessary condition for experimentation, and for social change... “If I’m dissatisfied with this world—and I think that I might be—a problem is that you can only desire based on what you know,” Marlinspike said. “You have certain experiences in this world, they produce certain desires, those desires reproduce the world. Our reality today just keeps reproducing itself. If you can create different experiences that manifest different desires, then it’s possible that those will lead to the production of different worlds.”

2016 Subpoena

- Assistant attorney in Virginia requested email addresses, history logs, browser cookie data, other info associated w/ two phone numbers
- Only supplied registration date and last date one of the numbers was used

The Point of Signal

“Signal’s mission has always been to make end-to-end encryption as ubiquitous as possible, rather than a commercial success”

- Marlinspike

Security

- Signal protocol
    - combines the Double Ratchet Algorithm, prekeys, and a 3-DH handshake. It uses Curve25519, AES-256, and HMAC-SHA256 as primitives.
    - client-server connections protected by TLS
    - open-source !

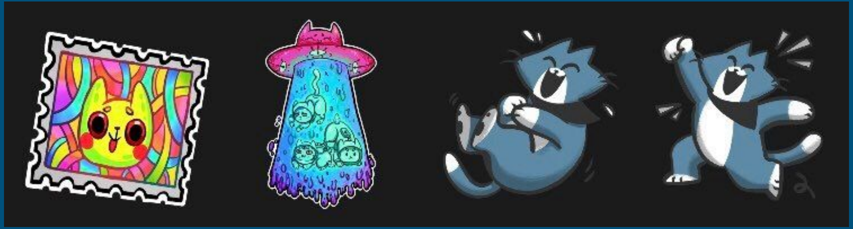
Use in Social Movements

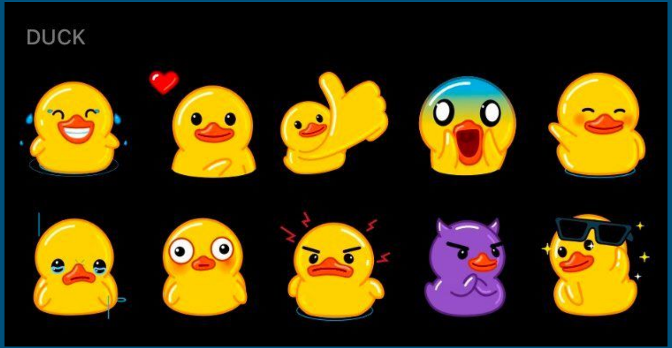
- Has become particularly prominent in the wake of the 2020 BLM protests and the June 2020 Hong Kong national security law
- App downloads:
  - week before George Floyd's death on 5/25/20: 51,000 first-time users
  - following week: 78,000 new downloads
  - first week of June: 183,000 new downloads

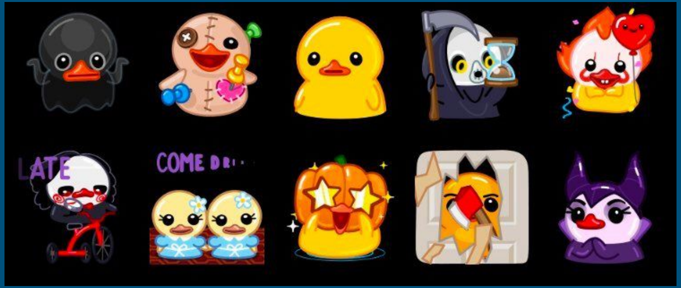
Use by bad people

- 2016: Authorities in India arrest members of suspected ISIS-affiliated terrorist cell that communicates via Signal and Telegram
- Used for organizing by far right, right-wing militias, white nationalists
    - Unite the Right II rally in 2018 that was not well-attended

Some of my favorite stickers on each






LATE
COME DR