

From Russia With Crypto: A Political History of Telegram

*in Use Signal, Use Tor?
The Political Economy of Digital Rights Technology*

Nathalie Maréchal, PhD 2018
University of Southern California
Annenberg School for Communication and Journalism
@MarechalPhD

What is Telegram?

- Smartphone & desktop app combining messaging (encryption optional) with elements of social media (Channels)
- Privately owned by Durov brothers, legal structure hidden by a network of shell companies
- Peculiar business model: self-funding + cryptocurrency scheme
- Cypherpunk libertarianism combined with idiosyncratically Russian understanding of politics



The Brothers Durov, from Vkontakte to Telegram

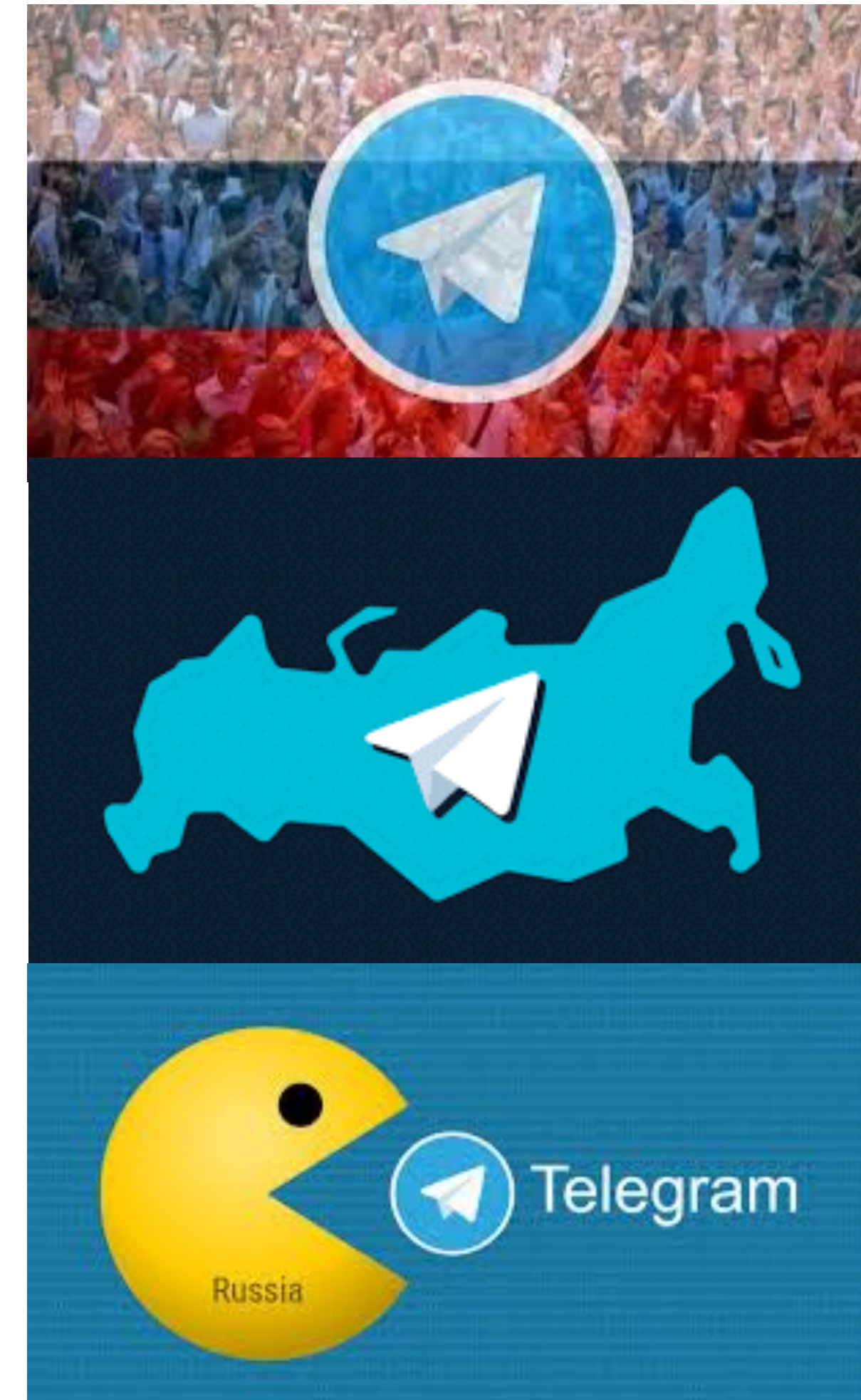
- VK — Facebook copycat
- Telegram created in reaction to Kremlin crackdown
- Forcible buy-out & exile
- Telegram launched in August 2013, benefitting from WhatsApp's acquisition by Facebook



The image shows a screenshot of Pavel Durov's profile on the VKontakte social media platform. The profile header includes the VK logo, the name "Pavel Durov" with a verified checkmark, and the text "last seen today at 2:54 pm". Below the header is a large profile picture of Pavel Durov. To the left of the profile picture is a login/sign-up form with fields for "Phone or email" and "Password", and buttons for "Log in" and "Sign up". Below the form is a link for "Forgot your password?". To the right of the profile picture, it says "157 posts". Below that is a post by Pavel Durov with a text description in Russian. The post text discusses his resignation from VKontakte and the company's transition to new management. At the bottom of the post, it shows engagement metrics: "Yesterday at 10:50 pm" with 31770 comments and 123773 likes. Below the post, there is a section for "Noteworthy pages" showing "52 pages".

Telegram's Russian roots

- Telegram is the product of its founders' contentious relationship with the Russian state
- Information & internet as a threat to political elites
- Information controls intensifying since 2012
- 2016 Yarovaya laws, including requirement to preemptively make decryption keys available to authorities
- Telegram banned and (sort of) blocked in April 2018



Ideology

- Cyber-libertarian
- Cypherpunk
- Rejection of the nation-state
- Commitment to privacy & rejection of surveillance capitalism
- Unaccountable to anyone except Pavel Durov himself



Crypto controversial

- Reputation as the terrorist's app of choice
- “Secret chats” not enabled by default
- They rolled their own crypto
- Only sort-of open source



The Telegram ICO

- Telegram was self-funded by Durov until this year (USD\$300 million from VK sale)
- “Pre-sales” brought in USD\$1.7 billion, then the ICO itself was cancelled
- Intended to fund the development of the Telegram Open Network
- White Paper promises a cryptocurrency (the “Gram”) and in-app marketplace, encrypted file storage & more.



Conclusion

- Cyber-libertarianism vs. human rights
- Control vs. accountability
- Cypherpunk, open-source optional ?



Thank you!

Data, Sources, & Methods

- Content analysis of Telegram's publications (including website) & public statements by the Durov brothers
- Secondary sources (academic & popular)
- Interviews with encryption experts
- "Walk-through method" (Light et al. 2016)