THE MISSING DETAIL ABOUT ENCRYPTION IN THE PAVEL DUROV INVESTIGATION

Yesterday, France charged Pavel Durov and set €5 million bail for the Telegram founder. The public release regarding the charges provides scant new detail from what prosecutors released when he was first arrested.

For example, the new release confirms that a preliminary inquiry started in February, before the formal investigation was started on July 8. That's consistent with a Politico report that France first issued arrest warrants for Pavel and his brother, Nikolai, subsequent to an investigation into someone using Telegram to engage in child sexual abuse, including rape.

> Warrants for Pavel and his brother Nikolai, the platform's co-founder, were issued on March 25 over charges including "complicity in possessing, distributing, offering or making available pornographic images of minors, in an organized group." French media had previously reported the probe was opened in July.
>
> The warrants were issued after an undercover investigation into Telegram led by the cybercrime branch of the Paris prosecutor's office, during which a suspect discussed luring underaged girls into sending "self-produced child pornography," and then threatening to release it on social media.
>
> The suspect also told the investigators he had raped a young child, according to the document. Telegram did not respond to the French authorities' request to identify the suspect.

The list of charges in the release yesterday does not exactly match those released last week. The lead charge, "web-mastering an online platform in order to enable an illegal transaction in organized group," is further described as a crime that carries a 10-year sentence and/or a €500,000 fine. Given how particular French code is about punishment, one might be able to hone in what lead crime that language is pursuing (it seems more common for five year sentences to match a €150,000 fine).

In addition to listing Telegram's refusal to cooperate with law enforcement requests second among suspected crimes, as the original release did, yesterday's release has that bolded below, with a description of how other authorities, including Belgium, are having the same problem. This investigation seems to primarily stem from the way Telegram has allowed crimes to flourish on the platform, and as such, most of the rest of the charges *may* reflect efforts to further criminalize Durov's choice to do nothing about crimes that rely on Telegram.

There are other changes between the initial release and yesterday's, which may be of little or no import or may reflect what prosecutors have learned since they arrested Durov. For example, *possessing* (as distinct from disseminating) CSAM images has been dropped; that's the kind of change that might reflect the server configuration Telegram uses, and whether any Telegram server hosts CSAM material *within* France.

Criminal association has now been included in the general list, rather than as a separate bullet point. Money laundering, however, has not. One unanswered question is whether Durov was more directly involved in money laundering than the other crimes, in which case prosecutors might show that he had a personal pecuniary incentive to let all the other crime flourish on Telegram.

In that same general list, the dissemination of hacking tools was moved up to first, from

fourth.

But one of three encryption-related crimes, "Importing a cryptology tool ensuring authentication or integrity monitoring without prior declaration," was dropped. Again, that *could* reflect new information about server locations.

It's the commentary regarding the (now two) encryption-related crimes that most befuddles me. The American press, at least, continues to discuss this as if this is a crime about *using* encryption.

> Some online speech experts and privacy advocates agreed that France's indictment of Durov raises concerns for online freedoms, pointing in particular to charges relating to Telegram's use of cryptography, which is also employed by Apple's iMessage, Meta's WhatsApp and Signal.
>
> "French law enforcement has long hated encryption," said David Kaye, a professor at University of California, Irvine School of Law and former U.N. special rapporteur on freedom of expression. "This seems like a potential avenue for them to blame what happens on Telegram at least in part on encryption, when the truth is that the other counts suggest that Telegram's noncooperation with judicial orders is the real problem."
>
> Stamos agreed the charges related to cryptography are "concerning," because "that seems to apply even to platforms that are actively working to prevent the spread of child sexual abuse material." He said that while Telegram has at times banned groups and taken down content in response to law enforcement, its refusal to share data with investigators sets it apart from most other major tech companies.

As far as I understand it, the law in question is one passed in 2004 that required affirmative *registration* of encryption. Signal, easily the most protective encrypted messaging app, *did* register under this law when it first applied to offer Signal in French app stores. So, no, they're not going to be prosecuted under that law, because they're following the law.

And therein lies the question I keep asking but people are ignoring: whether this law works like the affirmative registration requirements in the US for acting as a foreign agent. The US uses 18 USC 951, for example, to prosecute people who are secretly doing things for a foreign government — such as the targeting for which Maria Butina was prosecuted — without having to prove they were affirmatively spying. DOJ didn't have to prove that Butina (speaking purely hypothetically here) honey trapped Patrick Byrne as part of a Russian effort to recruit nutballs with an investment in cryptocurrency; they could instead prove merely that she was taking orders from a government official (in this case, Alexandr Torshin), without alerting DOJ to that fact. The obligation to register provides a law enforcement tool that can be used when an underlying crime — like spying — is far more difficult to prove, or would harm counterintelligence if one tried.

For example, 18 USC 951 was used in the failed prosecution of Mike Flynn and his business partner, Bijan Kian. it wasn't until the eve of the Kian's trial that DOJ revealed the existence of, but not the details about, far more extensive communications pertaining to Flynn and the Turks (that revelation did not explain whether these were communications between Flynn and the Turks, and/or communications the Turks had about Flynn) than had previously been revealed.

I don't know if this is how France uses this law, or if they may be doing here. What I'm saying is that the crime is failing an affirmative obligation to register, a law that

has not prevented Telegram's counterparts from operating lawfully in France.

Let me extend the analogy to a case where we know Telegram was used to facilitate crime (though not one of the crimes in which Durov has been charged with complicity).

As I laid out here, we know that after January 6, the FBI discovered that the Proud Boys were using unencrypted Telegram group chats to organize in advance of the insurrection. But once it obtained and exploited Enrique Tarrio's phone, which took over a year to do, the FBI also discovered that Tarrio was using Telegram (in addition to Google Voice chat and iMessage) to communicate with a DC intelligence cop, Shane Lamond. Those encrypted communications will be key evidence in Lamond's trial in October, but the use of Telegram, whether encrypted or not, was not a crime and not charged as one.

Those Telegram communications include:

- The message where Lamond was added to an unencrypted Proud Boys chat (meaning, of course, that a cop with close ties to the FBI did know how the Proud Boys were using Telegram long before January 6, and indeed Tarrio tried to use his comms with Lamond as an affirmative defense to the sedition charges against him).
- Private unencrypted Telegram messages that at least started as Lamond's effort to learn what the Proud Boys were doing ahead of time, and so fell squarely within Lamond's job as an

intelligence officer, but which — after the election — started to include advice about how to avoid law enforcement scrutiny.

- Starting after the December 12, 2020 burning of a DC Church's BLM flag, secret, encrypted Telegram messages about Tarrio's role in that act and the investigation into him for it; those encrypted communications would later include discussion of the planning and aftermath of January 6.
- Telegram calls about the investigation that could not be reconstructed (though some conducted with his replacement phone may have been).
- Starting on December 22, encrypted Telegram messages with the auto-delete set; the FBI was able to reconstruct some, but not all, of these. Among those they weren't able to reconstruct, a January 4, 2021 encrypted text successfully destroyed must have alerted Tarrio that DC had obtained a warrant for his arrest, because Tarrio immediately told some girlfriends and Jacob Engels

> via unencrypted Telegram texts, as well as some Proud Boy Telegram group chats, that about the arrest warrant. The men appear not to have tried to delete Tarrio's self-exonerating encrypted Telegram text, "I could have stopped this thing." But they did resume destroying encrypted Telegram messages as the investigation into the Proud Boys progressed.

That use of Telegram, whether unencrypted, encrypted, and/or self-deleting, is not illegal in the US. Rather than busting Lamond for that, prosecutors charged him for lying about the earlier communications, for obstructing the investigation into burning the BLM flag. There's no charge related to Lamond's warnings about January 6, and indeed, the reconstruction or not of later texts between the men is not included in the trial exhibit. But more of the January 6 texts were successfully destroyed.

Now consider the significance of a case where cops knew a militia group were using Telegram's unencrypted features, ones the FBI could have hacked, but that collusion between the militia and law enforcement was hidden via the use of Telegram's encryption. The FBI wasn't looking in any case, but even if they had been, it is at least conceivable where a seditionist like Tarrio used better operational security and didn't immediately undercut the value of using encryption by blabbing to others, but that the encryption prevented the FBI from understanding the extent that the cops were helping the seditionists.

The use of Telegram is not illegal in the US. As I understand it, the *use* of it is not being

charged in France.

But in France, the requirement to pre-register provides a tool prosecutors might choose to use if the use of encryption ends up playing a detrimental role in crimes in the country, as Telegram notoriously has.

I have no idea whether that's how it's being used here.

But it is at least possible that Durov is being charged under these two encryption crimes because criminal (or intelligence) investigations in France discovered, via exploiting suspects' phones or possibly even with the help of a cooperating witness, that Telegram encrypted chats played a key role in one or another particular plot. That could have been nothing more than the child sexual abuse whence this investigation started. Or it could be something that raised the stakes for France, such as sabotage attempted by a foreign power.

Pavel Durov is being charged because communications to which Telegram had ready access were used to commit a number of crimes (but not, notably, hate crimes). Far too many outlets are describing these crimes as pertaining to encryption; it may not be. It pertains to the commission of crimes, using Telegram, including a great number that Telegram allegedly had means to learn about but, by refusing law enforcement process, sustained deniability.

It appears that he is also being charged because he made it possible to further protect communications, including from Telegram engineers, without following French registration laws before he did that. That is, France *appears* to be charging Durov not because he knows what the encryption is serving to hide, but by dint of his failure to adhere to French registration requirements, his plausible deniability regarding encryption doesn't help him dodge criminal liability.

I may be misunderstand the law — I'm still

looking for French sources to explain this, because American ones are not citing French lawyers — but if people are writing about the role of encryption in this case, the difference between “providing” encryption and “providing it without registration” is key.

Update: Since we’re focused on Telegram’s non-cooperation with law enforcement, this exhibit list for Lamond’s trial shows how they have to authenticate those comms instead: Through a variety of forensic reports, and then via summary chart.