# EXPERT OPINION

## EVALUATION OF THE ARGUMENT THAT THE BYLOCK APPLICATION HAS BEEN USED EXCLUSIVELY

This expert opinion has been prepared under Paragraph 6 of Article 67 of the Code of Criminal Procedure No. 5271 by examining and assessing from a technical and legal perspective the questions conveyed to us or raised by a number of people who were suspects/defendants (client) at ongoing investigations/trials or by their lawyers.

"The ongoing debates at the proceedings involving the charge of using the ByLock mobile communication application focus on whether the application in question was used "exclusively," i.e., it was used solely by FETÖ/PDY (Fethullahist Terrorist Organization / Parallel State Formation) members and non-members were unable to use it. In this context, answers to the following questions were sought:

i. What is an encrypted communication application? Is it rare for communication applications to be encrypted? If a communication application is encrypted, does this prove beyond reasonable doubt from a technical perspective that the application is for exclusive use?

ii. Was it possible to use the ByLock application by downloading it from the app stores for mobile devices running Android or iOS operating systems? Was a third party's reference needed in order to download and use the application? Was there any obstacle to its being used by downloading it from app stores?

iii. The following arguments have been made to prove the exclusiveness of the application. It has been requested that the following arguments should be evaluated individually in order to demonstrate if it is possible to prove beyond reasonable doubt from a technical perspective that the ByLock application is for exclusive use and to determine if there are other applications with similar characteristics listed in these arguments. The arguments in question are as follows:

a. The developers of the application are FETÖ/PDY members.

b. The application does not have a corporate website.

c. The application has not resorted to advertising, etc. for promotion and it has exerted no effort to boost the number of its users.

d. In order to download and install the application, the Google Play Store and Apple App Store stores and websites as well as flash disks/pendrives, SD cards or Bluetooth can be used.

e. The application does not authenticate the user ID indisputably. It is not mandatory to have an e-mail address or GSM line in order to register with the application. Using the application without authentication is supported.

f. The application allows users to use any username they may chose.

g. The application does not use the user's address book. The user creates his/her own address book.

h. The application does not allow the user to find other users by searching based on certain criteria (phone number, username, e-mail address, etc.) Users who want to communicate using the application have to contact each other beforehand and accept the request for mutual communication.

i. The application does not offer any password recovery option to be used in case of forgotten passwords.

j. The application uses self-signed certificates instead of digital certificates generated by certificate authorities.

k. The application automatically deletes messages.

l. The use of a VPN was made mandatory for signing in the application from Turkey after a certain date.

m. The ByLock application was shut down without informing its users.

iv. Is it possible to determine beyond reasonable doubt from a technical perspective that an application that can be downloaded, installed and used from mobile app stores was for exclusive use?

v. What are needed in order to determine beyond reasonable doubt from a technical perspective that the ByLock application has been used?"

The questions/requests have been answered/evaluated from a technical and legal perspective within the framework of an expert opinion.

While this is a work describing an expert opinion, the examination has been conducted with impartiality that can be seen in (court-appointed) expert reports and the technical data were presented in a way to portray the concrete facts.

This expert opinion, prepared by us, is presented for the appraisal of courts/tribunals if submitted by suspects/defendants at investigations/trials or by their lawyers.

With regards, September 1, 2021

**T. Koray PEKSAYAR**
Digital Forensics Expert
Engineer (MS)

**Dr. Levent MAZILIGÜNEY**[1]
Digital Forensics Expert
Engineer (MS, Ph.D.)

[1] Dr. Levent Mazılıgüney, a lawyer by profession, is also an engineer (MS, Ph.D.) and Digital Forensics Expert. He has co-authored and undersigned this expert opinion with his colleague within the framework of his Digital Forensics Expertise.

**Technical Evaluation**

i. *"What is an encrypted communication application? Is it rare for communication applications to be encrypted? If a communication application is encrypted, does this prove beyond reasonable doubt from a technical perspective that the application is for exclusive use?"*

1. "Encrypted" generally means "protected by a password." A basic security concern with messaging applications is the possibility that third parties other than messaging parties, namely the corporations behind the applications in question or the government bodies that collect informations of their citizens or any individual(s) seeking to have access to communication content for any reason, may read private messages. Virtually all communication applications use methods with varying degrees of encryption in an effort to prevent the access of third parties to communication content. It is a widespread method to use encryption in order to prevent manipulation of electronically circulating communication content by eliminating the possibility of its being heard, changed, added or deleted.

2. All commonly used mobile communication applications (WhatsApp, Telegram, Skype, Signal, BİP, etc.) provide encrypted communication at varying degrees. There is no widely used mobile communication application that does not use encryption.

3. If a communication application is encrypted, this does not prove beyond reasonable doubt from a technical perspective that the application in question is for exclusive use.

4. Encryption of communication is generally a legal requirement. Communication content represents personal data, and mandatory protection and destruction policies for the transfer of data are recommended in national or international legislation.

ii. *"Was it possible to use the ByLock application by downloading it from the app stores for mobile devices running Android or iOS operating systems? Was a third party's reference needed in order to download and use the application? Was there any obstacle to its being used by downloading it from app stores?"*

5. Based on the information obtained from publicly available sources, it can be said that it was possible to use the ByLock application by downloading it from Google Play Store between April 2014 and March 2016 and from Apple App Store between April 2014 and September 2014.

6. It is possible to download the Android application package file with the "apk" extension for the ByLock application from the publicly available sources and test it on a virtual machine. Any reference from any third party was not needed to download and use the ByLock application (other than the user and the application).

7. There was no obstacle or restriction to users' downloading and using the ByLock application from mobile app stores.

iii. *The following arguments have been made to prove the exclusiveness of the application. It has been requested that the following arguments should be evaluated individually in order to demonstrate if it is possible to prove beyond reasonable doubt from a technical perspective that the ByLock application is for exclusive use and to determine if there are other applications with similar characteristics listed in these arguments. The arguments in question are as follows:*

*a. The developers of the application are FETÖ/PDY members.*

*b. The application does not have a corporate website.*

*c. The application has not resorted to advertising, etc. for promotion and it has exerted no effort to boost the number of its users.*

*d. In order to download and install the application, the Google Play Store and Apple App Store stores and websites as well as flash disks/pendrives, SD cards or Bluetooth can be used.*

*e. It is not mandatory to have an e-mail address or GSM line in order to register with the application. Using the application without authentication is supported.*

*f. The application allows users to use any username they may chose.*

*g. The application does not use the user's address book. The user creates his/her own address book.*

*h. The application does not allow the user to find other users by searching based on certain criteria (phone number, username, e-mail address, etc.) Users who want to communicate using the application have to contact each other beforehand and accept the request for mutual communication.*

*i. The application does not offer any password recovery option to be used in case of forgotten passwords.*

*j. The application uses self-signed certificates instead of digital certificates generated by certificate authorities.*

*k. The application automatically deletes messages.*

*l. The use of a VPN was made mandatory for signing in the application from Turkey after a certain date.*

*m. The ByLock application was shut down without informing its users.*

8. Whether the developers of the ByLock application are FETÖ/PDY members is not a matter of technical nature, but one that should be examined by judicial authorities. Nevertheless, any charges of membership to any organization against the developers of the application do not mean that the application in question was for exclusive use by alleged members of that organization. Likewise, it was reported that the developers of the Morbeyin applications were charged with FETÖ/PDY membership, but everyone could download and use the Morbeyin applications.

9. A portion of other matters cited as proof of exclusiveness of the ByLock application stems from the preferences of application developers or admins. It is possible to find numerous communication applications having similar features. If several or all features specified are found in a communication application, this does not prove beyond reasonable doubt from a technical perspective that the application in question is for exclusive use.

10. While the lack of a specific website for the application, the use of self-signed certificates, and the lack of a password recovery option are not frequently encountered among the commonly used applications, it is very usual for many applications that do not have a large user base. This may be due to the developer's or admin's preference. It does not prove beyond reasonable doubt from a technical perspective that the application in question is for exclusive use.

11. Likewise, lack of promotional activities, the mandatory VPN use, closing the application without informing the users, etc. may be the developer's/admin's choice. These matters do not prove beyond reasonable doubt from a technical perspective that the application in question is for exclusive use.

12. It is impossible to know for certain that no effort was made to increase the number of the application's users. This does not prove beyond reasonable doubt from a technical perspective that the application in question is for exclusive use.

13. Snapchat, WhatsApp, Telegram, Line, Skype, Twitter, Instagram, Facebook, Signal, Hangouts, etc. have one or more features listed above.

14. It is possible to install any application using the Android application package files with the "apk" extension for that application via the flash memory/pendrive, SD card or Bluetooth. The ability to install applications via any data carrier is attributable to the characteristics of mobile devices and operating systems, not to those of applications. This does not prove beyond reasonable doubt from a technical perspective that the application in question is for exclusive use.

15. It is possible to register with the Line application using the Facebook credentials or with the Instagram application with an e-mail address (users may easily have numerous e-mails with different names). No authentication is required during the obtaining of a Hotmail account. Requirement of authentication during registration or lack of it does not prove beyond reasonable doubt from a technical perspective that the application in question is for exclusive use.

16. Communication applications' access to address books is an optional feature in virtually all applications.

17. The requirement for approval by users for mutual communication can be found as an optional feature in many communication applications, particularly including the Line application.

18. Many applications including Facebook, Instagram, Twitter, etc. allow their users to choose any username.

19. Automatic deletion of messages is a feature available also in many communication applications such as Snapchat and Telegram.

20. If one or more features specified are available in a communication application, this does not prove beyond reasonable doubt from a technical perspective that the application in question is for exclusive use.

iv. *Is it possible to determine beyond reasonable doubt from a technical perspective that an application that can be downloaded, installed and used from mobile app stores was for exclusive use?*

21. It is considered that an application that can be downloaded, installed and used from mobile app stores and that can be used without a third party's reference cannot be for exclusive use. If the application in question has been turned into an application for exclusive use using a different method not known to us, this can be determined beyond reasonable doubt from a technical perspective only by examining all communication content of all users. It is considered that any communication content which is not related to the organization in question will undermine the argument that the application has been designed for exclusive use by that organization. There are numerous messages which cannot be characterized as belonging to the affairs of the organization among the communication content which was reportedly obtained by law enforcement forces in the investigation/trial case files

or court decisions with charges of ByLock use, examined by the experts who undersigned this expert opinion. Given the content that has nothing to do with the organization's affairs, it is considered that the application in question cannot be characterized as for exclusive use.

v. *What are needed in order to determine beyond reasonable doubt from a technical perspective that the ByLock application has been used?*

22. This was discussed by Digital Forensics Expert T. Koray Peksayar in his article " Yargıtay 16. Ceza Dairesi Kararına Teknik Bakış: CGNAT Neden Tek Başına Delil Olamaz?-Bölüm 1" (A Technical Review of the Decision by the 16th Criminal Chamber of the Court of Cassation: Why CGNAT cannot be Standalone Evidence: Part 1)[2] accessible from his personal website.

23. In order to prove beyond reasonable doubt from a technical perspective that the ByLock application has been used, the following steps:

i. that the ByLock application is installed on a cellphone or any other smart device with required characteristics,

ii. that this application is used to register as a user,

iii. that after the user is registered, the user IDs of other users to be contacted are added to the address book,

iv. and the application is used to communicate with other users, have to be fulfilled, and complete fulfillment of these steps has to be proven.

In order to prove that real connection has been established with the ByLock server using the ByLock application after it has been installed as described above, the smartphone in question has to be examined, the connection records have to be examined and the content and user registration query has to be made on the data obtained from the ByLock server.

If only all these conditions have been fulfilled and there is no contradiction among them, it can be said that a real connection has been established with the ByLock server using the ByLock application and the continued use has been in question.

**CONCLUSIONS AND EVALUATIONS**

Based on the foregoing scientific facts, described in detail above, we have reached the following conclusions and evaluations:

There is no widely used mobile communication application that does not use encryption.

If a communication application is encrypted, this does not prove that the application in question is for exclusive use.

It was possible to use the ByLock application by downloading it from mobile app stores during the period when it was available on mobile app stores.

[2] https://koray.peksayar.org/yargitay-16-ceza-dairesi-kararina-teknik-bakis-cgnat-neden-tek-basina-delil-olamaz-bolum-1/

Any reference from any third party was not needed to download and use the ByLock application (other than the user and the application).

There was no obstacle or restriction to users' downloading and using the ByLock application from mobile app stores.

A portion of the matters cited as proof of exclusiveness of the ByLock application stems from the preferences of application developers or admins. It is possible to find numerous communication applications having similar features. If several or all features specified are found in a communication application, this does not prove beyond reasonable doubt from a technical perspective that the application in question is for exclusive use.

It is considered that an application that can be downloaded, installed and used from mobile app stores and that can be used without a third party's reference cannot be for exclusive use.

In order to prove that real connection has been established with the ByLock server using the ByLock application, the smartphone in question has to be examined, the connection records have to be examined and the content and user registration query has to be made on the data obtained from the ByLock server.

If only all these conditions have been fulfilled and there is no contradiction among them, it can be said that a real connection has been established with the ByLock server using the ByLock application and the continued use has been in question.

This expert opinion is presented for the appraisal of courts/tribunals if submitted by suspects/defendants or by their lawyers.

With regards, September 1, 2021

Levent Mazılıgüney

Dijital olarak imzalayan Levent Mazılıgüney
ÖA: cn=Levent Mazılıgüney, email=maziliguney@gmail.com
Tarih: 2021.09.05 23:34:20 +03'00'

**T. Koray PEKSAYAR**
Digital Forensics Expert
Engineer (MS)

[This document has been digitally signed as per the Law on Electronic Signatures No. 5070]

**Dr. Levent MAZILIGÜNEY**
Digital Forensics Expert
Engineer (MS, Ph.D.)

[Digitally Signed by Levent Mazılıgüney
ÖA: cn=Levent Mazılıgüney, email=maziligüney@gmail.com
Date: 2021.09.01 22:38:26 +03'00' ]

*Translated from the Turkish original published on 01 September 2021 to English by Dr. Levent MAZILIGÜNEY. Turkish original of the expert opinion signed digitally by both experts is available from the link https://www.patreon.com/posts/55803801