REPORT:
EVER-CHANGING EVIDENCE
ByLock

*Turkish government’s favourite tool to arrest its critics*

Turkish Prosecutors Say 11,500 Mistakenly Investigated For ByLock Use

THE ARRESTED LAWYERS INITIATIVE
DECEMBER, 2017.
EVER-CHANGING EVIDENCE: ByLock

A stallholder woman in Aksaray was detained over being alleged ByLock user.

The unprecedented mass arrest campaign which started immediately after the 2016’s failed coup attempt continues. According to the last figures given by Suleyman Soylu, Internal Affairs Minister, only in 2017, 48,305 people have been arrested and as of 5 January 2018 twice as many people had been taken into custody. It is estimated that over ten thousand people have so far been released after spending some time in detention.

ByLock, an encrypted online messaging application, has emerged as the Turkish government’s favourite tool throughout mass arrest campaign which targeted critics of its policies. AKP officials claim that BYLOCK has exclusively been used by the members of the Gülen Movement as a secret communication tool. The government claims that anybody who might have downloaded it is in fact a “terrorist.”
A. WHAT IS BYLOCK?

ByLock is an encrypted i-message app that provides written and voiced communication between its users which was downloadable via Google Play Store, Apple Store and some other online markets. According to a report prepared by FOX-IT, a Netherland based prominent forensic IT company, BYLOCK only from Google Play Store itself was downloaded more than a hundred thousand times.

The US-based think tank Freedom House, which in its “2017 NET Freedom” report has listed Turkey among the countries in which internet freedoms are restricted most, stated that tens of thousands of Turkish citizens have been arbitrarily detained for their alleged use of the ByLock application. “Despite a lack of evidence, and the arbitrary nature of the blanket arrests, numerous users have been deemed guilty by association for simply downloading the app.” the report concluded.
B. TIMELINE OF BYLOCK

1. WHEN HAS THE BYLOCK APP BEEN IN SERVICE?

According to the Fox-IT report, ByLock was in service between 14 March 2014 and 19 February 2016.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 March 2014</td>
<td>At this date, it was observed that ByLock.net resolved to IP address 184.168.221.39 hosted by godaddy.com</td>
</tr>
<tr>
<td>18 March 2014</td>
<td>At this date, it was observed that ByLock.net resolved to IP address 184.168.221.39.</td>
</tr>
<tr>
<td>31 March 2014</td>
<td>At this date, it was observed that ByLock.net resolve IP address was changed from 184.168.221.39 to 69.64.56.133</td>
</tr>
<tr>
<td>29 April 2014 – 10 August 2014</td>
<td>Between these dates, it was observed that IP address 69.64.56.133 was hosted by server4you-inc.</td>
</tr>
<tr>
<td>4 August 2014</td>
<td>At this date, it was observed that ByLock.net was last resolved to IP address 69.64.56.133</td>
</tr>
<tr>
<td>10 August 2014 – 12 March 2016</td>
<td>Between these dates, it was observed that IP address 46.166.160.137 was hosted by uab-cherry-servers</td>
</tr>
<tr>
<td>14 August 2014</td>
<td>At this date, it was observed that the ByLock.net hosted on IP address 69.64.56.133 and was changed to IP-address 46.166.160.137</td>
</tr>
<tr>
<td>19 February 2016</td>
<td>At this date, the last activity was observed for IP address 46.166.160.137</td>
</tr>
</tbody>
</table>

Timeline for ByLock Server
2. WHEN DID THE TURKISH GOVERNMENT AND JUDICIARY BECOME AWARE OF BYLOCK APP?

Turkey’s National Intelligence Agency said in its press statement that all findings about BYLOCK app and the raw data compiled with intelligence effort were shared with judicial, security and other authorities on 2016 May.

3. WHEN WAS THE FIRST ARREST MADE ON GROUNDS USING / DOWNLOADING BYLOCK APP?

Although ByLock was taken off service by its owner on 19 February 2016, almost 4 months before the failed coup, the AKP government immediately after the failed coup attempt said that it was used by the putschists. The first arrests based on ByLock usage were made on 20 July 2016, only 4 days after the coup attempt.
Since then ByLock has been the primary evidence in dismissing, arresting and convicting those who do not agree with the AKP rhetoric. Turkish Constitutional Court and the Court of Cassation has also decided, contrary to their previous decisions on digital evidence, that using or downloading ByLock was enough evidence to convict a person of membership to an armed terrorist organisation even in the absence of any other evidence.

4. THE EVERCHANGING FIGURES AND CRITERIAS

4.a. 2016 SEPTEMBER – OCTOBER | THE NUMBER OF BYLOCK USERS IS 225.000

On 2016 September, Faruk Ozlu the then the minister of Science and Technology said that there were 215,000 ByLock users and on 2016 October Veysi Kaynak the then deputy Prime Minister said that 18 million messages were obtained and that the process of decrypting them was underway.

The two statements above show that as of 2016 October,

- The government and judiciary had a ByLock user list which included IDs of some 215,000 people and data which included 18 million messages albeit some of them still decrypted.
- Work was underway for the decryption and examination of the digital evidence obtained.

4.b. 2017 APRIL | THE NUMBER OF BYLOCK USERS IS 122.000

As from 2017 April, pro-government media started to say that “the number of ByLock users was 122,000 and all of them would be taken into custody without exemption.
On 7 April 2017, Karar, a pro-government daily, published a story which said that:
i) MIT, the Turkish intelligence agency, had created a new and sensitive inquiry screen,
ii) by a double confirmation system any incorrect findings had been eliminated
iii) an investigation had been launched by the Ankara Prosecutorial Office to establish those who were responsible of the incorrect findings in question.

4.c. 2017 JUNE | THE NUMBER OF BYLOCK USERS IS 102,000

102,000 suspects accused of Gülen links are ByLock users, Turkish communication authority says

Ankara

Turkey's Information and Communication Technologies Authority (BTK) has said that it analyzed various messages of 102,000 suspects accused of being members of the Fethullahist Terrorist Organization (FETÖ) and determined that they were sent through ByLock, the group's encrypted messaging application, Sabah daily reported on June 26.

“A list of 102,000 people has been sent to us from courts. We have prepared reports and met the demands of the courts one by one, whichever court has the investigation files of these people on the list,” Özer Fatih Sayan, the head of BTK, told the daily.
On 2017 June, Ömer Fatih Sayan, the head of the BTK (Information Technologies Agency) said that “a list of 102,000 people has been sent to us from courts. We have prepared reports and met the demands of the courts one by one, whichever court has the investigation files of these people on the list. By exposing the records of which days, where and how many messages the names on the list, which the courts have sent us, exchanged correspondences, we have confirmed that they have used ByLock. Those on the ByLock list therefore have no excuse left. By getting detailed records of their correspondences, we have once again determined that they have used ByLock.”

4.d. 27 DECEMBER 2017 | 11480 PEOPLE WERE MISTAKENLY PROSECUTED | 90500 BYLOCK USERS ARE LEFT BEHIND

Turkish Prosecutors Say 11,500 Mistakenly Investigated For ByLock Use

According to the state-run Anadolu News Agency, The Ankara Chief Public Prosecutor’s Office on 27 December 2017 stated that 11,480 GSM users had been found to have been involuntarily directed to the mobile phone application ByLock.

The prosecutor’s office said that “the legal status of the 11,480 mobile phone users would be re-evaluated”. Yüksel Kocaman, Ankara’s Chief Public Prosecutor, said; “Nearly a thousand people, who were found to have been directed to ByLock through Mor Beyin application, have been in jail in different provinces,” and added; “They will be released unless there is other evidence against them.”
It thus became clear that 11,480 of the 102,000 people which were included in a list sent to the judicial authorities by the BTK and MIT in June 2017 were not ByLock users after all.

After 11,480 people eliminated from the list of 102,000, 90,500 alleged ByLock users are left behind.
In the light of the new information, Turkish intelligence has started reinvestigating at least 30,000 people it formerly believed to have been accessing a mobile messaging application called BYLOCK pro-government newspaper Milliyet said.

On 3 January 2018, lawyer Ali Aktas said that the findings about 40,000 people are dubious and that 11,480 people had been removed from the list and a re-evaluation of data concerning another 30,000 was underway.
Between 2016 August and 2017 April, Turkish intelligence, police, and judiciary used a “three-color categorization system” devised by MIT.

In the three-color categorization system, ByLock users were sorted into categories as red, blue and orange;

- **Red**: User and its user id has been established, the margin of error is between 0.1 and 1 per cent.
- **Orange**: Although the identity of the user has been determined, his user id could not
- **Blue**: Possible user, actual usage can neither be confirmed nor ruled out.
4.ii. | AS FROM 2017 APRIL| The Three-colour Categorisation was Abolished, The Three-time Log-in Criteria is in effect. (updated)

10 April 2017; The Colouring (three-colour) Criteria was abolished.

In April 2017, the Pro-government media claimed that, “the Three-color categorisation” was abandoned and ByLock users list was amended according to “minimum three logins criteria” and a new list of 122,000 people had been sent to judicial bodies.

Pro-AKP daily Sabah says that those who used three-times will be considered as ByLock user.

Turkish Intel says in its report that those who have IP traffic with ByLock server at least 3 different days were listed as ByLock user.
C. BYLOCK, AS REGARD TO EVIDENCE INTEGRITY AND AUTHENTICITY

1. IP Convergence (updated)

The main method through which ByLock users are identified is monitoring the respective IP traffic of suspects. If a suspect is found to have accessed to any of the ByLock servers, he is defined a ByLock user and charged and subsequently indicted for being a member of an armed terrorist organisation.

This method of identifying ByLock users through their respective IP addresses is not reliable as Turkey telecommunication operators and particularly Avea and Turk Telekom do not provide static IP service which means that the same IP number can be appointed to different customers.

As revealed by Ahmet Takan, a Turkish journalist, this is called “IP Convergence” and when it was first noticed by Turkish security authorities in 2016 October a circular was promptly sent to relevant authorities warning them of the IP Convergence issue.
The notice (above) dated 14 October 2016 says that:

- The MIT list dated 3 September 2016 included 18,074 individuals which were identified as ByLock users through examination of their respective IP traffic.

- Mobile phone operator AVEA appoints same IP number to each and every device which connect to the same mobile base station.

- Anybody who have accessed to the ByLock server less than 20 times might therefore not be an actual ByLock user.
In an official notice, the telecom operator Turk Telecom says that “given the numerous customers use the same IP address at the same time, misleading results can arise from IP address based queries.”
2. IP Routing

Two independent forensic experts have found out that users of eight different smart phone apps were being routed to ByLock servers as a result of some random pop-up advertisement. A review of the matter has subsequently revealed that at least 11,480 individuals had been routed to ByLock servers as a direct result of the said 8 applications.

On December 2017, Ankara Chief Public Prosecutor conceded that 11,480 people, over a thousand of whom had been arrested, were wrongly prosecuted as ByLock users.

On 3 January 2018, Milliyet Daily reported that although 11,480 individuals had so far been removed from the BYLOCK list, the circumstances of another 30,000 people who had been included in the same list were being reviewed.
3. DELAYED FORENSIC EXAMINATION

On 6 October 2016, Veysi Kaynak the then deputy Prime Minister said that 18 million messages had been obtained and they were being decrypted. This statement shows that the Turkish Intelligence Agency had obtained ByLock data on or before 6 October 2016. But then it was revealed that MIT sent the said data to judicial authorities on 9 December 2016. That means MIT in two months had managed to decrypt and process the digital evidence which included at least 18 million messages.

On the other hand, the MIT should have duly passed the obtained data to the judiciary as is and without delay for them to carry out their own evaluation. Although the processing of the data by MIT and its consequent late delivery to the authorities raises some serious questions as to the integrity and authenticity of the evidence submitted to the authorities, this is not the only problematic point in this matter. Another very serious issue which concerns the integrity of the ByLock evidence is the disintegration of the digital evidence and carrying out of forensic examination (forensic image taking) as two separate processes on two separate dates (9 December 2016 and 24 March 2017).
Neither the judicial authorities nor the defendants know:

- How was the digital data regarding BYLOCK saved until 9 December 2016 and 24 March 2017?

- Why was the digital evidence disintegrated?

- Was the digital data corrupted by the Turkish INTEL (MIT)?

- Were measures were taken to preserve the authenticity of the digital evidence while MIT processed it?

- Why was forensic image taking not carried out as soon as the data was obtained from ByLock servers?
4. PRECEDENT DECISIONS OF TURKISH COURTS AS TO DIGITAL EVIDENCES AND INTELLIGENCE INFO

In its decisions regarding the cases called Balyoz, Ergenekon, Poyrazkoy, Izmir Espionage, the 16th Circuit of the Turkish Court of Cassation has consistently underlined following:

- the copy of (forensic) image of digital evidences must be given to the defendants,
- the forensic image of digital evidences must be taken in situ,
- the original copy of the digital evidence must be left to the suspect after its image was taken,
- if the image taking in situ is not possible because of technical obstacles such as encryption:
  i. the seized digital evidences must be sealed
  ii. the process to unseal and image taking must be done in the presence of the defendant of his / her legal counsel;
- independent forensic experts’ examination must be done to check the authenticity of the digital evidence.

“In criminal proceedings, evidence must be by the law and must be obtained with methods by the law. In order to be able to conduct a fair trial and to be able to evaluate the findings collected during the investigation (and prosecution) as evidence; the digital data obtained from suspects (or defendants) must be collected in accordance with the technical requirements set by the law, and must be submitted to the judicial authorities in a complete, uncorrupted state. It is the intention of the Legislator to arrange Article 134 of the Criminal Procedure Law (CMK) in detail. Since the fact that external intervention to the digital evidence is technically feasible and that it is often not possible to determine by whom the intervention was made, it is necessary for the safe confiscation and examination to leave the original media to the suspect after its image was taken in the situ… Under the articles 2/e and 161 of the Criminal Procedure Law (CMK – No:5271) and the article of annex-6 of the Law as to Duties and Authorities of Police, The law enforcement agent who learns a situation that implies a crime was or is being committed should immediately inform the public prosecutor and proceed the investigation under his orders. The proceedings without a legal search warrant or proper judicial order are considered as illegal.” is said in decision of the 16th Circuit of the Turkish Court of Cassation regarding Ergenekon case.
In its precedents (2013/2312, 2013/7800, 2014/253), the Turkish Constitution Court has consistently decided that withholding the copy of the digital evidence from defense is the violation of the principle of equality of arms and the right to fair trial.

According to the Turkish Laws and particularly the law as to duties and authorities of the Turkish INTEL (MIT), the Turkish INTEL (MIT) has law enforcement authority only the cases regarding the espionage and counter-espionage; it has no authority on the terrorism-offences related cases. Therefore, Turkish Police adds a warning notice to all its reports on BYLOCK that says “since the information compiled from the BYLOCK inquiry module is intelligence info, don’t have legal evidence qualification… itself does not constitute the ground for administrative and judicial procedures.”
D. CONCLUSION

Under above mentioned the facts, we can say without hesitation that

i. The delayed and disintegrated forensic authentication of the digital data related the BYLOCK,

ii. Obtaining the digital data / evidence related with BYLOCK app without order and oversight of a judicial authority,

iii. Processing the digital data / evidence related with BYLOCK app before a forensic authentication (under a judge’s warrant),

makes it less than an improperly obtained evidence, and shades doubts over its authenticity thereby depriving it of the legal evidence qualification.

The ever-changing arguments about the ways in which it was obtained, processed, evaluated, and shifting claims about the facts about the evidence such as the number of persons and messages; the unwillingness of the prosecutors to share the evidence with the defendants, together with the law enforcement agency’s warning that the data cannot be a basis for judicial procedures create doubts of fabrication, alteration or corruption of the data.

Also, withholding the copy of the digital data/evidence related with BYLOCK app from defendants and their counsel both casts a thick and reasonable shadow on the evidence and constitutes the violation of the right to fair trial.

BYLOCK is not legal evidence but a pathogen that is contaminated to the Turkish Judiciary by the Turkish INTEL (MIT). The only possible remedy for this contamination is quashing the all decisions to convict that grounds on the BYLOCK and trying defendants by the right to fair trial.

END.