OPINION

ON

THE LEGALITY OF THE ACTIONS OF THE TURKISH STATE

IN THE AFTERMATH

OF THE FAILED COUP ATTEMPT IN 2016

&

THE RELIANCE ON USE OF THE BYLOCK APP AS EVIDENCE OF MEMBERSHIP

OF A TERRORIST ORGANISATION

INTRODUCTION

1. There was an attempted coup in Turkey on the 15th July 2016, it was suspected by the Turkish government that those responsible were a Gulenist faction within the military. Fethullah Gulen is a US-based Islamic cleric who was previously an ally of President Erdogan until about 2013 when, it is alleged, pro-Gulen judges levelled corruption charges against him.

2. After the coup had failed the Gulen movement was accused of being responsible. Earlier, In May 2016, President Erdogan announced that the Gulen movement was an illegal terrorist organisation and the group was registered in the Turkish National Security Council's list of organisations that pose a threat to Turkey.

3. In addition, following the coup, President Erdogan declared a state of emergency for three months which has been extended several times since and is currently still in force. The state of emergency gave the government the power to remove Gulenists and those suspected of being Gulenist from across state institutions.

4. On the 16th April 2017 a national referendum was held into constitutional reform which was described by the Deputy Prime Minister Numan Kurtulmus as being *"to provide for the continuance of measures aimed at securing the rights and freedoms of citizens."* However despite these laudable objectives the state of emergency remains in place at the time of writing.

5. Since the state of emergency was declared tens of thousands of people have been suspended or dismissed from their employment. In September 2016 the Turkish Prime Minister Binal Yildrim stated that *"since the coup attempt and until August 2016 over 40,029 people had been arrested and arrest warrants issued for 20,355. 79,000 public servants have been dismissed so far and 4,262 companies and institutions have been closed down."*

6. The US State Department noted, in their Country Reports on Human Rights Practices for 2016, that *"The suspension, firing and freezing of personal assets of more than 3,000 members of the judiciary after the July 15th coup attempt, (representing 22 percent of the total) accused of affiliation with the Gulen movement had a chilling effect on judicial independence."*

7. Turning to lawyers Human Rights Watch in a report dated 24th October 2016 noted that *"Lawyers have been targeted too. The Union of Turkish Bar Association informed Human Rights Watch that 79 bar associations had reported in total 202 lawyers had been placed in pre-trial detention on suspicion of involvement in the coup attempt or links to the Gulen movement."*

8. The military faced the initial dismissal of more than 1,000 ranking officers, nearly 44% of land force generals were dismissed, 42% of air force generals and 58% of navy admirals. By the end of July 2016 Radio Free Europe had reported that arrest warrants had been issued for 73 military pilots and on the 27th October 2016 Turkish State News

Agency reported that 45 pilots had been detained and another 28 were still being sought. The suspects included 2 colonels and 71 lieutenants.

9. Academics and other professionals have been faced with arrests and detentions on a similar scale.

10. This startling reaction to the failed coup by the Government has obviously had wide implications not only in Turkey but in many other countries.

11. Turkey is a signatory to the European Convention of Human Rights and there have been allegations that the arrest and detention of people following the failed coup has breached their convention rights. There have also been allegations of torture including sleep deprivation, severe beatings and sexual abuse of those detained and an increasing number of deaths in custody. Amnesty International has reported that it has credible evidence that detainees in Turkey have been beaten, tortured and on some occasions raped. These allegations have been robustly denied by the Government. Although worryingly the media reports Mehmet Metiner, a Justice and Development Party (AKP) deputy, as saying that there will be no investigations into claims of torture and mistreatment of people detained after the coup if the victims are sympathisers of Fethullah Gulen. It is difficult to imagine a more flagrant disregard of the convention rights of a detained person.

MY ROLE AS AUTHOR OF THIS REPORT

12. I am a Queen's Counsel practising law in England. I was called to the bar of England and Wales in 1972 and appointed to the rank of Queen's Counsel in 1991. I have sat as a part-time judge (known as a recorder) in the Central Criminal Court in London for some 23 years.

13. I have no knowledge of Turkish national law but consider myself an expert on English Criminal Law, European Human Rights Law and International Criminal Law.

14. I have been asked to advise on the circumstances in which people have been arrested and detained in Turkey since the failed coup and to give an opinion on whether the convention rights of those arrested and detained have been breached and whether the actions of the Turkish State since the failed coup has breached International Criminal Law.

15. I have been asked in particular to consider the alleged use of the Bylock App and whether use of the App could provide a safe basis for conviction.

16. I consider myself well qualified to provide such an advice.

17. I have been assisted in the drafting of this report by Simon Baker, an experienced barrister with expertise in IT issues, who is a member of the Bar Council of England

and Wales IT Panel. He has been responsible for drafting paragraphs 21 and 22 of this opinion and has been responsible for the liaison with our technical experts.

MATERIAL CONSIDERED

18. I have read extensively of background material including the reports by the British Home Office "Country Policy and Information Note Turkey; Gulenism April 2017" and "Country Policy and Information Note Turkey: Human Rights Defenders version 2 June 2017", reports from the US Government "Turkey 2016 Human Rights Report, United States Department of State – Bureau of Democracy, Human Rights and Labor" and extracts of numerous other reports.

19. In addition I have been provided with the following documents:-

    (i) An English translation of a report originally in Turkish titled "Bylock Application Technical Report" (hereafter referred to as the MIT report")

    (ii) An English translation of a court judgement in the case of a person detained after the coup who was charged with offences under Article 314/2 of the Turkish Criminal Code and Articles 51, 53 and 63 of Act number 3713 for allegedly being a member of a terrorist organisation. In order to avoid possible repercussions the person has not been identified in this report and will be referred to as X although his identity is known to me.

    (iii) A technical report on Bylock one titled "Bylock App Report Within the Scope of Allegations" the source of which is unclear to me (and to which I have therefore attached little weight)

(iv) A technical report on Bylock titled "Technical Solutions", the source of which is unclear to me (and to which I have therefore attached little weight) and

(v) A number of documents marked "sample message content 1", 2sample message content 2", "sample message content 3" and "sample message content 6" which are translations of some of the Bylock messenger exchanges included in the graphics at sections 3.6.2.4 of the MIT report.

20. I have also been provided with a copy of the Penal Code of Turkey as published in English by the European Commission for Democracy Through Law (Venice Commission.) I have read Article 314 which provides that:-

(1) Any person who establishes or commands an armed organisation with the purpose of committing the offences listed in parts four and five of this chapter, shall be sentenced to a penalty of imprisonment for a term of ten to fifteen years.

(2) Any person who becomes a member of the organisation defined in paragraph one shall be sentenced to a penalty of imprisonment for a term of five to ten years.

(3) Other provisions relating to the forming of an organisation in order to commit offences shall be applicable to this offence.

Parts four and five of this chapter include articles 197 to 224 inclusive and cover offences globally described as "Offences Against Public Confidence" and "Offences Against Public Peace."

21. Finally, I have the benefit of a report prepared by Thomas Moore, who is an experienced forensic IT specialist. He is a member of the British Computer Society and a member of the Expert Witness Institute. His CV is appended to the report, and it is clear that he is a qualified expert with considerable experience in providing expert digital forensic evidence to courts and tribunals both within the United Kingdom and overseas. Mr Moore's report reviews the MIT Report and answers a number of specific questions that I have posed for them, namely:

(i) What is ByLock?

(ii) How does it work?

(iii) Is it possible to identify how widely it was used (both within Turkey and generally)?

(iv) How, if at all, does it differ from other commercially available private messaging Apps?

(v) Is it possible to establish through any technical means whether use of Bylock is limited to supporters of any particular political or social movement?

(vi) Are there any aspects of the MIT report on ByLock which appear to be flawed either technically or in terms of methodology?

(vii) In relation to the ByLock server:

(a) Was the Bylock central server turned down before the end of March 2016?

(b) If so what impact would that have on the ability of those who had downloaded the App to communicate using Bylock?

(c) If so would the statement "it is not possible to use Bylock after March 2016" be correct?

(viii) Even if the App was widely used by supporters of the Gulen movement, is there any proper evidential basis for inferring that use of ByLock necessarily connotes support for the Gulen movement or its political views?

(ix) Even if ByLock could establish support for the Gulen movement or its political views, does that provide a proper evidential basis for establishing membership of the Gulen movement (itself registered as a terrorist organisation since May 2016) and/or complicity in any conspiracy to stage the coup and/or conspiracy to commit terrorist offences?

22. A copy of the report is appended to this advice at Annex 1. As such it is unnecessary to repeat the contents in full within this opinion. However, it is perhaps helpful to highlight some of the concerns identified in relation to the MIT Report, and the consequences of those matters:

(i) The MIT Report makes a number of assertions of fact without providing any evidential source or justification for the assertion. As such, it is impossible to say whether the assertions are correct or not. In consequence of this, no Court receiving the report would be in a position properly to assess the credibility or accuracy of the assertions, and so it would be quite unfair and improper for any Court to rely upon those assertions to found a conviction.

(ii) There are a number of assertions contained in the MIT Report which are fundamentally contradictory. For example:

(a) The MIT Report asserts at paragraphs 3.5.1 to 3.5.5 that IP blocking was used to force users to use a VPN (virtual proxy network) to access the ByLock App. At 3.6 however, it is suggested that IP addresses were used

to identify ByLock users. These two assertions are mutually incompatible, since the IP addresses would not have been able to be used to identify users if VPNs were being used;

(b) There is an assertion at paragraph 2.4 of the MIT Report that access to ByLock was being limited and tightly controlled to ensure that access was limited to members of the Gulen movement, yet the report acknowledges at paragraph 2.3 that the ByLock App was available for download from the Google Play Store and the Apple Store. Not only did this mean that there was no means of controlling access to the App, but it was downloaded over 600,000 times between April 2014 and April 2016 by users all over the world. The fact that the App was openly available to anyone in the world to download is simply incompatible with the assertion that access to the App was limited, tightly controlled and available only to a limited group of users;

(iii) A number of the assertions made in the MIT report are simply factually unsustainable. For example:

(a) The assertion at paragraph 2.4 of the MIT Report that "people generally [use messenger apps to] engage with their social environment about daily issues" simply does not reflect the reality of the use of many similar Apps on the market (such as WhatsApp, Telegram etc);

(b) The assertion at paragraph 3.3 of the MIT Report that the worldwide searches related to the ByLock App are either "members in foreign countries or Turkish users utilizing VPN services" could not be established without access to protected Google information or to IP records showing

the use of VPNs. The assertion is no more than speculation masquerading as technical evidence; and

(c) The observations in relation to SSL certification at paragraph 4 of section 4 of the MIT Report are factually unsustainable and reflect either a lack of understanding on the part of the author of the MIT report as to the purpose of a SSL certificate or an intention to mislead a non-technical reader. A SSL certificate is simply a cryptographic key to enable a browser to confirm that they have connected to the correct site. Server data is of the sort contemplated by the MIT report would never be transferred through a certificate authority. As such, a self signed SSL certificate authority is far more likely to be a cost-saving measure rather than being, as claimed in the MIT report, and attempt to ensure secrecy;

(iv) The assertion at paragraph 3.5.5 of the MIT Report that the blocking of IP addresses was intended to force users to use VPNs is both speculative (no explanation is given in the report why the more plausible inference that the blocking was to prevent DDOS attacks on the server is not drawn instead) and implausible (as it assumes a degree of technical proficiency in the use of VPNs which is unrealistic); and

(v) The MIT report draws inferences from the setting up of the ByLock App (for example the use of the Paysera platform and yandex.com e-mail account and the locating of the servers in Lithuania) which are highly speculative, and which exclude alternative explanations with no reasons or evidence given. For example, the report assumes that the use of servers in Lithuania was in the interests of secrecy rather than for the more obvious innocent reason that

such servers would almost certainly have been cheaper and more cost-effective at the time and so the use of Lithuania as a server base is more likely to have been a function of commercial reality.

THE ROLE OF THE BYLOCK APP IN THE SUBSEQUENT ARRESTS AND DETENTION OF TURKISH CITIZENS

23. It seems clear that the authorities in Turkey believe that the Bylock App was used by those members of the Gulen movement now referred to as FETO/PDY by the Turkish State. This movement was registered as a terrorist organisation in May 2016 (this is not the same as proscription which must be decided by a Court of Law.)

24. There have been a number of expert reports prepared on the Bylock App. One of these headed the "Bylock Application Technical Report" was clearly produced under the authority of the National Intelligence Organisation of Turkey and includes references to the mechanism for obtaining the data relied upon in the report as "confidential" on grounds of national security. I have read this report.

25. A copy of this report is to be found online.

26. In addition other reports on the Bylock App have been submitted in relation to other individual cases in the criminal courts in Turkey by the Public Prosecutor. I assume that they are consistent with the Bylock Application Technical Report and are probably

extracts from the main report containing those parts considered relevant to the individual case being considered.

27. Support for this view is to be found in the judgement in the case of X which includes direct quotations from the Bylock Application Technical Report although no reference to that report can be found in the court file.

28. It is important at this stage to emphasise a number of facts that are agreed and confirmed by the Bylock Technical Report. The first is that the Bylock App was taken down in March 2016. After that time no-one could use the App. This is confirmed in paragraphs 2:1 of the Bylock Applicatio0n Technical Report *"Bylock, which was offered for [public] use in the beginning of 2014 and had been available through different versions until the first months of 2016" and* paragraph 3:5:4 *"It has been found that until February 2016 payments [for the hire of] the server and IP addresses were made by PaySera."* It appears to be agreed that from mid-March 2016 no-one could use Bylock because those paying for the server, which was situated in Lithuania, and the IP addresses ceased to make the payments necessary to keep the App functioning.

29. It follows that by the time of the failed coup the server for the App had been down for four months. Further it has never been alleged that the App was actually used by those involved in the coup in the actual events of July 2016. This is important because, throughout the time that Bylock was available, it could be downloaded for use by any member of the public anywhere in the world. The use of the App and support for the

Gulen movement was not unlawful in Turkey at a time when the App was capable of being downloaded.

30. These uncomfortable truths do not sit easily with the bold assertion in the Bylock Application Technical Report where in paragraph 4:9 of the Report, under the heading "Assessment and Conclusion" the statement is made that *"when all of the above are taken into consideration, it is concluded that the application was made available to the members of the FETO/PDY under the disguise of a global application."*

31. Unfortunately as paragraph 3:1 of the report makes clear the mechanism by which intelligence was collected to produce the report have been excluded from the report itself "so as not to reveal the state's means of technical intelligence and its capabilities as well as for counter-intelligences reasons" so there is no way of testing the accuracy of these statements

32. The startling conclusion identified in paragraph 4:9 appears inconsistent with a simple reading of the earlier sections of the report. In paragraph 3:3 of the report, for example, it states that "the vast majority of users who posted content about "Bylock" before July 15 2016 are observed to have [also] been posting content in support of the FETO/PDY." This presumably indicates that a minority of users in Turkey who posted content about Bylock posted nothing that supported FETO/PDY. Quite how this sits comfortably with the later assertion that the App was used exclusively for members of the terrorist organisation is a mystery.

33. It is also clear that the Bylock App was available on Google Play and Apple App Stores as is conceded in paragraph 3:3 of the report and was hence available to anyone. As a matter of common-sense and logic innocent use of the App cannot be eliminated in any case and unless other evidence proves membership of the Gulen movement after the date when it was added to the list of terrorist organisations use of the App alone could never prove guilt.

34. Unless there is further independent evidence capable of proving membership of the Gulen Movement then the fact that an individual used and/or downloaded the Bylock App before mid-March 2016 cannot prove membership of the movement post May 2016.

35. In any event many people who had Gulenist sympathies may not have been members of the Gulen Movement and may have not have supported the movement after it had been registered as a terrorist organisation. It must be remembered that only ongoing membership or support, after May 2016, was capable of being support for a movement that had been registered as a terrorist organisation.

36. Furthermore there is a concession in paragraph 3:3 of the report that use of the App is not confined to Turkey has been used in other countries including *"France, UK and USA."* This uncomfortable fact is dealt with by the assertion that *"it is believed that searches made from outside Turkey had been made by members of the organisation who lived abroad or by Turkish users who were utilizing VPN."* This statement is worthy of analysis, it is not claimed that there is any evidence to support the belief claimed.

The importance of this claim cannot be overemphasised, if it were to be conceded that some users of the App could not be linked to the alleged terrorist organisation then it would mean that use of the App could form the safe basis for either arrest or detention.

37. The report "Bylock App Report Within the Scope of the Allegations" makes a number of powerful points. In the paragraph headed "Who Used Bylock" it observes that Bylock *"is a public application that existed in Google Play and Apple Store in the past and it can still be downloaded from different web pages."* It does not exist anymore in either Google Play or Apple but an analysis of applications and digital industries indicate that it existed on Apple from April 2014 to September 2014 and in Google Play from April 2014 to April 2016.

38. According to the AppAnnie Report the Bylock App was ranked in the top 100 Apps in 12 countries and in the top 500 in 47 countries. This would seem to demolish the claim that only those who were members of FETO/PDY were users of the App.

ANALYSIS OF EVIDENTIAL VALUE OF USE OF BYLOCK APP

39. On the material that I have seen, the claim that the Bylock App was used by some of those in the Gulen movement seems a conclusion of fact that I must accept. Although the Bylock Application Technical Report, which was presumably prepared for use by the courts in Turkey, does not disclose the mechanism by which it arrived at its

conclusions I proceed on the basis that at least some of those who are members of the movement used the App. I base this conclusion on the entirety of the report including the claim that some of those in the movement had admitted using the App for *"inter-organisational communication."*

40. However I find the evidence that the App was used exclusively by those who were members or supporters of the Gulen movement utterly unconvincing and unsupported by any evidence. Indeed, in my opinion, there is no evidence at all from which any reasonable person could conclude that the App was exclusively used by members of FETO/PDY and a great deal of evidence, much unchallenged, which demonstrates that the App was widely available and used in many different countries, some of which had no links to Turkey.

41. In reaching this decision I rely upon the following facts, the App was available to everyone, it had features that could be attractive to many and was used in many countries. If the conclusion in the Bylock Application Technical Report was correct it would mean that members of FETO/PDY were to be found in numerous countries other than Turkey. The App had been downloaded throughout the world and was in the top 500 Apps in 41 separate countries. It is ridiculous to suggest that all those users were members of the Gulen movement.

42. It follows that if the Bylock App cannot sensibly be claimed to be the exclusive province of those members and supporters of the Gulen movement then there can be no

justification for the arrest and/or detention in Turkey of those who had used the use of the App without other compelling evidence.

EXAMINATION OF TRIAL TRANSCRIPTS

43. I have read with care a translation of the trial transcript in the case of X.

44. He was charged with being a member of a terrorist organisation contrary to Article 314/2 of the Turkish Criminal Code. This offence is considered to be a terrorism related offence under Article 3 of Act 3717, as a consequence the sentence of imprisonment passed on conviction was increased.

45. The judgment of the Court asserts that, when considering all the evidence, *"when all the above are taken into consideration, it is concluded that the application was made available to the members of the FETO/PDY under the disguise of a global application."* This is a direct quotation from the Bylock Technical Application Report discussed earlier and is a conclusion which has already been demonstrated to be an unsustainable. The fact that this is a direct quotation must mean that either the court had the report which for some reason never found its way into the court record or that the differently described reports that are referred to in the court record, but not available to me, are a "cut and paste" job from the other report.

46. We are informed that a recent decision by the Court of Cessation (Yargitay), the equivalent of the Court of Appeal in the United Kingdom, has confirmed reliance on the MIT report in a case involving a different detainee. (Yargitay 16th Criminal Chamber Decision No.2017/3 *"courts may in order to be informed about technical matters require information from public bodies. In the same way this chamber has obtained from MIT information about Bylock."*)

47. Even assuming that the court in the case of X was correct in coming to the decision that the accused had used the Bylock App, which was disputed by the defence, it is impossible to conclude from that that he was a member of a terrorist organisation. The one cannot, as an exercise in logic, lead to the other. Furthermore use must have been before mid-March 2016 as the server went down then. At that time use of the App was lawful and membership and support of the Gulen movement also lawful.

48. Other evidence is relied on against the accused was having a bank account in BankAsya and staying in student accommodation the location of which is not disclosed in the judgement.

49. This other evidence, when analysed, is incapable of proving membership or support for the Gulen movement.

50. BankAsya was a regulated bank in Turkey, it was the largest Islamic bank in the country, which had branches throughout the country available to everyone. Until 2014 the depositors included a number of state owned firms and institutions. It was taken

over in February 2015 by Turkey's Saving and Deposit Insurance Fund (who were the Turkish regulator). The bank being ultimately closed down by the regulator in July 2016, at all times banking at a branch of the bank was perfectly legal.

51. It seems clear that the bank had links with Fethullah Gulen but it cannot be said that every customer of the bank was necessarily a member of the Gulen Movement. The bank was a major bank in Turkey, it had deposits in 2013 of $28,4 billion and in 2015 of $13.2 billion. Clearly many substantial companies, historically some of them state owned, had used the banks services. To suggest that having an account at the bank was evidence of membership of a terrorist organisation is nonsensical.

52. Likewise to rely upon the fact that the defendant stayed in student accommodation as proof that he shared the same beliefs as those who operated the accommodation is frankly ridiculous. The current president of the United States of America, President Donald Trump, owns through his family a number of hotels, to suggest that anyone staying in them shared his political beliefs would be equally as absurd.

53. When analysed there is no evidence that could conceivably justify a conclusion that X was a member of a terrorist organisation. Once the proposition that the use of the Bylock App was for the exclusive use of the terrorist organisation is shown to be wrong then any justification for the conviction collapses.

54. What is clear is that X was, on the basis of the evidence cited in the judgement, wrongly and unjustifiably convicted of a criminal offence when, on any fair analysis of the evidence, there was none that could possibly establish his guilt.

55. What is so worrying is that, on the basis of what has been reported in the media, contained in numerous international NGO's, reported on by human rights organisations, by the Foreign and Commonwealth Office and by the US State Department, evidence of this type has been used not just in this case but in many similar cases. This raises fundamental questions about the legality of the detention and imprisonment of many thousands of people following the failed coup.

THE LEGAL POSITION

56. Turkey is a signatory to the European Convention on Human Rights that guarantees the citizens of Turkey the human rights identified in the convention. Turkey is obligated by international treaty to protect the human rights of its citizens and any failure to do so can be litigated before the European Court for Human Rights {ECtHR}

57. The denial of a citizens convention rights is a serious failure by a state to accord to its citizen those basic rights that everyone is entitled to.

58. Following the failed coup Turkey submitted a formal notice of derogation to the Convention as permitted by Article 15. While it could be argued that in the immediate

aftermath of the failed coup such a derogation could be justified such derogations are not limitless and the ECtHR remains the ultimate authority to determine whether measures taken during a state of emergency and after the derogation are in conformity with the Convention.

59. The fact of derogation does not permit the state unlimited and unregulated power to breach the human rights of its citizens. All breaches of a citizens convention rights by the state must be proportionate and the ECtHR will, and already has, examined the measures taken by Turkey in order to determine whether they amount to a breach of the convention rights of the citizen even allowing for the state's derogation. In Aksoy v Turkey (judgement given 18th December 2016) the court held that the detention without access to a judge for 14 days was not necessary by the circumstances then prevailing in the country.

60. Turkey is not a signatory to the International Criminal Court and hence no question of that court's jurisdiction arises.

61. Focusing then on the European Convention a number of convention rights are potentially engaged despite derogation.

ARTICLE 5

62. Article 5 of the Convention provides for the right to liberty and security. The Convention guarantees these rights subject to certain identified exceptions which include both the lawful detention of persons after conviction be a competent court and the lawful detention of persons for the purpose of bringing them before the competent legal authority on reasonable suspicion of having committed a criminal offence.

63. This Article is essentially concerned with arbitrary detention and is derived from the Universal Declaration of Human Rights, article 3 ("everyone has the right to life, liberty and security of person") and article 9 ("no-one shall be subjected to arbitrary arrest, detention or exile".)

64. There are no accurate figures for the number of people detained since the failed coup but the figure of 75,000 has been accepted by many as a reasonable estimate. In my opinion the detention of such a huge number of people cannot conceivably be justified if the basis for their detention is the fact that they have used the Bylock App and had engaged in some other activity that was lawful at the time they engaged in it such as banking at BankAsya or staying in student accommodation at an educational establishment believed to have Gulenist connections.

65. Such detentions are arbitrary, unjustified and in breach of the convention rights of those detained. Detention for criminal prosecution will be arbitrary if it is not justified by the "reasonable suspicion" that the person detained has committed a criminal offence. Although this is a low threshold, where detention is being authorised on the

basis of the use of the Bylock App, coupled perhaps with some lawful activity at the time such as the reading of a particular newspaper, the banking at a particular bank or the staying in certain accommodation which might demonstrate a sympathy for the Gulenist cause then this would, in my opinion, be arbitrary and in breach of the convention.

66. It is worthy of note that the reasoning and evidence behind the conclusion in the Bylock Application Technical Report that "Bylock has been offered to the exclusive use of the members of the terrorist organisation of FETO/PDY" is not disclosed for security reasons. This is particularly significant as the final conclusion is both controversial and the subject or reasoned disagreement by other experts in the field. The ECtHR has held in O'Hara v United Kingdom no. 37555/97, # 35, ECHR 2001 – X that the "exigencies of dealing with terrorist crime cannot justify stretching the notion of "reasonableness" to the point where the safeguard secured by Article 5 : 1 (c) is impaired."

67. There is no doubt in my view that the detention of persons on the basis that they had downloaded the Bylock App is arbitrary and in breach of Article 5 of the convention.

ARTICLE 6

68. Article 6 guarantees a person a fair trial. The trial in Turkey convicted X on the basis of a technical report assessing the Bylock App, in the transcript of the judgement the court quotes the conclusion of the report namely that *"Bylock has been offered to the exclusive use of the members of FETO/PDSY terrorist organisation."*

69. It follows that once any suspect is found to have used the Bylock App, as it is allegedly for the exclusive use of the terrorist organisation FETO/PTY then membership of the organisation is proved with no other evidence being necessary. Although in the case of X alleged supporting evidence was claimed to have been found in the form of having a bank account at BankAsya and having stayed at student accommodation associated with the Gulen movement. It seems unlikely that the last two aspects of the evidence could prove membership of the allegedly terrorist organisation by themselves and they must be viewed as support for the main and decisive evidence of membership which stems from the use of the Bylock App.

70. It is a fundamental principle of a fair trial that a suspect has the right *"to examine or have examined witnesses against him"* this is enshrined in Article 6(3)(d). The use of the technical report at trial as evidence is a clear breach of this convention right. The authors of the report were not identified, they did not give evidence, no-one knows who they are, their qualifications and experience are unknown and the mechanism by which they arrived at the crucial conclusion upon which any verdict will turn is not revealed. No questions can be asked of the authors of the report and they cannot be

asked to provide any explanation for the fact that the App has been downloaded in over 40 countries many with no connection to Turkey, nor can they be asked what evidence they relied upon to come to the belief that the downloading in countries other than Turkey was by members of the terrorist organisation involved in the failed coup.

71. In addition Article 6 guarantees an independent and impartial tribunal established by law. The Grand Chamber has explained *"it is of fundamental importance in a democratic society that the courts inspire confidence in the public and above all, as far as criminal proceedings are concerned in the accused."* In order to achieve this objective a judge needs to be independent, impartial and not subject to threats of dismissal if cases are decided in a particular way. The Court will look at factors such as the manner of appointment of judges, the duration of their term of office, the existence of guarantees against outside pressure, and the appearance of independence.

72. On the material before me I note that The Country Report on Human Rights Practices for 2016 the US Department of State noted that 3,000 members of the judiciary were suspended, detained, fired and/or had their personal assets frozen following the failed coup. Which it reported *"had a chilling effect on judicial independence?"* Some 956 new judges have been appointed. This conduct by the state strikes at the heart of judicial independence and also appears to be a further clear breach of Article 6.

73. A more fundamental question arises in relation to whether the trial process as a whole is fair. The ECtHR will not normally consider the admissibility of evidence or the weight given to the evidence by the domestic courts. However in this case the Court is faced with a unique situation where there has been arbitrary detention in breach of Article 5 and a trial where there is no evidence capable of proving the accused's guilt. In these circumstances it cannot be said that any trial held in these circumstances is *"fair"* and the court may be persuaded to take a broader look at these trials and form a view as to overall fairness, although the easier route may be to focus on the clear breach of the right to examine witnesses and the lack of judicial independence.

74. However the courts approach the problem there are in my opinion clear breaches of Article 6 in the trial of X.

ARTICLE 7

75. Article 7 protects the citizen from retrospective legislation. It protects against being guilty of a criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time it was committed. This right is not subject to derogation under the Convention.

76. In the case of X there was no evidence of any membership or support for the Gulen movement the addition of the movement to the list of terrorist organisations membership of which was prohibited. The evidence relied upon to prove a connection

to the Gulen movement all predated the naming of the organisation in the prohibited list. Put another way use of the Bylock App was established only when membership of the Gulen movement was not illegal. There was no evidence after the addition of the movement to the prohibited list of continuing membership or support.

77. Furthermore the supporting evidence of banking at BankAsya and staying at the student accommodation also pre-dated the addition of the movement to the prohibited list of organisations. Such activity not being illegal at the time.

78. So the position is that the conviction of X is based entirely on conduct that pre-dated the addition of the Gulen movement to the list of registered terrorist organisations in Turkey. This is clearly a breach of Article 7. Taken at its highest, all that the evidence cited in the judgement could have proved was that, before the movement was added to the list of terrorist organisations, X had downloaded and used the Bylock App, banked at BankAsya and stayed in certain student accommodation. All activities perfectly lawful at the time he engaged in them and at a time when membership and support of the Gulen movement was also legal.

79. In these circumstances to convict of membership of a terrorist organisation on the basis of this evidence is clearly retrospective criminality and a clear breach of Article 7.

80. As a general principle the ECtHR will not normally interfere with the interpretation of national laws by the domestic courts but an exception to that is made in the case of

alleged Article 7 breaches. Where Article 7 is being considered the Grand Chamber will examine whether there was a contemporaneous legal basis for the conviction that was not incompatible with Article 7.

CONCLUSION

81. There are clear breaches Articles 6 and 7 of the European Convention of Human Rights in the trial transcript that I have read.

82. In addition the detention of huge numbers of citizens following the failed coup was arbitrary and based on a deeply flawed belief that the use of the Bylock App proved membership of the prescribed group. The individuals so detained had their convention rights under Article 5 breached and if their trials were conducted in the same way as the trial of X then there would also be a breach of Articles 6 and 7.

83. Under Article 34 of the convention the ECtHR may receive applications from any person, non-government organisation or group of individuals claiming to be the victim of a violation of one of their convention rights. An application can certainly be made in this case.

84. It may be that further breaches have occurred but I am unable to come to a conclusion in relation to that in the absence of further evidence. Allegations of torture have been

made which if true would be a breach of Article 3. The failure to permit discussion about the aims and objectives of the Gulen movement could also breach Article 9 but I do not have sufficient material to form an opinion on this,

85. On the material before me there is strong evidence that some of those detained following the failed coup have been tortured. That is the view of Amnesty International and numerous other human rights organisations. Unfortunately the evidence does not disclose who was responsible for the torture, who authorised it and who approved it. Without such evidence it is not possible to bring any individual to justice. However, if the identity of those could be established, then that would be an international criminal offence over which the courts of this country would have jurisdiction pursuant to Sections 135 & 136 of the Criminal Justice Act 1988. The consent of the Attorney General would be needed before proceedings could be instituted.

86. It follows that were evidence to be forthcoming of torture then those who the evidence identified as responsible could be placed on trial in this country subject to the Attorney General giving consent.

WILLIAM CLEGG QC
SIMON BAKER
25th July 2017

ANNEX ONE – FORENSIC REPORT OF THOMAS MOORE

Report of Thomas Kevin Moore

Dated	:	July 24th 2017
Specialist Field	:	Digital Forensics

[redacted]

On the Instructions of	:	William Clegg QC of 2 Bedford Row, London WC1R 4BU
Subject Matter	:	Analysis of a technical report into the functionality of the byLock messaging application

Mr Thomas K Moore

Suite C, City House

96a High Road,

Beeston

NOTTINGHAM NG9 2LF

Telephone: 01773 770 267

Fax: 01773 770 268

E-mail: tom.moore@marclay.co.uk

1. Table of Contents

2. Introduction

2.1. The Writer

I am Thomas Kevin Moore. My specialist field is computer forensics, in particular the recovery of information from **computer systems** and the subsequent analysis of this information.

I have been a computer forensics specialist for approximately 15 years. I have acted as an expert witness under instruction from law firms in the United Kingdom and Europe. I have recovered data from **computer systems** and storage media and I am experienced in examining electronic evidence and hardcopy reproductions. I have presented evidence and expert opinion in cases in the UK and overseas. I have developed guidelines and delivered training in the handling of digital evidence. I am a professional member of both the British Computer Society and the Expert Witness Institute.

Full details of my qualifications and experience entitling me to give expert opinion evidence are in Appendix A.

2.2. Summary Background of the Case

This case concerns a number of individuals, who were arrested following an attempted coup in Turkey on July 15th 2016. I understand that these individuals were identified by way of communications records recovered from a server, which was used to handle messages sent and received through the *byLock* instant messaging application. I further understand that the recovery of such messages and the subsequent identification of the individuals was carried out by Millî İstihbarat Teşkilatı (MIT), the Turkish national intelligence agency. Representatives of MIT further produced a report on the byLock application, entitled *byLock Uygulamasi Teknik Raporu* (*byLock Application Technical Report*) (the 'MIT report').

I have been instructed to examine this report and to provide an opinion on the assertions made therein regarding the technical operation of the byLock application and the associated recovery and identification of users' details from the server used to administer the application and service.

2.3. Technical Terms and Explanations

80 I have indicated any technical terms in **bold type**. I have defined these terms when first used and included them in a glossary in Appendix B.

3. The Issues to be Addressed and a Statement of Instructions

3.1. Instructions

I have been instructed in this case by William Clegg QC of 2 Bedford Row, London, WC1R 4BU. I received instructions on June 22nd 2017. I was instructed to examine an English translation of the report entitled *byLock Uygulamasi Teknik Raporu* and to provide an opinion on the following:

- The accuracy of the technical assessment of the byLock application, it's mode of operation and the server-side computer system through which it was operated.

90 **3.2. Purpose**

I produce this report to provide independent assistance to the Court by way of objective, unbiased opinion in relation to matters within my expertise.

3.3. Issues

I will address the following issues in this report:

- To what extent can the technical opinion in the report entitled *byLock Uygulamasi Teknik Raporu* be relied upon as true and accurate?

4. My Investigation of the Facts

I have been provided with a copy of the English translation of the report entitled *byLock Uygulamasi Teknik Raporu* which, I am advised, is a professionally certified translation.

My investigation of the facts is based upon this evidence and, where appropriate, the introduction of supporting factual information based on my own tests and research.

4.1. Assumed Facts

I have not been asked to assume any other facts without first verifying these to my satisfaction through my own examinations. I set out the nature of such examinations in sections 4.2 and 4.4 below.

4.2. Enquiries / Investigation into Facts

I have carried out a series of investigations based on the documentation supplied to me and in the context of the issues outlined in section 3.3. The full details of these are included in section 4.6.

4.3. Documents

In compiling this report, I have examined several documents, both from my instructing solicitor and a variety of other sources. A full list of documentary sources is included in Appendix C.

4.4. Interview and Examination

I did not deem it necessary to carry out any interviews in relation to this matter, save as described in section 4.6.

4.5. Research

I did not deem it necessary to carry out any research in relation to this matter, save as described in section 4.6.

4.6. Measurements, Tests and Experiments

My opinion is based upon a review of the documentary evidence provided to me. I did not deem it necessary to carry out any measurements, tests or experiments in relation to this matter.

130

5. Opinion

5.1. Issue 1

To what extent can the technical opinion in the report entitled byLock Uygulamasi Teknik Raporu *be relied upon as true and accurate?*

byLock was a publicly available smartphone application that allowed users to communicate between each other privately and using encryption. It was available to download via the Google Play store onto handsets running the Android operating system and via the Apple iTunes Store onto handsets running the Apple iOS operating system. Although the application was removed from these locations some time ago, unofficial versions are still available via third-party websites, although the installation process for these versions is less straightforward and requires a greater level of technical expertise. byLock was designed to operate in a similar way to other secure communications applications such as *Telegram*, *WhatsApp* and *Silent Circle*. Significantly, the application allows users to...

- hold secure voice over internet protocol (VoIP) calls
- send and receive encrypted instant messages, which may be configured to self-destruct after a specified period
- exchange images, documents and videos securely

byLock employed a client-server architecture and content transmitted between users was processed via a centralised server. Privacy was maintained by a scheme of private security keys, which were generated for each new user when the application was downloaded and installed. Very little official documentation exists relating to the application but it appears that these private security keys were sent to the byLock server using passwords were stored there in plain, unencrypted text. As a result, should the server be compromised, all message traffic and user data stored thereupon would be vulnerable and could potentially be decrypted. Furthermore, the server represented a single point of failure and any disruption to the server's operation would cause the byLock message service to stop functioning.

Availability of byLock through the Google Play Store and Apple iTunes Store

Para. 2.3 of the MIT report states that...

There are two basic version of the [byLock] *app which could be named as "serie 1" and "serie 2" which works on the Android operating system. Serie 2 was also called "ByLock++" so as to offer*

160 *it as a new app on a different page of Google Play.*

It is understood that "ByLock 1.1.7", the last of the serie 1 versions, was updated in December 2014. Subsequently, ByLock++ (serie 2) was released and made available until it was removed from Google Play all together. The approximate dates of the versions are shown in Appendix-1, screenshot of the approximate number of downloads from Google Play is shown in Appendix-2.

byLock was publicly available for download via the Google Play Store and Apple iTunes Store. A review of the application history on the Google Play Store shows the following event timeline[1]:

Date (in descending chronological order)	
April 3rd 2016	Application unpublished
January 19th 2015	Milestone of 100,000+ installs
December 27th 2014	Update to version 1.1.7 (last recorded update)
September 7th 2014	Update to version 1.1 6
September 1st 2014	Update to version 1.1.5
August 28th 2014	Update to version 1.1.4
August 24th 2014	Milestone of 50,000+ installs
July 15th 2014	Update to version 1.1.3
June 29th 2014	Category Moved from News & Magazines to Communication
June 29th 2014	Update to version 1.1.2
June 1st 2014	Milestone of 10,000+ installs
May 28th 2014	Update to version 1.1.1
May 20th 2014	Installs 5,000+
May 20th 2014	Update to version 1.0.8
May 16th 2014	Update to version 1.0.7
May 12th 2014	Update to version 1.0.5
May 4th 2014	Milestone of 1,000+ installs
April 30th 2014	Update to version 1.0.1
April 24th 2014	Milestone of 100+ installs

[1] Refer to https://www.appbrain.com/app/bylock%3A-secure-chat-talk/net.client.by.lock

April 22nd 2014	Milestone of 50+ installs
April 11th 2014	New application

Similar detailed timeline information is not readily available for the Apple iTunes Store. However, it has been possible to obtain historical data relating to the popularity ranking for byLock in the Turkish marketplace iTunes Store[2]. Ranking data shows the relative popularity of an application compared to both the entire body of available applications and other applications in a subset, segregated by function. In the case of byLock, historical data shows that the application was first ranked on April 28th 2014 and last ranked on September 7th 2014. Data from the iTunes Store (United States market) shows a minor variation, with initial ranking six days earlier, on April 22nd 2014.

Furthermore, historical ranking data is available for the iTunes Store service for other regional markets[3]. This data shows that the byLock messaging application was ranked in the category of 'Social Networking' applications in 63 countries overall and achieved a ranking in the top one thousand such applications in 60 of these countries.

Promotion of the byLock application

Para. 2.4 of the MIT report appears to suggest that the developer of byLock refrained from promoting or advertising the application, with the intention of limiting the number of new users. There is some evidence to support this assertion in a blog entry dated November 15th 2014[4], which appears to have been written by the developer of byLock and posted online and in which he states…

> *"First of all, I really appreciate your great interest, that byLock has approximately 1M registered users, which is beyond my expectations. Handling that many users is very difficult, and it is increasing day by day. To slow it down, I Unpublished my app from AppStore a few weeks ago. It helped a lot, but not that much."*

This statement does support the assertion that the developer sought to limit the registration of new byLock users. However, contrary to the assertion in the MIT report, the language used in this post

[2] Refer to https://www.appannie.com/apps/ios/app/bylock/rank-history/?vtype=day&countries=US,TR&start_date=2014-04-13&end_date=2014-09-07&view=rank&legends=22%7C02

[3] Refer to https://www.appannie.com/apps/ios/app/bylock/app-ranking/?type=best-ranks&date=2014-09-07

[4] Refer to https://bylockapp.wordpress.com/

suggests, in my opinion, that this was due to the inability of the developer's technical infrastructure to handle such an unforeseen volume of users, rather than for any reasons relating to anonymity. Indeed, there is no evidence to suggest that a greater number of users would impact upon anonymity or security but it is apparent that rapid growth would affect the performance of the application.

According to the MIT report, the byLock application relies upon a client-server model for the processing and delivery of messages. Each message sent by a byLock user is effectively uploaded to a server and made available for delivery to the intended recipient. As part of this process, the message itself, along with various metadata, is stored in a series of database tables on the server. Again, according to the MIT report, at the time that the byLock server was seized, it contained records of more than 17million messages and 215,092 registered users. No analysis appears to have been undertaken of the load placed upon the byLock server by such activity but it is quite possible that was was nearing operational capacity. In such a case, it is, in my opinion, entirely reasonable that a developer would seek to restrict the registration of new users until infrastructure capacity could be increased.

Furthermore, I note from the MIT report that byLock was not offered on a commercial basis and that it was not possible to establish any credentials for the developer. The description given of the mechanism by which new users could download and register with the byLock application suggests that no payment was required and it is explicitly stated that the application contained no advertising. This being the case, it appears that the person responsible for developing and administering byLock did so on a non-commercial basis. It is not uncommon, in my experience, for such projects to gain market traction more quickly than expected and, as a result, outgrow their development infrastructure in short order. Without commercial revenue to support additional infrastructure, the only viable option is to restrict user activity by, for example, limiting awareness of the application or restricting access by jurisdiction or market segment. Since social networking services are dependent upon a critical mass of users, such measures which restrict user uptake are generally a short-term solution and, in the absence of a longer-term strategy for increasing operational capacity, such services tend to cease operation.

Use by organisations

Para. 2.4 of the MIT report states that "...usage for organizational purposes and subjects has been observed". It is far from clear, however, how this conclusion has been arrived upon or, in fact, what is meant by 'organizational purposes'.

It is true to say that instant messaging applications are commonly used for social purposes, but it is increasingly common to find that businesses, community groups, charities, criminal gangs and even terrorist organisations make use of these services to communicate with customers, members and associates. Indeed, the use of the *Telegram* messaging application by ISIS has been widely reported[5]. It would not, in my opinion, be surprising, therefore, if byLock had been used by organisations as well as individuals.

Method by which the byLock server was accessed

It is apparent from the content of the MIT report that access was gained to content held on the server through which the byLock application processed messages, user registrations and so on. Extensive reference is made to the database structures which facilitate the operation of the application and a large volume of user registration and messaging data has apparently been recovered. Para. 3.1 of the MIT report suggests that such access was obtained by exercising powers granted to the Turkish intelligence agencies under national legislation. It is not stated whether the application developer was complicit in facilitating such access or in the subsequent analysis of the byLock server-side technology.

Notable, however, various e-mails and attachments are partially reproduced under para. 3.5.4 of the MIT report. Of particular relevance is the e-mail shown on p.14 of the report, which has been reproduced as a screenshot from the *Yandex* webmail service. Reference to the e-mail header shows that this message was sent to the e-mail address 'dashjohn@yandex.com'. According to the account information in the top right-hand corner of the screenshot, this same user is logged in to the webmail interface at the time the image was captured. This implies that the person responsible for capturing

[5] Refer to http://www.washingtontimes.com/news/2017/jan/8/isis-using-telegram-app-to-broadcast-terror-instru/

the screenshot had either deduced the account password for 'dashjohn@yandex.com' or was being assisted by the account holder.

byLock search statistics

Para. 3.3 of the MIT report shows two graphs, which are reproduced below for ease of reference[6]. The first of these (fig. 1) indicates the number of searches carried out for the term 'bylock' through the Google search engine from Turkish locations in the period December 17th 2013 to February 17th 2016. The second graph shows similar information but includes additional data series showing the number of searches carried out from locations in France, the United Kingdom and the United States.

fig. 1 Relative search interest for term 'bylock' (Turkey only)

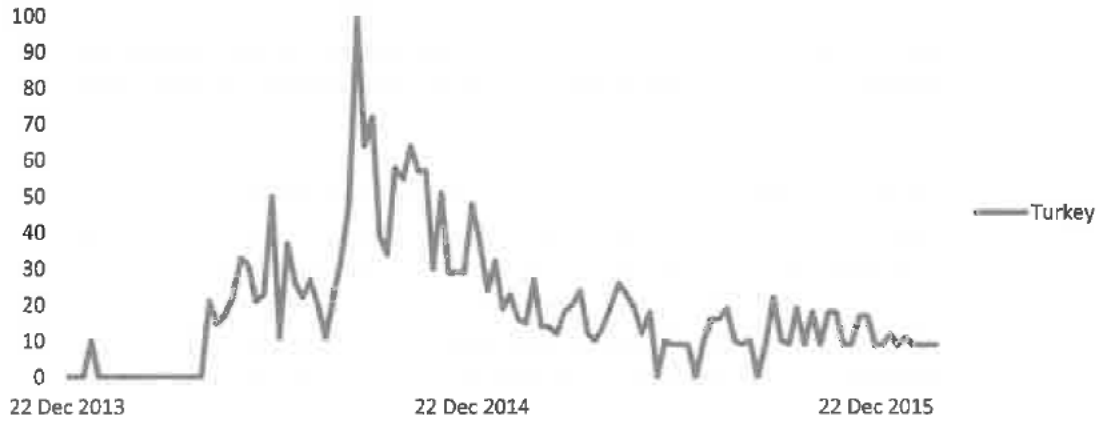
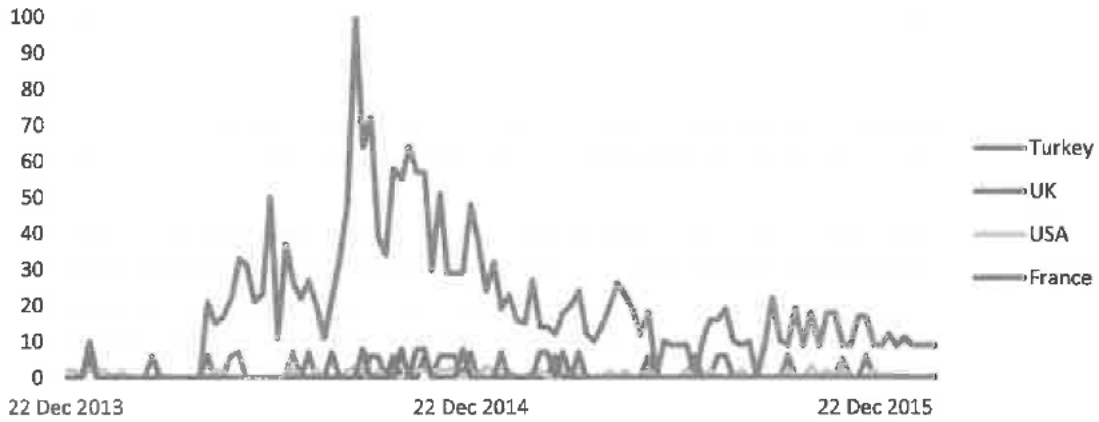


fig. 2 Relative search interest for term 'bylock'



[6] Source: Google Trends source data for the search term 'bylock' in the period 17-Dec-2013 to 17-Feb-2016

These graphs show only the number of searches made from each location and only through the Google search engine. Despite this limitation, the author of the MIT report asserts that "*it is believed that searches made from outside of Turkey had been made by members of the organisation who lived abroad or by Turkish users who were utilizing VPN*". However, no evidence whatsoever is presented to justify this statement. The graphs do not give any indication of organisational affiliation for the individuals conducting each search and cannot be used to determine whether virtual private networks were in use at the time each search was conducted. This assertion within the context of the report is, therefore, without justification and is entirely speculative.

Internet postings relating to byLock

It is further alleged, at para. 3.3 of the MIT report, that "*the vast majority of users who posted content about "ByLock" before July 15, 2016 are observed to have [also] been posting content in support of the FETO/PDY*". Such an assertion should be relatively straightforward to demonstrate by way of a reproduction of the various online posts made by these users. Again, however, there appears to be no such evidence in the report to justify this statement.

Use of Turkish language in the byLock source code

It is alleged, in para. 3.4.2.1 of the MIT report, that a disassembler was used to reverse-engineer the source code which constituted the client-side byLock application. Such so-called *decompiler* tools are readily available and provide a means by which underlying source code, albeit potentially in a limited form, may be derived using only the distributed form of an application. The fact that MIT were able to gain access to underlying source code does not, in itself, therefore, serve to demonstrate that the developer of byLock was complicit in their investigation.

It is noted that phrases in the Turkish language were identified in the byLock source code but it is not stated whether the application provided a facility to customise the user interface. It is relatively common, where an application is designed for use internationally, for the developer to include options to change the primary language in which prompts, system messages and so on are displayed. This being the case, it would be reasonable to expect that translations of phrases from the application would be present in the source code.

Network model for the byLock application

Para. 3.5.1 of the MIT report includes a diagram which allegedly "*...illustrates the operation of ByLock and the software running on application servers*". Again, however, it is unclear how this diagram has been produced. In particular, the diagram shows elements of a network infrastructure which are clearly outside the scope of the byLock server. These could not be determined with any certainty purely from an analysis of the server or the client-side application.

There appears to be no evidence in the report to support the assertion that virtual private networks were a necessary component of the infrastructure required to send and receive messages. Furthermore, in para. 3.6.2.11 of the MIT report, is it stated that the IP addresses recorded in the application database on the server were used to identify each individual user of the byLock service. Had the system been configured with VPN services in place as shown in the report, however, the IP address records held in the byLock database could not have been used to identify individual users, since one of the principal functions of a VPN in this context would be to obfuscate end-users' genuine IP addresses.

There are further glaring inconsistencies in the network diagram proposed in the MIT report. For example, it is generally accepted that the byLock application could be used to send and receive messages from mobile devices over mobile data networks. Despite this, a "home type wireless modem" has been included as part of the diagram. It is not clear what purpose this is intended to serve or why it is shown. Furthermore, the description of the cellular base station as belonging to "Turkcell, TurkTelecom, Vodafone" is misleading, since the byLock application appears to have been capable of communicating with its server from other mobile networks globally.

Blocking of IP addresses

Contained within para. 3.5.5 of the MIT report is an assertion that the administrator of the byLock application intentionally blocked Turkish IP addresses from sending and receiving messages through the byLock server, in order to force users within Turkey to route their traffic through a VPN service, thereby protecting their anonymity. The justification for this assertion appears to be a short post, which appeared on a byLock blog on November 15th 2014 and which is reproduced below for ease

of reference. In my opinion, the interpretation placed upon this blog post by the authors of the MIT report is highly subjective and, in the absence of other supporting information, thoroughly misleading.

In the post, the administrator appears explain that usage of the byLock application has significantly exceeded his expectations and that he has taken steps to limit further user registrations. Specifically, he refers to having removed the application from the 'AppStore' and goes on to explain that he has barred certain IP address ranges from accessing the byLock service, apparently due to malicious activity from these addresses.

Restriction on byLock Usage

Hi all.

First of all, I really appreciate your great interest, that byLock has approximately 1M registered users, which is beyond my expectations.

Handling that many users is very difficult, and it is increasing day by day. To slow it down, I UNpublished my app from AppStore a few weeks ago. It helped a lot, but not that much.

As an additional precaution, I also blocked some IP ranges (most of these ranges belong to middle east countries) because I detected some malicious connections from those IP blocks. Hopefully, this will also slow down the increase in byLock usage. If you encounter connectivity issues, try using some VPN service. There are lots of free ones out there.

Sorry for the inconvenience, but I had to do so. I hope my next app (byLock++, which is currently very buggy) will succeed in serving that many users. Hold on a little, it is on its way

Bye

The explanation advanced in the MIT report for restricting the IP addresses is curiously specific and overlooks a far more pragmatic and common explanation. In my experience, it is relatively common for systems that are exposed to the internet on public IP addresses to become the target of attacks, such as so-called *denial of service attacks*, where internet-facing servers are intentionally bombarded with high volumes of traffic such that they can no longer function properly. Building long-term resiliency to such attacks can be challenging and expensive and it is, therefore, relatively common for the operators of small-scale informal services to simply block the IP addresses from which the

attacks are thought to originate. Such action provides an immediate short-term remedy at the expense of potentially blocking legitimate service users whose IP addresses happen to fall within the blocked range.

On p.18 of the MIT report, a list of commands is given, which were allegedly used to block specific IP address ranges from accessing the byLock messaging service. Notably, however, these commands are not associated with blocking IP addresses. Eight commands are shown in total, all with the format...

```
iptables -A INPUT -s x.x.x.x/yy -j LOGGING
```

Such a command would not, in fact, block the specified IP address range but would, instead, create a rule for logging purposes. Such a rule would cause any access attempts from the specified IP address range to be logged for future reference. Interestingly, there is no reference in the MIT report to any log files containing access records for the server. An analysis of such logs, if available, may help to determine whether the server had previously come under attack and from which IP address ranges such an attack originated. This, in turn, might help in understanding the server administrator's motivation for blocking specific IP address ranges.

From a usability perspective, requiring registered users to implement a secure and anonymised VPN through which to access the byLock service would be an unusual strategy. Whilst feasible for technical users, configuring and using such a VPN service would present a significant barrier to use for less technically-capable individuals. Such a move could serve to actively disrupt communication between any established network of individuals, where such users' internet connections feature IP addresses within the blocked ranges. Indeed, no evidence is provided in the MIT report to suggest who may have been using the blocked IP addresses.

Use of IP addresses to identify individuals

There is a well-established complication with the notion of using IP addresses to positively identify individual users. Specifically, whilst IP addresses allocated to internet-facing devices are globally unique, the same cannot be said for IP address allocated to devices connected within local networks. For example, a household with a broadband internet service will typically have a wired or wireless router installed and connected to the incoming service. This router will have a unique public IP

address assigned to it, which may change periodically. For the time period during which it is assigned, it will be the only device connected to the internet globally with that specific IP address. Individual devices within the household will then typically connect to the router – either by a cable or wirelessly – to obtain access to the internet. These devices are not assigned *public* IP address but rather *private* ones. That is to the say that the IP address assigned to each device on a home network is unique within that network, but is not unique in a global context. Where an IP address is logged by a server such as the byLock server, it is the public IP address of the household that would be recorded, not the private internal address of the individual device. Where multiple individual devices are connected to a household or company internet connection, therefore, it is not possible to deduce, solely from the IP address logged on a server, from which specific device the access originated. From a practical perspective therefore, in a household or business with multiple individuals and devices, the logged IP address cannot identify one particular device or individual.

Paysera payment service

Para. 4 of the MIT report states that the byLock developer "...made the payment for the hire of the servers and IP addresses by anonymous means (Paysera)...". The inference that Paysera was used to facilitate covert payments is misleading in my opinion. Paysera is an established payment service, which operates in a manner comparable to more well-known services such as PayPal. Covert and anonymous payment services do exist (such as those employing Bitcoins) but there appears to be no suggestion that such facilities have been used in this case.

SSL certificates

Para. 4.4 of the MIT report notes that the byLock application employed a self-signed digital certificate and states that "*the application developer did not prefer 'authority signed SSL certificate' because he did not want user information transmitted to the certificate authority*". This is misleading and shows a fundamental misunderstanding of the manner in which digital certificates function.

Secure sockets layer (SSL) certificates are small data files that digitally bind a cryptographic key to a particular computer system. Such a certificate allows for the positive verification of a computer system's identity prior to transferring data. Typically, SSL certificates are used when data is to be transferred securely between private computers which are connected together using a public

network, such as the internet. Crucially, at no point is the data in transit routed through the computer systems of the certificate-issuing organisation.

Exclusivity of use

As covered above, the byLock application was available for download from the Google Play store and the Apple iTunes Store. There is no suggestion in the MIT report that downloads were restricted to a territory or jurisdiction. Since both application marketplaces are managed by their respective corporations, the developer of byLock, having made the application available for download, would have no direct control over who could obtain it. It is, in my opinion, therefore, nonsensical to suggest that it's availability was restricted to a particular group of people. It may, of course, be true that it was used by members of certain organisations or groups, but this is the case with many social networking and messaging applications.

I would, at this stage, draw the parallel with the Telegram Messenger application, which allows users to send messages between each other in an encrypted form and with the option to configure such messages to self-destruct after a specified time period. This application is publicly available in a similar manner to byLock, albeit on a larger scale, and is financed privately by Pavel DUROV. There is compelling evidence to show that Telegram has been used by ISIS as a secure communication tool and yet there is no move by law enforcement authorities to detain every user of the service. It is generally recognised and accepted that, with such services, there is a clear distinction between the functionality provided by an application and those who seek to use it for a variety of purposes. Critically, the use of an application for nefarious purposes cannot be said to prove that it was created for such purposes.

6. Statements

6.1. Statement of Compliance

I, Thomas Moore, DECLARE THAT:

1. I understand that my duty is to help the court to achieve the overriding objective by giving independent assistance by way of objective, unbiased opinion on matters within my expertise, both in preparing reports and giving oral evidence. I understand that this duty overrides any obligation to the party by whom I am engaged or the person who has paid or is liable to pay me. I confirm that I have complied with and will continue to comply with that duty.
2. I confirm that I have not entered into any arrangement where the amount or payment of my fees is in any way dependent on the outcome of the case.
3. I know of no conflict of interest of any kind, other than any which I have disclosed in my report.
4. I do not consider that any interest which I have disclosed affects my suitability as an expert witness on any issues on which I have given evidence.
5. I will advise the party by whom I am instructed if, between the date of my report and the trial, there is any change in circumstances which affect my answers to points 3 and 4 above.
6. I have shown the sources of all information I have used.
7. I have exercised reasonable care and skill in order to be accurate and complete in preparing this report.
8. I have endeavoured to include in my report those matters, of which I have knowledge or of which I have been made aware, that might adversely affect the validity of my opinion. I have clearly stated any qualifications to my opinion.
9. I have not, without forming an independent view, included or excluded anything which has been suggested to me by others, including my instructing lawyers.
10. I will notify those instructing me immediately and confirm in writing if for any reason my existing report requires any correction or qualification.
11. I understand that:

a. my report will form the evidence to be given under oath or affirmation;

b. the court may at any stage direct a discussion to take place between experts;

c. the court may direct that, following a discussion between the experts, a statement should be prepared showing those issues which are agreed and those issues which are not agreed, together with the reasons;

d. I may be required to attend court to be cross-examined on my report by a cross examiner assisted by an expert;

e. I am likely to be the subject of public adverse criticism by the judge if the Court concludes that I have not taken reasonable care in trying to meet the standards set out above.

12. I have read Part 19 of the Criminal Procedure Rules and I have complied with its requirements.

13. I confirm that I have acted in accordance with the code of practice or conduct for experts of my discipline, namely The Expert Witness Institute's Code of Professional Conduct.

6.2. Declaration

This statement, consisting of 26 pages each signed by me, is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it anything which I know to be false or do not believe to be true.

Signature _____ **Date** July 24th 2017

[redacted]

Appendix A Summary CV

Mr Thomas K Moore MBCS MEWI

Qualifications

Member of the British Computer Society, Member of the Expert Witness Institute

Career

Since 2001, I have specialised in the field of computer forensics. My expertise lies in the recovery of complete, deleted and damaged information from **computer systems** and in the analysis of such information.

I also have particular experience relevant to the analysis of **network** communications systems, especially those used in the provision and delivery of e-mail, internet and database services.

My instructions as an expert witness have come from law firms in the United Kingdom and Europe and my caseload is split approximately evenly between criminal and civil disputes.

I have provided evidence and expert opinion in cases in the UK and overseas and I am a consultant to public and private organisations in the development and delivery of digital forensics training, handling standards and best practice in digital evidence.

Case History

I have acted in a number of cases and prepared expert reports on matters including the following...

- The unauthorised access by individuals to corporate information and **computer systems**
- The use of computers to tamper with financial records for the purposes of theft
- The use of computers to send and receive e-mail messages pertinent to a very large scale financial fraud investigation
- The use of computers to post defamatory content on **internet** message boards
- The alleged use of computers to store and view indecent images

Training and Experience

I regularly undertake a variety of training both in respect of my professional field and in order to maintain and develop my skills as an expert witness.

I comply with the training and assessment requirements of my professional accrediting bodies and maintain a schedule of continuous professional development.

[redacted]

Appendix B Glossary of Terms

Allocated space	a portion of space on a computer's **hard disk** which is used to hold some or all of the contents of a current file
Allocation algorithm	the set of rules used by a **file system** to select the **clusters** that will hold some or all of the contents of a file
Boot	booting (booting up) is a process that starts an **operating system** when a user turns on a **computer system.**
CD-ROM	*compact disc read-only* ***memory***; a compact disc that contains data accessible by a computer.
Cluster	the smallest addressable unit of **hard disk** space which can be used to hold the content of a computer file
Computer network	an interconnected group of computers and associated equipment.
Computer system	a single computer or multiple computers designed to function in connection with each other.
CPU	*central processing* unit; sometimes just called **processor**; a description of a class of logic machines that can execute computer programs
CRT monitor	*cathode ray tube* monitor; a 'conventional' computer monitor using a vacuum tube containing an electron gun and a fluorescent screen (c.f. LCD or plasma monitors)
Diskette	floppy disk; a data storage medium that is composed of a disk of thin, flexible magnetic storage medium encased in a square or rectangular plastic shell
Ethernet	a family of frame-based computer networking technologies for local area networks (LANs)
FAT32	a **file system** used by various **operating systems**, including Microsoft Windows 95 and 98
File slack	unused **hard disk** space left over between the end of a file's content and the start of the next **cluster**

[redacted]

File system	a method for storing and organising computer files and the data they contain to make it possible to retrieve them
Fresh space	**hard disk** space which has not previously been used to store information and which is identified as available for storing new data
GHz	*gigahertz*; a measurement of frequency equivalent to 10^9 hertz (10^9 cycles per second); in modern computing, used to refer to the speed of the computer **processor**.
Hard disk [drive]	a form of permanent storage media for a computer, which retains data even when the power is turned off. Such disks are commonly installed within a computer's chassis but can be external.
Hardware	the mechanical, magnetic, electronic, and electrical devices comprising a **computer system**, as the **CPU**, disk drives, keyboard, or screen.
ICT	*information* [and] *communications technology*; an umbrella term that includes all technologies for the communication of information.
IP address	*internet protocol address*; a numerical label that is assigned to devices participating in a **computer network** that uses the Internet Protocol for communication between its nodes.
Memory	See ***RAM***.
Metadata	data concerning other data; a means by which to describe the characteristics or attributes of other information.
MHz	*megahertz*; a measurement of frequency equivalent to 10^6 hertz (10^6 cycles per second); in modern computing, used to refer to the speed of the computer **processor**.
Network	See ***computer network***.
NIC	*network interface card*; (networking) a piece of computer **hardware** designed to allow computers to communicate over a **computer network**.

	Operating system	the collection of **software** that directs a computer's operations, controlling and scheduling the execution of other programs, and managing storage, input / output, and communication.
	Partition	an area of a computer's **hard disk drive**
	PC	*personal computer*; a computer whose original price, size, and capabilities make it useful for individuals, and which is intended to be operated directly by an end user, with no intervening computer operator.
540	**Processor**	See ***CPU***.
	RAM	*random access* ***memory***; a type of computer data storage which commonly takes the form of integrated circuits that allow the stored data to be accessed in any order.
	Sector	a subdivision of a track on a magnetic or optical disk, each sector storing a fixed amount of data (typically 512 bytes in the case of magnetic disks)
	Software	a collection of computer programs, procedures and documentation that perform some tasks on a **computer system**.
	Unallocated space	Disk space which has previously been used to store information but which is now identified as available for overwriting with new data
550	**URI**	*uniform resource identifier*; a string of characters used to identify or name a resource on the Internet (for example, a web address)
	Virtual PC	a **software** product that allows multiple workstation or **server**-class virtual machines to run on one physical computer; the specification and **hardware** configuration of a virtual **PC** is usually specified by the user.
	VMware	a generic term referring to a range of **software** products by VMware Inc., some of which facilitate the creation and use of one or more **virtual PCs.**
	[Logical] volume	an instrument used to allocate data storage space on a mass storage device

Appendix C List of Documents

Reports & Opinions

byLock Uygulamasi Teknik Raporu (English translation) (undated)

Witness Statements (in ascending chronological order)

None

Exhibits

None

Interview Transcripts (in ascending chronological order)

None

Letters and E-Mail Correspondence

None