Upper Tribunal
(Immigration and Asylum Chamber)

XX (PJAK - sur place activities - Facebook) Iran CG [2022] UKUT 00023 (IAC)

THE IMMIGRATION ACTS

Heard at Field House and also via Teams	**Decision & Reasons Promulgated**
On 8 th to 10 th June 2021	.....

Before

THE HON. MR JUSTICE LANE

MR C M G OCKELTON, VICE PRESIDENT

UPPER TRIBUNAL JUDGE KEITH

Between

XX

(ANONYMITY DIRECTIONS CONTINUED)

Appellant

and

THE SECRETARY OF STATE FOR THE HOME DEPARTMENT

Respondent

Representation :

For the Appellant: Mr B Jaffey QC and Ms M Cleghorn , instructed by Halliday Reeves Solicitors

For the Respondent: Mr C Thomann , instructed by the Government Legal Department

Direction Regarding Anonymity – Rule 14 of the Tribunal Procedure (Upper Tribunal) Rules 2008

Unless and until a Tribunal or court directs otherwise, the appellant is granted anonymity. No report of these proceedings shall directly or indirectly identify him or any member of his family. This direction applies both to the appellant and to the respondent. Failure to comply with this direction could lead to contempt of court proceedings.

The cases of BA (Demonstrators in Britain – risk on return) Iran CG [2011] UKUT 36 (IAC); SSH and HR (illegal exit: failed asylum seeker) Iran CG [2016] UKUT 00308 (IAC); and HB (Kurds) Iran CG [2018] UKUT 00430 continue accurately to reflect the situation for returnees to Iran. That guidance is hereby supplemented on the issue of risk on return arising from a person's social media use (in particular, Facebook) and surveillance of that person by the authorities in Iran.

Surveillance

1) There is a disparity between, on the one hand, the Iranian state's claims as to what it has been, or is, able to do to control or access the electronic data of its citizens who are in Iran or outside it; and on the other, its actual capabilities and extent of its actions. There is a stark gap in the evidence, beyond assertions by the Iranian government that Facebook accounts have been hacked and are being monitored. The evidence fails to show it is reasonably likely that the Iranian authorities are able to monitor, on a large scale, Facebook accounts. More focussed, ad hoc searches will necessarily be more labour-intensive and are therefore confined to individuals who are of significant adverse interest. The risk that an individual is targeted will be a nuanced one. Whose Facebook accounts will be targeted, before they are deleted, will depend on a person's existing profile and where they fit onto a "social graph;" and the extent to which they or their social network may have their Facebook material accessed.

2) The likelihood of Facebook material being available to the Iranian authorities is affected by whether the person is or has been at any material time a person of significant interest, because if so, they are, in general, reasonably likely to have been the subject of targeted Facebook surveillance. In the case of such a person, this would mean that any additional risks that have arisen by creating a Facebook account containing material critical of, or otherwise inimical to, the Iranian authorities would not be mitigated by the closure of that account, as there is a real risk that the person would already have been the subject of targeted on-line surveillance, which is likely to have made the material known.

3) Where an Iranian national of any age returns to Iran, the fact of them not having a Facebook account, or having deleted an account, will not as such raise suspicions or concerns on the part of Iranian authorities.

4) A returnee from the UK to Iran who requires a laissez-passer or an emergency travel document (ETD) needs to complete an application form and submit it to the Iranian embassy in London. They are required to provide their address and telephone number, but not an email address or details of a social media account. While social media details are not asked for, the point of applying for an ETD is likely to be the first potential "pinch point, " referred to in AB and Others (internet activity – state of evidence) Iran [2015] UKUT 00257 (IAC). It is not realistic to assume that internet searches will not be carried out until a person's arrival in Iran. Those applicants for ETDs provide an obvious pool of people, in respect of whom basic searches (such as open internet searches) are likely to be carried out.

Guidance on Facebook more generally

5) There are several barriers to monitoring, as opposed to ad hoc searches of someone's Facebook material. There is no evidence before us that the Facebook website itself has been "hacked," whether by the Iranian or any other government. The effectiveness of website "crawler" software, such as Google, is limited, when interacting with Facebook. Someone's name and some details may crop up on a Google search, if they still have a live Facebook account, or one that has only very recently been closed; and provided that their Facebook settings or those of their friends or groups with whom they have interactions, have public settings. Without the person's password, those seeking to monitor Facebook accounts cannot "scrape" them in the same unautomated way as other websites allow automated data extraction. A person's email account or computer may be compromised, but it does not necessarily follow that their Facebook password account has been accessed.

6) The timely closure of an account neutralises the risk consequential on having had a “critical” Facebook account, provided that someone’s Facebook account was not specifically monitored prior to closure.

Guidance on social media evidence generally

7) Social media evidence is often limited to production of printed photographs, without full disclosure in electronic format. Production of a small part of a Facebook or social media account, for example, photocopied photographs, may be of very limited evidential value in a protection claim, when such a wealth of wider information, including a person’s locations of access to Facebook and full timeline of social media activities, readily available on the “Download Your Information” function of Facebook in a matter of moments, has not been disclosed.

8) It is easy for an apparent printout or electronic excerpt of an internet page to be manipulated by changing the page source data. For the same reason, where a decision maker does not have access to an actual account, purported printouts from such an account may also have very limited evidential value.

9) In deciding the issue of risk on return involving a Facebook account, a decision maker may legitimately consider whether a person will close a Facebook account and not volunteer the fact of a previously closed Facebook account, prior to application for an ETD: HJ (Iran) v SSHD [2011] AC 596. Decision makers are allowed to consider first, what a person will do to mitigate a risk of persecution, and second, the reason for their actions. It is difficult to see circumstances in which the deletion of a Facebook account could equate to persecution, as there is no fundamental right protected by the Refugee Convention to have access to a particular social media platform, as opposed to the right to political neutrality. Whether such an inquiry is too speculative needs to be considered on a case-by-case basis.

DECISION AND REASONS

1.
This is the re-making of the decision in the appellant’s appeal against the respondent’s refusal of his protection and human rights claims. The representatives and the Tribunal panel attended the hearing in person, while the appellant attended via Teams . He gave evidence on the third day of the hearing, with the assistance of a Kurdish Sorani interpreter, who also attended via Teams . The parties did not object to the appellant attending and giving evidence via Teams and we were satisfied that he was able to participate effectively in the hearing.

2.
We deal with the issues in the following order:

(i)
the background;

(ii)
the procedural history to the appeal;

(iii)
existing country guidance;

(iv)
the principal questions we have considered;

(v)

preliminary issues at the hearing;

(vi)
the evidence;

(vii)
our findings and conclusions; and

(viii)
the Country Guidance.

3.
The representatives provided written skeleton arguments and made substantial oral submissions. Rather than recite these in detail, we address their substance, and refer to them as necessary, as we progress through the findings and our conclusions. Finally, the error of law decision which this re-making decision follows is set out in the Annex to these reasons.

Background

4.
The appellant, an Iranian citizen of Kurdish ethnic origin, entered the UK unlawfully on 4th December 2017. He then claimed asylum, based on his fear of persecution because of his political beliefs, specifically his support for the Kurdistan Free Life Party (Partiya Jiyana Azad a Kurdistanê, ("PJAK")). He based his claim on his activities in Iran, where he had been persecuted; and in the UK, where he had attended demonstrations and set up a Facebook account, which included material critical of the Iranian government.

5.
The respondent refused the appellant's claim in her decision of 14 th February 2019. The appellant appealed that refusal, and the First-tier Tribunal ("FtT") Judge rejected his appeal on 12 th April 2019. The FtT Judge regarded the appellant's narrative of events in Iran as entirely fabricated and found that the appellant had no genuine political adherence to the PJAK, which was manufactured to bolster his asylum claim. His attendance at demonstrations in the UK and his Facebook account were opportunistic. The FtT Judge concluded that the appellant's activities in the UK would not result in a well-founded fear of persecution on his return to Iran. Faced with return, he would delete his Facebook account, which would have the effect of removing all "likes", comments, and other contents that the appellant had shared. The FtT Judge reminded herself of the risk factors set out in the Country Guidance case of HB (Kurds) Iran CG [2018] UKUT 00430. While the appellant was likely to be questioned on his return, because of his Kurdish ethnicity, he would not be regarded as having played a leading or organising role in the UK demonstrations he had attended. It was not even clear when and where these demonstrations had occurred and there was no evidence that they had attracted any media attention. None of the other risk factors in HB applied to the appellant.

6.
The appellant appealed against the FtT Judge's decision and FtT Judge J K Swaney granted permission on 10 th May 2019. Her permission to appeal was not limited in its scope.

Procedural history of the litigation

7.

Three case management review hearings have taken place: on 22 nd October 2019; 8 th June 2020; and 17 th December 2020, to identify and agree the list of factual questions to be put to Facebook about the storage and deletion of information on its website. The Vice President identified the following two issues at the case management hearing on 22 nd October 2019:

(i)
the extent to which authorities anywhere can recover data which the user has used his best efforts to delete; and

(ii)
the extent to which Facebook will help the user to do so.

8.
On 17 th December 2019, this Tribunal made anonymity directions. By the same date, the parties had agreed, and the respondent had put to Facebook, a list of questions. Facebook did not respond and following the case management review hearing on 8 th June 2020, this Tribunal issued an order to Facebook UK Limited on 3 rd July 2020, requiring a response by 28 th August 2020. Facebook Ireland responded initially on 14 th August 2020. The parties then put further questions to Facebook Ireland on 18 th December 2020, to which Facebook Ireland responded on 22 nd January 2021. This Tribunal issued final directions, following the case management review hearing on 17 th December 2020.

Existing country guidance

9.
We remind ourselves of some of the principles set out in Country Guidance and reported cases below.

10.
BA (Demonstrators in Britain – risk on return) Iran CG [2011] UKUT 36 (IAC). This case is authority for the finding that the Iranian government is unable to monitor all returnees involved in UK demonstrations. A decision maker must analyse the level of involvement of an individual, including the nature of sur place activities.

11.
SSH and HR (illegal exit: failed asylum seeker) Iran CG [2016] UKUT 00308 (IAC) confirms that status as a failed asylum seeker, with no prior adverse interest, will not, of its own, result in a risk to a returnee to Iran.

12.
HB sets out particular risk factors for those Iranians of Kurdish ethnic origin returning to Iran, even where political activity is “low level”.

13.
The reported case (but not Country Guidance) of AB and Others (internet activity – state of evidence) Iran [2015] UKUT 00257 (IAC), conceived the notion of a “pinch point” of risk on return at Tehran Airport.

Principal questions

14.
We consider the following questions and issues:

(i)

Facebook and other social media (§§69 to 72).

(ii)
Facebook accounts: their characteristics, publicity and permanence (§§73 to 84).

(iii)
Iranian state surveillance generally, and of Facebook, in particular (§§85 to 89).

(iv)
What Facebook material is visible to the Iranian authorities (a) on application for an emergency travel document ("ETD") and (b) on arrival at an Iranian port of entry (typically Tehran airport)? Will the visibility of material be affected by whether the person was previously a person of interest to the Iranian authorities? (§§90 to 96).

(v)
Will the fact of having no Facebook account on arrival in Iran cause the Iranian authorities to have suspicion or prompt further investigation? (§97).

(vi)
To what extent can a person be expected on return to their country of origin not to volunteer the fact of having previously had a Facebook account? (§§98 to 102).

(vii)
What difference does a Facebook account containing material critical of the Iranian authorities (whether deleted or not) make to the risk faced by someone returning to Iran? (§103).

(viii)
Does the appellant have a well-founded fear of persecution? (§§104 to 119).

Preliminary issues at the hearing.

15.
Two issues arose at the start of the hearing, both relating to the scope of our fact-finding. First, the parties disputed the scope of the preserved findings, on which we would base our decision.

16.
The findings which the parties agree are preserved are as follows. At §9 of her decision, the FtT Judge outlined the appellant's circumstances, where she recorded the appellant as being an Iranian citizen of Kurdish ethnic origin. He had lived in Iran with his parents and sister. He did not go to school and could not read or write. He worked as a farmer and smuggled goods over the Iran/Iraq border. He left Iran clandestinely and entered the UK without permission. He then claimed asylum. He was aware of discrimination against the Kurds but did not realise there was anything he could do about it. The FtT Judge recorded the appellant's claim of adverse attention in Iran because of distributing leaflets on behalf of the PJAK. The FtT Judge did not believe that account. She went on to find, in respect of UK activities, the following:

"27. I find the Appellant's activities as a supporter of PJAK in the UK are merely opportunistic. He told me that he enquired about PJAK in February or March 2018 when he was having his hair cut in Stockton and heard people talking about PJAK. He then told them that he was also a supporter and asked them to let him know about demonstrations and give him a lift to them. In my judgment if the Appellant was genuinely a supporter of PJAK and had risked his life to be involved in activities in Iran with the consequence that he had to flee the country, he would have made an effort to contact PJAK as

soon as he arrived in the UK in December 2017. I place little weight on the photographs of demonstrations and printouts from Facebook submitted by the Appellant. All they show is that he was present at some demonstrations and has asked to have his photograph taken with prominent members at meetings. In relation to the demonstrations whilst I accept that he was present I do not find that any of the photographs clearly show that people inside the Iranian embassy have taken photographs of him.

28. Furthermore, I find it lacks credibility that somebody who is illiterate has set up a Facebook account on which he shares messages supportive of Kurdish rights. In addition, I find it inconsistent that the Appellant claims that he does not wish to contact his family in Iran in case it puts them in danger but has no qualms about setting up a public Facebook page publicising his support for PJAK. When asked to explain this, he said that he did not believe this would put them in danger because Etela'aat are only looking for him."

17.
In preserving these findings in his error of law decision, Upper Tribunal Judge Dawson stated, at §20:

"20. … The decision is set aside solely in relation to the appellant's sur place activities and any risks that he would face as a consequence. The judge's findings as to the basis of the appellant's support for the PJAK in the United Kingdom (recorded at [27] and [28]) are preserved and, for the avoidance of doubt the judge's findings on the appellant's pre-flight activities are also preserved. Directions for a further hearing for the remaking of the decision in the Upper Tribunal will be issued in due course."

18.
The parties disagree on whether it follows that the appellant would close and delete his Facebook account (which the FtT Judge had found at §32 of her decision, but which Judge Dawson did not specifically preserve). Mr Thomann submitted that we must, as a matter of common sense, make such a finding, while Mr Jaffey QC argued that even if the appellant's sur place activities have been contrived, it does not follow that he would necessarily close or delete his Facebook account, or not volunteer the fact of such activities to the Iranian authorities, as to do so may place him at risk – instead, he may, with good reason, decide to make a "clean breast of it" on his return. We discuss this issue further, below.

19.
The second preliminary issue related to Mr Jaffey's suggestion that we only resolve general questions and remit the questions specific to the appellant's fear of persecution, and any necessary fact-finding, to the FtT. He suggested this because on the first day of the hearing, the appellant had not adduced any additional evidence about his personal circumstances, that had not been before the FtT Judge.

20.
Mr Jaffey accepted that this Tribunal had never given any indication that the appellant's specific case would not be fully resolved. While this was a case where we are invited to make general findings, it has always been listed as a re-making of the appellant's appeal.

21.
We did not accept that Mr Jaffey's proposed course was appropriate. On the morning of the first day of the hearing, we directed that the appellant must apply to adduce any additional evidence on which he sought to rely, by 4pm on the second day. He applied at the start of the second day. The respondent did not object and we granted the application. We have been able to make findings on the appellant's specific circumstances.

Evidence

22.
We were provided with a core bundle ('CB') running to 1,447 pages; a supplementary bundle ('SB'), which included the appellant's updated witness statement and excerpts from his Facebook account, on which he was cross-examined; and an authorities bundle. We heard oral evidence from two expert witnesses called by the appellant: Dr Richard Clayton; and Mr James Marchant, who also provided written reports. Given the extent of the written evidence, while we have considered it as a whole, we only refer to a small part of it where discussed by Dr Clayton and Mr Marchant, or where we regard it as necessary. We include excerpts of Facebook Ireland's responses, which Dr Clayton discusses. We also refer to a report which Dr Clayton cites and which we found to be particularly helpful: 'Iran and the Soft War for Internet Dominance,' written by Claudio Guarnieri and Collin Anderson dated August 2016, a copy of which was at pages [576] to [632] CB (https://iranthreats.github.io/us-16-Guarnieri-Anderson-Iran-And-The-Soft-War-For-Internet-Dominance-paper.pdf)

23.
Dr Clayton's evidence relates to how material published on a Facebook account may be viewed by others; and generally, how people's personal data (for example, their emails or other messages) may be accessed without their knowledge or consent.

24.
Mr Marchant discusses in his evidence the Iranian government's past record and likely current intentions in monitoring social media activity, including Facebook.

25.
We express our gratitude to both witnesses for the candour and clarity of their written reports and oral evidence. They are witnesses who were willing to concede limits in their expertise and we are satisfied that they have attempted to assist this Tribunal as independent experts, to the best of their abilities.

Dr Clayton's evidence

26.
Dr Clayton does not profess to be an expert in relation to Iranian politics or state activities, beyond his general reading. His unchallenged expertise is in computer science. He is currently a principal research assistant at the computer laboratory of the University of Cambridge, of status equivalent to that of a Reader. He also acts as the director of the Cambridge Cybercrime Centre which collects, collates and distributes data relating to criminal activity on the internet. His longstanding expertise in industry, before becoming an academic, includes building a computer program business, producing software for Amstrad games machines and a word-processor which was sold to Demon Internet, then the largest UK internet services provider in the mid-1990s, for whom he then worked until 2000. After 2000, he has studied for, and gained, his PhD at Cambridge University, and works in various aspects of computer security. He has acted as specialist adviser to the House of Lords and Commons Select Committees in relation to internet security. He has written or co-authored over 50 peer-reviewed professional publications. We accept, without hesitation, his particular expertise in how personal data, stored in email and social media accounts and on computers, can be accessed and monitored.

27.

One of the social media sites that Dr Clayton discusses in his evidence is Facebook. In his first report dated 9 th November 2020, a copy of which was at pages [172] to [179] CB, Dr Clayton deals with the issue of the privacy of users on Facebook, at §§36 to 47:

"36. Facebook exists to share information between people (and of course to show them advertisements and thereby make money) … and although there are some simple controls to limit sharing, the platform design is intended to make it easy to share data and hard to limit that sharing.

37. The privacy controls available on Facebook have varied over time and any description of current controls must be caveated by saying that the situation tomorrow may be different – and also that because of those changes, long time users of the platform may have expectations that their data can be seen by rather fewer people than is currently the case.

38. At present data such as lists of 'friends' and posts (both text and images) can either be shared with 'friends' or with the whole world. Additionally, information on which you can be searched: name, email address, phone number, can be restricted completely, or shared with 'friends', or with the whole world. There are more complex, fine-grained controls to add or remove people from sharing lists but they are complex to set up and will be used only exceptionally.

39. Where it gets rather complicated to understand is when people's 'friends' have different settings. So, I might not share my own list of 'friends' but one of my 'friends' may share their list – and I will appear on that. Additionally, even when 'friends' lists are not shared, when you visit my page you will [be] told if we have any mutual 'friends'.

40. Since, as explained above, a key aspect of monitoring a social network platform is to map the 'social graph' (who knows who) and thereby to find new people it might be worth collecting data about. Hence it's clear that an individual who wanted to be invisible to strangers would not only have to carefully set all of their own sharing options but also cajole their 'friends' into checking their privacy settings as well.

41. Besides individual accounts Facebook also operates 'groups' where like-minded people can share posts. The posts made in these groups may or may not default to only being visible to group members – and membership of the group may or may not be restricted. It is of course possible to determine what the situation might be, but the likely audience of a particular post will not be immediately apparent at the time it is made – albeit it is possible to delete or restrict the visibility of old posts.

42. At present Facebook has a wide array of complex and sophisticated privacy controls – so complex and sophisticated that it is unlikely that most people select anything other than the most basic 'share with the whole world' or 'share with the people in my list of friends'', although they may also pay some attention as to whether or not they want to be locatable by email address or phone number.

43. I have written 'friend' with quotation marks in my discussion above because on Facebook a 'friend' is someone who has asked to be added to your list of 'friends' and you have agreed to this. The decision to add may be based on actually knowing the person, or assuming that you do, or may just be based on them having an attractive photograph.

44. LinkedIn, the professional networking site is regularly reported to be overrun with fake profiles operated, it is said, by intelligence agencies – with the aim of establishing initial relationships which may then later be manipulated to the advantage of a foreign state.

45. The Associated Press wrote an article about the LinkedIn issue in June 2019 – it was only 'news' because it was claimed that the photo of the attractive female purporting to have the LinkedIn account was believed to have been computer generated: https://apnews. com/article/ be2fl9097a4c4fffaa00de67708a60d.

46. I have received invitations from fake Facebook accounts myself – probably because they wanted to send me spam rather than because I am of any interest to an intelligence agency – and it [is] known that this is an issue that it is borderline impossible for Facebook to monitor and block without doing themselves significant commercial damage by making account creation too hard.

47. Thus, although I make some mention below about the possibility of informants infiltrating themselves into groups and asking to become your 'friend' it is also possible for people to be socially engineered into forming a 'friend' relationship with a completely non-existent person."

28.
Dr Clayton also considers the issue of the identification of Facebook users, through looking at their photographs, at §32 of his first report:

"32. Facebook will 'tag' photographs of people with their identity – using an automated system for spotting facial similarities (with considerable assistance being given to the automation of Facebook being aware of all of the friends lists held on their system). This system may also provide hints of new people whose data may be of interest."

29.
Dr Clayton clarified in his oral evidence that the tagging of photographs has developed over time. He provided a supplementary letter, following his oral evidence to us, dated 10 th June 2021, which was inserted into page [1465] CB, in which he states:

"In my evidence I explained that my understanding was that facial recognition was automatically switched on, but I said that I had not checked this or conducted any tests. In response to a request passed on to me from Mr Thomann, I have now checked the position.

In 2019 Facebook retired an old "privacy" setting (this is far from unusual) and offered users a new setting (which my earlier investigation showed is "on" for XX's account).

Facebook's website contains useful information, and a video, about what this new setting does (and how they were drawing the attention of some of their users to the change):

https://about.fb.com/news/2019/09/update-face-recognition / and

there is a more detailed list of what it does at

https://www.facebook.com/help/122175507864081

The upshot is that at present it will be suggested to "friends" of XX that they tag him if he is recognised (viz: if the facial recognition technology flags a hit) in a picture that they post and XX will be told if he is recognised in any picture posted to a feed that he would be able (given relevant privacy settings) to view.

I also think I mis-spoke in my evidence when I said that German regulators were concerned about the use of facial recognition by Facebook. The German regulators were very concerned about what Facebook was doing back in 2012, but in more recent times they do not seem to have expressed an

opinion, albeit there are at present considerable concerns being expressed by NGOs and civil society groups in Germany about the use of facial recognition in a wide range of contexts."

30.
At this juncture we pause and turn to deal with the evidence from Facebook, on which Dr Clayton comments.

31.
We do not recite the correspondence from Facebook Ireland dated 19 th August 2020 and 22 nd January 2021 at pages [1450] and [1454] CB respectively in full, as several of the answers simply refer to generic policies or refer to earlier answers. The format is to answer, in brief terms, the questions that were posed by the parties to this litigation, because of this Tribunal's orders. Facebook Ireland, which is the corporate entity with legal accountability for providing Facebook services in the UK and the rest of Europe, does not regard itself as being bound by the Tribunal's order, but has provided the answers to questions, "on a voluntary basis as a one-time goodwill gesture." The parties' questions and Facebook Ireland's answers to them are set out below.

Facebook Ireland's evidence

"(a) What is the process whereby a Facebook user's personal account (hereafter "account") is "deleted"?

Answer: A Facebook user can deactivate their account temporarily and choose to come back whenever they want. Or they can choose to permanently delete their account by taking the following steps:

1. Select "Settings & Privacy" and then "Settings" at the top right of their screen;

2. Click "Your Facebook Information" in the left column;

3. Click "Deactivation and Deletion";

4. Choose "Permanently Delete Account", then click "Continue to Account Deletion"; and

5. Click "Delete Account", enter their password and then click "Continue".

(b) What is the effect of such a deletion upon the storage of posts by the user

a.
on his own account and

b.
on the accounts of others who have reacted to (i.e. "liked") and/or

c.
"shared" posts by the former account holder on their own personal accounts?

Answer: The effect of permanent deletion of a Facebook user account is as follows:

1.
The user cannot reactivate their account.

2.
Their profile, photos, posts, videos, and everything else the user added will be permanently deleted. The user will not be able to retrieve anything they have added.

3. The user will no longer be able to use Facebook Messenger.

4. The user will not be able to use Facebook Login for other apps they may have signed up for with their Facebook account, like Spotify or Pinterest. The user may need to contact the apps and websites to recover those accounts.

5. Some information, like messages the user sent to friends, may still be visible to those friends after the user deletes their account. Copies of messages the user has sent are stored in their friends' inboxes.

In addition, when a user chooses to delete something they shared on Facebook, we remove it from the site.

(c) Is such deletion permanent and/or "complete"?

Answer: Where a Facebook user chooses to delete their account, if it has been less than 30 days since the user initiated the deletion, they can cancel the account deletion. After 30 days, the user's account and all their information will be permanently deleted, and they will not be able to retrieve their information.

It may take up to 90 days from the beginning of the deletion process to delete all the things the user has posted. While Facebook is deleting this information, it is not accessible to other people using Facebook.

Copies of the user's information may remain after the 90 days in backup storage that Facebook uses to recover in the event of a disaster, software error, or other data loss event. Facebook may also keep user information for things like legal issues, terms violations, or harm prevention efforts.

Some information, such as messaging history, isn't stored in the user's account. This means their friends may still have access to messages the user sent after their account has been deleted.

For more information, please see Facebook's Data Policy (available at: https://www.facebook.com/policy.php).

(d) If not, what, if any, "digital footprint" is left by a personal account following deletion?

Answer: Please see the answers to questions (b) and (c) above.

(f)
Is there any distinction in this respect between the posts of an individual which were made available to the public generally and/or those only shared with specific individuals?

Answer: The meaning of this question is unclear. However, the Facebook user information which is always included on their public profile, to the extent provided by the user, includes age range, language, country, name, gender, username and user ID (account number), profile picture, cover photo and networks.

(l) Are you aware whether the Iranian authorities to have the capacity or ability to access a Facebook account/content once it has been closed down/deleted?

Answer: This question relates to the capabilities of a third party (the " Iranian authorities ") and therefore Facebook Ireland Limited is not in a position to answer.

(m)

Are you aware whether the Iranian authorities hold copies of Facebook data e.g. by screen prints/ captures or otherwise?

Answer: This question relates to the actions of a third party (the " Iranian authorities ") and therefore Facebook Ireland Limited is not in a position to answer.

(n)
Which third parties other than Facebook, if any, store personal account data following the deletion of an account?

Answer **:** This question relates to the actions of third parties and therefore Facebook Ireland Limited is not in a position to answer.

(o)
Does Facebook receive requests from the Iranian authorities for date concerning individual users (1) prior to and/or (2) after the deletion of their accounts?

Answer: Facebook has received requests from Iranian authorities for Facebook user data. There were a total of four such requests between July and December 2019 [8]

(p)
If so, how does Facebook respond to those?

Answer: Facebook responds to government requests for data in accordance with applicable law and our Terms of Service. For further information see Facebook's Transparency Report in respect of Iran: https://transparency.facebook.com/government-data-requests/country/IR "

32.
In their letter of 22 nd January 2021, Facebook Ireland states:

" In response to questions 5(b) and (c), you state that a user's information, once deleted, may remain after 90 days in backup storage that Facebook uses to recover in the event of disaster, software error, or other data loss event.

(a)
Can you confirm whether such backup storage is made available to state authorities upon request, and if so what conditions attach to such provision?

Facebook Ireland will search for and disclose data that is specified with particularity in an appropriate form of legal process and which we are reasonably able to locate and retrieve. However, Facebook Ireland does not retain data for law enforcement purposes unless we receive a valid preservation request before a user has deleted that content from our service. Formal preservation requests can be submitted by law enforcement through Facebook's Law Enforcement Online Request System, or via post (Facebook Law Enforcement Guidelines). As for "conditions" attaching to provision of data to law enforcement authorities, please see the answer to question (g) below.

Please also see the answer to question (e) below regarding emergency requests from law enforcement authorities.

In response to question 5(e), it is accepted that the information as to Facebook's awareness of historic "screen shots" being stored and/or distributed by companies linked to Facebook and/or others relates to third parties.

(b)
Can you nonetheless confirm whether Facebook Ireland Limited is aware of such storage and distribution by companies linked to it, and/or others?

Facebook Ireland reiterates that this question relates to the actions of third parties. Facebook Ireland has no control over this process and is therefore unable to answer this question.

In response to question 5(i), it is accepted that the information as to Facebook's awareness of the Iranian authorities' capacity or ability to access a Facebook account/content once it has been closed down/deleted relates to the capabilities of third parties.

(c)
Can you nonetheless confirm whether Facebook Ireland Limited is aware of such a capability?

Facebook Ireland is not aware of the Iranian authorities being able to access a Facebook account on the Facebook service once the account has been permanently deleted.

Facebook Ireland reiterates that it does not provide governments with direct access or "back doors" to people's information (se e Our Continuing Commitment to Transparency).

(d)
Can you confirm whether Facebook Ireland Limited is aware of any third parties storing personal account data following the deletion of an account?

This question is broad and vague, and Facebook Ireland is unable to speak to the actions of unnamed third parties.

However, before permanent deletion of a Facebook account, users can avail themselves of the "Download Your Information" " tool to obtain a copy of their Facebook information.

A user can download all of the available categories of information at once, or can select specific categories and date ranges.

In response to questions (o) and (p), it is noted that Facebook has received requests from the Iranian authorities for Facebook user data, and that there were a total of four such requests between July and December 2019.

(e)
Can you confirm what the category "Legal Process Request" encompasses?

"Legal Process Requests" include requests for user data that are accompanied by formal compulsory legal process, like a search warrant, subpoena, production order and similar instruments (see Facebook's Transparency Reports) .

"Legal Process Requests" do not include "Emergency Requests". In emergencies, law enforcement may submit requests without legal process. Based on the circumstances, we may voluntarily disclose information to law enforcement where we have a good faith reason to believe that the matter involves imminent risk of serious physical injury or death.

Since 2013 Facebook publishes biannual Transparency Reports concerning government authorities' requests for user data. These Reports set out, for both Legal Process Requests and Emergency Requests, the number of requests received, the number of user/accounts requested, and the percentage of requests where Facebook produced some data.

(f)

Can you confirm whether the information provided by Facebook Ireland Limited on request includes material in respect of accounts which the user has deleted?

Facebook will search for and disclose data that is specified with particularity in an appropriate form of legal process and which we are reasonably able to locate and retrieve.

However, Facebook does not retain data for law enforcement purposes unless we receive a valid preservation request before a user has deleted that content from our service. Formal preservation requests can be submitted by law enforcement through Facebook's Law Enforcement Online Request System, or via post (Facebook Law Enforcement Guidelines) .

Facebook discloses account records solely in accordance with our terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account.

I note the following statement: When something on Facebook or Instagram is reported to us as violating local law, but doesn't go against our Community Standards, we may restrict the content's availability in the country where it is alleged to be illegal.

(g)

Can you confirm the types of proceedings with respect to which Facebook Ireland Limited has responded favourably to requests for data and/or any criteria applied?

As mentioned in Facebook's Data Policy , we comply with government requests for user information only where we have a good-faith belief that the law requires us to do so. In addition, we assess whether a request is consistent with internationally recognized standards on human rights, including due process, privacy, free expression and the rule of law. We scrutinize every government request we receive to make sure it is legally valid, no matter which government makes the request. When we do comply, we produce only information that is narrowly tailored to respond to that request. If we determine that a government request is deficient, we push back and engage governments to address any apparent deficiencies. Where appropriate, we will legally challenge deficient requests. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account (see Our Continuing Commitment to Transparency).

As noted in the answer to question (e) above, since 2013 Facebook publishes biannual Transparency Reports concerning government authorities' requests for user data.

(h)

Can you confirm what, if any, criteria are applied by Facebook to determine whether local laws alleged to be violated comply with its Community Standards?

Facebook has developed a set of Community Standards that outline what is and is not allowed on Facebook. The criteria used to assess content on Facebook's platform against the Community Standards are described at length in Facebook's Community Standards and Community Standards Enforcement Report . Please also see Facebook's news room post at: : https:/ /about.fb.com/news/ 2018/04/comprehensive-community-standards/.

When governments believe that something on the internet violates their laws, they may contact companies like Facebook and ask us to restrict access to that content. Similarly, we may receive orders to restrict content from courts in the countries where we provide service, or requests from

non-government entities, such as members of the Facebook community, NGOs and charities. If, after careful legal review, we determine that the content is illegal under local law, then we make it unavailable in the relevant country or territory.

To learn more about the information Facebook restricts due to local laws, please review ou r Transparency Report – in particular under the heading " Content Restrictions Based on Local Law "

33.
Dr Clayton agrees with the accuracy of Facebook Ireland's comments, to which he has added his own, at §§49 to 51 of his first report (pages [176] to [177] CB).

"Deletion of Facebook accounts

49. Facebook are of course unable to cause data which has already been collected by a third party to be removed from such third party systems.

50. In particular, such engines are permitted to fetch information from many Facebook pages (there is a fairly obscure privacy setting for determining whether this is allowed for your own pages) and these search engines generally keep a 'cached' copy of the page for a period of time.

51. Thus although Facebook removes a deleted account immediately it may be possible to find some of the information about the account in a search engine cache. It is then relevant to note Facebook's explanation about images being stored on content delivery networks for some time after the deletion of the account. Essentially it is too expensive for Facebook to proactively remove this material so they leave it to age out and be discarded. Hence, the cached material at the search engine may display with the original images."

34.
Facebook users can set up a variety of "privacy" settings, but these are typically complex in nature. As a result, people tend either to have their account privacy setting as entirely "public," or to have posts shared with their "friends", because these are default settings set by Facebook and do not require adjustment by the user. However, Dr Clayton's view is that it is to misunderstand Facebook to think that merely because there is a privacy setting limited to friends, that only those friends can view the material posted by an individual user. Access also depends on the privacy settings of those friends.

35.
Dr Clayton adds that even after a Facebook account is deleted, which can be an irrevocable step, there is a delay, during which data which has been "cached" on internet search engines (like Google), which use "crawler software," may still be accessible for a period. Dr Clayton could not give a confirmed view as to how long any Facebook data was likely to be on a cache on a search engine as he had never done an experiment, but it was generally held for at least a few days after deletion, but it could be for a longer period.

36.
He also points out that a person's closure of their Facebook account will not affect data that has already been accessed and saved locally by a third party. In his experience, data monitoring, as opposed to ad hoc browsing, is not a "real-time" activity. Monitoring involves collection of data at scale, which is obtained and stored "just in case" and analysed later (§24 of his first report at page [174] CB). Dr Clayton continues, at pages [178] to [179] CB:

“ 64. I have been provided with the decisions from various immigration hearings and appeals which are relevant to the topics I have been asked to provide an expert opinion on. These decisions, and to a certain extent the questions I have been asked to address, show a rather old-fashioned view of social network monitoring.

65. The imagined scenario seems to be that someone arrives at the Iranian border, they reveal that they have a Facebook account and the immigration officer looks at the account and concludes that they have a dangerous subversive in front of them, marches them off to jail and throws away the key.

66. To counter this, it is suggested, the Facebook account should be deleted before the repatriation flight takes off – or more subtly, since duress might cause it to be resurrected, it should be deleted many weeks earlier in anticipation of travel.

67. The modern approach to monitoring, by any regime which sees value in collecting information about its opponents, would be to proactively scoop up any and all information from social networks that it can. There is of course a limit to quite how much data can be collected – monitoring a billion people would be unrealistic, but several tens of millions entirely plausible.

68. The first issue then, when someone arrives at the border, is the effectiveness of the search function – can social media posts be rapidly located and triaged sufficiently well by automated systems to ensure that human interrogators do not waste their valuable time on irrelevancies. In my view, an effective system is well within the capabilities of a country such as Iran.

69. The second issue is the extent to which the material that has been posted by the traveller, and the relationships that they have with people that the regime considers relevant, has been kept sufficiently private that it was never available to be scooped up by the monitoring systems.

70. As I indicated in the section discussing privacy controls, it is possible to set some very fine-grained controls – but most people will go for a broad-brush approach, perhaps choosing to share only with friends. However, since ‘friend’ is in practice ‘random person who once made a request to me’ it would only be the most paranoid of people whose friends consistently [sic] solely of highly trusted confidantes.

71. To summarise the conclusion, social networks are built so that people will share information about themselves. It is unrealistic, this decade, to suppose that anyone who has shared information has managed to keep that information out of the hands of regimes who view them as enemies.”

37.
As Dr Clayton reflects, it is not realistic to suppose that closure and deletion of a Facebook account by the time someone arrives at Tehran airport will mitigate any risk to the account user if they have been the target of focussed monitoring. In that case, it is likely to have happened substantially before their return.

38.
Dr Clayton explains how information on a person’s Facebook account could be monitored. Crucially, both he and Mr Marchant agree that there is no evidence that Facebook’s website and storage facilities themselves have been accessed illicitly or “hacked,” or that Facebook data can generally be accessed on a bulk, automated basis through “crawler” searches.

39.

Instead, access to someone's Facebook data can be obtained, to varying degrees, by one of three means, all of which are on a targeted basis. First, if a Facebook account has been set as fully public, any Facebook user can search their posts, friends, and some biographical data (as opposed to all their Facebook activity), although their data cannot be "scraped" in the same way as using the "Download Your Information" or "DYI" tool, which must be done by the account holder.

40.
Second, if a person's Facebook account has various privacy settings, preventing a search of their posts, a person wanting to know more about them could send them a "friend" request, using fake details. If accepted, the third party may look through their posts and contacts in the same way as in the first scenario.

41.
Third, if a person carrying out surveillance can find out a target's account name and password, they can download a very wide range of the target's Facebook data, in a matter of minutes, on to a separate file, using the DYI tool.

42.
Dr Clayton goes on to explain how someone's personal data, including their Facebook password, can be accessed without their consent – how they (as opposed to Facebook) can be "hacked."

43.
A common way is by "phishing," whereby a target is sent an email encouraging them either to reveal personal information (such as date of birth, often connected with passwords), or even worse, to open a computer program which then allows the information on their computer to be accessed, including their passwords. Software might, for example, take the form of a "keystroke logger," which logs what is being typed. It then transmits that information, which may include passwords, to the person carrying out the surveillance. The success or otherwise of phishing attempts depends on how targeted they are. Recent research by PayPal indicates that in a clumsy attempt, as few as 10% are successful. In more targeted attempts, called "spear phishing," the success rate can be as high as 90%. For example, if the recipient of a phishing email sees that the standard of written English is noticeably poor, they are more likely to be alerted to the attack, and not to respond to it. In contrast, if a phishing attack is successful, it is not uncommon for the attackers to send out emails from the victim's email address to their friends or associates in their list of email contacts.

44.
Dr Clayton also discusses how large amounts of data can be extracted swiftly by means of automated software – so-called "scraping." Some websites allow scraping through "web crawler" software, which may download large amounts of data on an automated basis, often for indexing purposes (internet search engines such as Google use crawler software). Facebook does not allow crawler access to the full range of users' data. At §§53 to 56, Dr Clayton deals with the situation of the Cambridge Analytica scandal, involving Facebook, where there was an attempt at automated data extraction (page [177] CB):

"53. The Cambridge Analytica scandal involved an app, which was installed by several hundred thousand willing participants from 2013 onwards, who answered survey questions to build psychological profiles. Behind the scenes, without permission, the app used a standard Facebook mechanism to collect the personal data of the friends of the people who had installed the app. This data was subsequently used for political advertising.

54. When this came to light in early 2018 Facebook removed the mechanism and gave the impression that this type of sharing was now a thing of the past, not least because they had to pay substantial fines imposed by various regulators.

55. However, an investigation by the New York Times in December 2018 found that Facebook had been sharing personal data, under various arrangements over various timeframes up to around 2017, with over 150 companies – namely for those companies to personalise the information (and adverts) which they served up to their customers.

https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html

56. There has been no public statement that I can locate that says that Cambridge Analytica app was the only (ab)user of the Facebook data retrieval mechanism, and although many of the 150+ companies with which Facebook shared data were well-known US corporations, one was Yandex, the Russian Internet services company. So, although it seems unlikely that large amounts of personal data were made available to the Iranian regime by means of the mechanisms I have just described, it cannot be entirely ruled out."

45.
Because Facebook does not generally allow crawler software to "scrape" data, Cambridge Analytica had to extract the data by other means.

46.
While Dr Clayton has posited the possibility that other commercial organisations may have access to Facebook data on a bulk basis, he does not suggest that Facebook has provided such data to the Iranian authorities. Indeed, Facebook's response, already referred to, at Answer 5(o) above, indicates their replies to four specific information requests from the Iranian government in a six-month period in 2019. Facebook also deploys considerable resources to trying to stop crawler access.

47.
How then could data extraction from Facebook be automated? Dr Clayton identifies DYI as one possible way, but that needs to be on a user-by-user basis. Automated attacks are likely to face two difficulties, even assuming someone's Facebook account name and password have been obtained.

48.
The first difficulty is that Facebook tries to monitor and stop unusual "scraping" activity, such as large numbers of connected users using the DYI tool, from the same IP address or networked computer. Dr Clayton is not able to comment on the level of activity that would prompt intervention. It is likely to be something of a "cat and mouse" game between Facebook and those attempting to "scrape" data. One way of trying to avoid detection is to use multiple IP addresses either from single or multiple computers, to spread the requests over several different locations and carry out "scraping" over a period, for example, over weeks. Dr Clayton personally has experience of using multiple IP addresses, which is inexpensive and easy for a government or computer laboratory such as his. Although the DYI process or "scraping" can be carried out in moments, in reality, Facebook's interventions stop or slow down any attempts at "scraping".

49.
The second difficulty, assuming that Facebook passwords have been obtained en masse, is knowing whom to target and what to look for. Given the number of Facebook users, unless parameters are put on an attempt at "scraping", by reason of the nature of social connections, those monitoring could

rapidly end up trying to “scrape” the data of all Facebook users, namely over two billion people, which would clearly be impractical even for a government with dedicated surveillance resources, such as the Iranian authorities.

50.
Dr Clayton’s opinion is that human input is needed to consider where to look for the proverbial needle in the haystack. Using his experience of hacking (lawfully) and observing criminal gangs on other social networks, any necessary focus is dependent on what is termed the “social graph,” or how networks of people may be related, and their relative importance. Dr Clayton gives the example of a group of friends who are in regular contact, with one person more on the periphery, with fewer interactions. They may attract less risk of being monitored. Human intervention is more costly than purely automated computer programs, but even with relatively limited resources, Dr Clayton’s team at Cambridge has “scraped” the data of around 10 million messages from a criminal gang who were using a supposedly encrypted chat channel called “Telegram.”

51.
Separately, Dr Clayton describes ways of covertly monitoring people’s internet use at §§57 to 63 of his report, (pages [177] to [178] CB), although these comments do not directly relate to the ability of the Iranian government to obtain a person’s Facebook password. He refers to “deep packet inspection” and “man in the middle” attacks:

“57. I have been asked to comment on the use of Deep Packet Inspection (DPI) for Internet monitoring.

58. The Internet is a packet-based system and the header of every packet gives the IP address of the destination for the packet, the IP address to which responses should be returned and an indication of the protocol that is in use. This information, which is relatively trivial to collect, can be used to identify the systems, and services being contacted by any user whose traffic is being monitored.

59. A DPI device considers the contents of the packets with a view to determining more detailed information about the communication. Thus, it is possible to pick out which particular web page is being visited, not just which website, or it is possible to scan traffic to see if there are any mentions, for example, of the name of an exiled opposition leader.

60. DPI is ineffective when communications are encrypted but there are still a great many websites on the Internet which do not use encryption. Additionally, it is possible to use a man-in-the-middle attack to view encrypted traffic. Essentially, each end of the communication has an encrypted link to the intervening node, which decrypts the traffic and then re-encrypts it for the second part of the journey – having had the opportunity to inspect it ‘in the clear’ as it passed by.

61. The technical defence against man-in-the-middle attacks is to use security certificates issued by trusted third parties. However, if the third party can be compromised and issues fake certificates then man-in-the-middle attacks can be made to work.

62. The classical example of this type of compromise was in August 2012 when the Dutch certificate issuing company DigiNotar was compromised and a number of fake certificates for email services and for google.com were issued. Investigations found that the main target of the attack was 300,000 Iranian gmail users and is widely believed that the Iranian government was complicit in the compromise of DidiNotar.

63. Returning to DPI specifically – in the current context, this is a technology which is suitable for identifying traffic on a particular network which is worth further investigation. Deploying it on the Iranian Internet would therefore allow the authorities to identify users to add to a watch list, or websites elsewhere in the world which might be blocked, or a list made of those who visited them. As such this is a technology which is more relevant to building watch lists than in day-to-day monitoring social network use."

52.
In his supplemental letter of 14 th April 2021, page [180] CB, Dr Clayton refers to two reports. The first is a report, "Computer Crime in Iran: Risky Online Behaviour" published by a campaigning group called "Article 19" in 2015, where at internal page [23], the report describes the claim of a person interrogated on his return to Iran, who was confronted with material he had posted on Facebook. The report suggests that there might be several reasons (not specified) why information is more publicly available than a Facebook user might intend or be aware. Dr Clayton refers to this as evidence of the likely interest of the Iranian authorities in scraping data.

53.
Second, he refers to Guarnieri and Anderson's report, "Iran and the Soft War for Internet Dominance" to which we now turn. The report gives specific detail of successful phishing attacks. It outlines that, in response to technology attacks upon itself, the Iranian state has actively attacked other companies, organisations and individuals. The authors are careful to qualify the state's capabilities, (page [576] CB):

"While Iran maintains strong technical universities and an extraordinarily active defacement community, the country has not invested in its capacity for internet-based espionage to the same degree as its traditional geopolitical rivals and is less able to seek capabilities abroad from companies … due to its pariah status."

54.
Nevertheless, the report goes on to detail Iranian "intrusion" efforts over a three-year observation period from 2014 to 2016 (page [578] CB). The authors go into a great level of detail about some of attacks they discuss, and they explain that this detail is needed to attribute the attack to the Iranian state, because of the use of proxies and the opaque nature of the activities. When an attack is discovered and/or publicised, attacks may be paused, or operations swiftly closed down. As a result, it may be difficult to construct a cogent narrative of specific state actors. However, by focussing on specific attacks, a pattern can be discerned. Attacks in some cases can be attributed, based on Iranian working patterns. For example, various attacks have paused during Iranian public holidays, when Iranian civil servants are not working, such as Nowruz, the Iranian new year.

55.
The authors discuss four attacks, in the period from 2010 to 2016, the first called "Infy" (page [579] CB), which targeted BBC Persian and other journalists with PowerPoint presentations. The presentations contained software which recorded keystrokes and transmitted them to the attacker's account, to steal credentials for social media and email accounts (page [588] CB).

56.
The second attack used software called "Ghambar," used by a group called "Cleaver" until at least June 2016 and included religious minorities as targets. The software included a keystroke logger and allowed the hacker to take control of infected computers; take screen shots; disable keyboards; and lock out users.

57.
The third attack was named “Rocket Kitten,” beginning in April 2014, which made phishing attacks on Israeli academic institutions, and used the compromised website of a British quilting society. It also compromised the accounts of Telegram users and collated the telephone numbers of some 15 million Iranian Telegram users within Iran. The same Iranian proxy group was said to have used a method whereby they successfully obtained a person’s Facebook password, by unknown means, and on an unspecified scale; downloaded their Facebook “DYI;” changed the email address linked to the Facebook account; impersonated the victim and then approached their contacts.

58.
Finally, the authors describe a proxy attack called “Sima,” in February 2016, which lasted for a relatively brief period until March 2016, when publicity resulted in it being shut down, where entire personas were generated, with false biographical details and their own websites, using “bait” documents relevant to their victims, such as a real report published by Human Rights Watch. The authors conclude that at least 21 people were compromised in that attack.

Mr Marchant’s evidence

59.
Mr Marchant does not claim to be a computer expert. His expertise is as the director of research of a campaigning and advocacy organisation for the rights of those wishing to publish social media material, without hindrance, in Iran and the wider Middle East. Consequently, he has practical experience of reviewing, over many years, publicly available material and reports about the Iranian authorities’ attempts to control and limit such freedoms, and the social media trends in Iran and the Iranian diaspora. He has been able to synthesise a large range of public reports in relation to the motives of the Iranian regime, on which he comments in his report. His organisation, Small Media, has also conducted some interviews with individual Iranians, notably members of the LGBTQI+ community, albeit on a limited scale. Mr Marchant is clear that he does not have any access to classified information, nor does he hold any security clearance.

60.
In his two reports, the first of which is undated but can be no earlier than 2020, because of its references, at pages [147] to [168] CB; and a supplementary report dated 12 th April 2021 at pages [169] to [171] CB, he deals with evidence of the Iranian authorities’ motivation in seeking to control social media.

61.
In his view, the Iranian state perceives all “on-line” activity as a threat to the Iranian state, prompting it to devote significant resources, over an extended period, to develop its own internet or “National Information Network” (“NIN”). Mr Marchant accepts in oral evidence that in its early stages, particularly around 2009, NIN was regarded as something of a joke; and that Iranian government announcements as to when NIN will be complete have shifted from one year to the next. Despite this, he refers to reports of the Iranian state’s capabilities as being extensive, with global reach. He reflects on reports in 2003, that the Iranian state had already filtered 10,000 websites, to prevent them from being accessed by those in Iran, although the BBC report cited for that proposition does not identify its sources. We accept, nevertheless, his analysis that the Iranian state either attempts to block entirely or produce what are called “forked” versions of social media channels (independently built versions of those channels, using their computer code, but modified, which can allow any activity on those channels to be monitored).

62.
The Iranian state's technological attempts are in tandem with its restrictive domestic legislation, notably a 2011 computer crimes law, which has since been criticised as a restriction on freedom of expression by the UN Special Rapporteur.

63.
Mr Marchant refers in his initial report, at page [153] CB, to a "military" exercise launched by the Iranian Revolutionary Guard Corps ("IRGC"), named "Eghtedare Sarallah" in 2015, in which the Iranian state claimed to have monitored the accounts of 8 million Iranian Facebook users, but without any other verification of that claim. Nevertheless, there is a consistency in at least the scale of the claims, with the establishment of an Iranian "Cyber Police" called "FATA," who boasted of recruiting 42,000 volunteers between 2014 and December 2018. Mr Marchant was careful to note that the veracity of the figures could not be confirmed (page [154] CB) and he is unable to comment on the recruitment criteria or process for such volunteers.

64.
Mr Marchant is, however, able to comment with direct experience on the model of control of high risk and politically sensitive groups, specifically a survey by Small Media in 2018 of 26 LGBTQI+ Iranian interviewees, one in five of whom reported attempts to entrap them by state agencies.

65.
Mr Marchant also refers in his report, at page [154] CB, to the IRGC announcing in May 2016 that they had arrested 170 people who had posted material on Instagram relating to fashion and design; and in 2018, FATA contacting high profile female Instagram bloggers, requiring them to remove content in which they did not wear the legally mandated hijab. Whilst Mr Marchant refers to the Iranian state buying telecommunications network equipment from a Chinese company, ZTE in 2012 (page [155] CB), which is capable of monitoring communications on the network, according to a former project manager of ZTE, Mr Marchant also accepts that there is no clear evidence that Iran has implemented facial recognition technology, to monitor citizens. He is not able to comment in detail on how ZTE surveillance equipment might work.

66.
Mr Marchant also refers to a report by the "Centre for Human Rights in Iran" of May 2019, when software was said to be used to target minority groups both within and outside Iran, to gather private information. The minority groups were identified as including Gonabadi Dervishes; Azeri dissidents; women's rights activists; and student activists.

67.
Mr Marchant refers at page 157 [CB] to a report by "Comparitech" in March 2020 that the use of a "forked" version of Telegram was said to have resulted in data from 42 million Iranian Telegram users being leaked online. He also refers to BBC Persian journalists being targeted (page [158] CB), with 157 individuals having their assets in Iran frozen; and a Canadian Iranian technologist who returned to Iran in January 2020 having his telephone, laptop and other information confiscated and being forced by the IRGC to hand over his passwords for his email and social media accounts. This is said to be one of the few occasions of an individual victim speaking openly of being intimidated into spying on the diaspora community, although the method of spying, and whether such spying activity had taken place, were not specified. Mr Marchant fairly accepts in oral evidence that other than the Comparitech report, no other claimed mass leaks of diaspora data have been reported, and even that leak cannot not be verified.

68.
Mr Marchant agrees that while the proportion of Facebook users in Iran may be declining, it remains important to the Iranian diaspora community. He also accepts, as a fair characterisation, the Iranian state's twin approach of targeting individuals; and intimidating the wider diaspora with boasts of activities. The dual approach is necessary as actual, targeted attacks are labour intensive, but he adds that no one to whom he has spoken is blasé about the increasing sophistication of attacks and the nearing to fruition of the NIN project. In the latter case, he gives the specific example, in 2019, of the Iranian state having shut down access to large parts of the internet, in response to public demonstrations, but the Iranian banking system still functioned. He also accepts that Facebook attempts to stop mass DYI downloads and data-scraping; and that state access to Facebook data can only be obtained by open requests (the "Legal Process Request procedure", referred to by Facebook in their answers), or by user consent, whether extorted or otherwise.

Findings and conclusions

Facebook and other social media

69. We do not propose to give an all-embracing explanation of Facebook. We deal with those areas necessary for the purposes of general guidance and in respect of the appellant's appeal.

70. We start with what we consider to be some uncontroversial findings regarding the nature of Facebook. Facebook is one of a number of "social media" or "social network" internet sites, which allow people to share information about themselves with others. Social network sites are in competition, and their active membership may significantly change over time. People may have initially used one website and then move to another, including when their group of contacts moves to a new network, or for reasons of privacy, to pick two examples.

71. Active use of particular social networks also varies from country to country. The phenomenon of political campaigning on Facebook and other social media platforms is well-known and for that reason in several countries with authoritarian governments, access to Facebook and other social media is either significantly controlled or banned entirely. Residents of those countries may attempt to circumvent those controls or restrictions, for example by means of a virtual private network or "VPN", as in Iran.

72. The changing landscape of social media use is exemplified by the increased popularity of Telegram, for a period, in Iran, because of its perceived data privacy. In contrast, Instagram has an enduring popularity in Iran, because of its ease of access. It is not blocked, unlike Facebook. As the range of social networks available to users has increased, so Facebook has less of a dominance or monopoly over social networks than it once had in Iran, falling from around 60% usage in 2015, as a high point, in favour of chat channels such as Telegram.

Facebook accounts: their characteristics, publicity and permanence

73. Facebook accounts are free to use, funded by targeted advertising and the monetary value of personal data that its users choose to share on, and with, Facebook. It numbers billions of the world's population amongst its users (see §49 above). People over specified ages, depending on the country in which a user is based, can register on the site and create a personal profile of themselves. The required age for users in the UK is currently 13.

74. Creation of a Facebook account requires a prospective user to visit a Facebook registration and account set-up page and provide their details, which include: their name; email address or telephone

number; a password; birthday and gender. While users are required to add these details, the veracity or accuracy of someone's identity are not routinely checked and other than the need for an accurate email address, false or inaccurate details may be provided either to disguise someone's identity, or for example, to avoid restrictions around people's ages.

75. Once a Facebook account has been created, a user may search Facebook or already have the details of someone they know is a user of Facebook and then invite them to become a "friend"; or similarly may receive "friend" requests. By means of that network of "friends", who may or may not know each other well, or not at all, people may share photographs; provide details of their activities; their locations; add "posts" on their own or others' "pages"; "like" posts of another user; or name and "tag" a friend in a photograph, provided that friend is content to be tagged.

76. As well as being able to accept and make friend requests, there are also Facebook "groups," which may either be public or private in nature and which allow users to share a common interest. Clubs, societies and political groups may all have "groups" on Facebook. The UK's parliament has its own public Facebook account. In summary, much material is available on Facebook to anyone with a Facebook account, regardless of whether they are "friends" with someone or not.

77. We turn to the question of publicity, in two senses: first, the extent to which material published on Facebook can be monitored; and second, how a person might generate interest on Facebook, i.e., how much publicity they might receive.

78. There are several barriers to monitoring, as opposed to ad hoc searches of someone's Facebook material. First, there is no evidence before us that the Facebook website itself has been "hacked," whether by the Iranian or any other government. Indeed, the apparent continued use of "phishes" tends to confirm the lack of access to data except through individual users' accounts.

79. Second, the effectiveness of website crawler software is limited, when interacting with Facebook. Someone's name and some details may crop up on a Google search, if they still have a live Facebook account, or one that has only very recently been closed; and provided that their Facebook settings or those of their friends or groups with whom they have interactions, have public settings.

80. The ability to extract further information, if the account remains open, will depend on the routes outlined by Dr Clayton. If someone has public Facebook settings, it requires going through their various posts. If they have private settings, another option is to identify friends with whom the target's material is shared and who have public settings. Alternatively, there is the route of having a "friend request" accepted by the target.

81. Finally, and most fruitfully, there is the option of trying to obtain the target's Facebook password, either from them (because they are required to disclose it under compulsion); or through clandestine means such as a phishing attack. It is only by obtaining someone's password that a "DYI" process can be completed with moments, which contains the broad range of someone's Facebook data. Even then, multiple DYI accesses may trigger the intervention of Facebook.

82. Without the person's password, those seeking to monitor Facebook accounts cannot "scrape" them in the same unautomated way as other websites allow automated data extraction. A person's email account or computer may be compromised, but it does not necessarily follow that their Facebook password account has been accessed. Again, were it the case that Facebook allowed automated data extraction by parties such as the Iranian government, the resources dedicated by the

Iranian government to the sophisticated spear-phishing attacks would be unnecessary, if the target has a Facebook account.

83. In relation to the second aspect of publicity, namely how a person might generate interest in their Facebook material, this is reflected by the number of meaningful interactions they have with people on Facebook and their interactions in the real world. At one extreme, a person who posts regularly on Facebook, but with few "friends" or followers on Facebook; or even if they have garnered many "friends", but with few "likes" in relation to their comments, and few other interactions, may have attracted little or no publicity at all. At the other extreme, a person with many friends or followers on Facebook, who has attracted many comments and much discussion, and whose activities reflect their prominence and activities in the real world, may attract great publicity. A person's publicity may also be relevant to whether there is a real risk of them being monitored by a state. This leads on to the question of the permanence of Facebook comments.

84. The evidence about Facebook account closure is unequivocal. It may be reversed before 30 days, but not after that time, and after deletion, the data on the person's Facebook account is irretrievable, even if their password is later discovered. The only exceptions to this are two limited pieces of residual data – limited caches of data, for a temporary period, on internet search engines; and photographs (but not links) on other people's Facebook accounts and messages sent to other people. Facebook account closure causes the data to be wholly inaccessible through or from Facebook or the user. However, if the data has been exported by a third party, that third party will continue to have access to the exported data, as stored.

Iranian state surveillance generally, and of Facebook in particular

85. Mr Jaffey refers to both the motivation of the Iranian state and their track record in surveillance of computer communications. Dr Clayton and Guarnieri and Anderson deal in detail with attempts to compromise people's email accounts. These were initially unsophisticated, but in the period from 2013 to 2016 in which Guarnieri and Anderson monitored specific attacks, and since, they have become increasingly sophisticated in the complexity of the methods, particularly in targeted "spear-phishing." We also have evidence on how the transfer of data can be monitored (deep-packet inspection); or interrupted ("man-in-the middle" or MITM attacks). The Iranian hackers discussed in the evidence have demonstrated increasing proficiency in their methods, honed over many years. We also accept that the Iranian state targets dissident groups, including religious and ethnic minorities, such as those of Kurdish ethnic origin. We note the substantial resources dedicated by the Iranian state generally in relation to cyber-security and surveillance, ranging from the NIN to the establishment of FATA.

86. Noting all that evidence, as Mr Marchant acknowledges, there is a disparity between, on the one hand, the Iranian state's claims as to what it has been, or is, able to do to control or access the electronic data of its citizens who are in Iran or outside it; and on the other, its actual capabilities and extent of its actions. This is consistent with the dual strategy of generally intimidating people where the Iranian state lacks the means to target them on a focussed basis. While we have been provided extensive evidence of how other computer systems may be compromised, such as a forked version of Telegram; the numerous phishing attacks; and Gmail accounts being compromised, there is a stark gap in the evidence, beyond assertions by the Iranian government, that Facebook accounts have been hacked and are being monitored.

87. While we accept Mr Jaffey's submission that the Iranian government may have the motivation and past record in other endeavours, the evidence fails to show it is reasonably likely that the Iranian

authorities are able to monitor, on a large scale, Facebook accounts, in the sense described by Dr Clayton, of the automated extraction of data. More focussed, ad hoc searches will necessarily be more labour-intensive and are therefore confined to individuals who are of significant adverse interest. We accept Mr Thomann's submission that the risk that an individual is targeted will be a nuanced one. Whose Facebook accounts will be targeted, before they are deleted, will depend on a person's existing profile and where they fit onto a "social graph;" and the extent to which they or their social network may have their Facebook material accessed.

88. Mr Jaffey argues that the existence of FATA's 42,000 volunteers resolves the problem of resources needed for individual targeting, and that surveillance by peers, as fake "friends," rather than through IT-driven bulk data extraction, presents the same risk of mass surveillance. We return to the point made by Mr Thomann of the lack of evidence of some of the bolder claims, including this one, made by the Iranian regime. Mr Marchant accepted that he does not know of the recruitment process for volunteers and that there was no way of verifying the claims. There is no evidence before us of the scale of any attempts at, or success of, peer surveillance. Instead, to pick one example, the February 2021 CPIN refers to a "number of Iranian Instagram influencers" deleting pictures of themselves without their hijabs. The further examples given relate to high-profile social media influencers, many based in Iran. They did not relate to Facebook and are focussed on a small number of high-profile individuals.

89. We conclude that the evidence does not show that, as a general matter, it is reasonably likely that the Iranian state, or its proxies, are able to conduct, through bulk data extraction or peer surveillance, mass surveillance of the Iranian diaspora's Facebook accounts.

What Facebook material is visible to the Iranian authorities on application for an ETD or at arrival at an Iranian port?

90. For reasons already discussed, the visibility of Facebook material will, in part, depend on whether an account has been closed more than 30 days prior to any search by the Iranian authorities. Unless any cache of that information remains, a simple Google search or search using other crawler software will not disclose someone's Facebook account details. Where the account remains open, provided that the target's privacy setting is set to public, a simple Google search will yield their name as having an account, along with accounts of those with the same or similar given names.

91. We accept (and it was not disputed) that a returnee from the UK who requires a laissez-passer or ETD needs to complete an application form and submit it to the Iranian embassy in London. They are required to provide their address and telephone number, but not an email address or details of a social media account. While social media details are not asked for, we nevertheless accept that the point of applying for an ETD is likely to be the first potential "pinch point", referred to in AB and Others (internet activity – state of evidence) Iran [2015] UKUT 00257 (IAC). We accept Dr Clayton's observation that it is not realistic to assume that internet searches will not be carried out until a person's arrival in Iran. Those applicants for ETDs provide an obvious pool of people, in respect of whom basic searches (such as open internet searches) are likely to be carried out. It also seems to us common sense that the Iranian authorities will carry out any searches at this stage, as they will be aware that in the period between applying for an ETD and arrival in Iran, accounts may be changed or deleted. The timeliness of a search therefore has a particular value.

92. The likelihood of Facebook material being available to the Iranian authorities is, in our view, affected by whether the person is or has been at any material time a person of significant interest, because if so, they are, in general, reasonably likely to have been the subject of targeted Facebook

surveillance. We refer to the level of political involvement of an individual, as in BA and HB ; and the nature of “real-world” sur place activity, which would prompt such surveillance. By way of summary, relevant factors include: the theme of any demonstrations attended, for example, Kurdish political activism; the person’s role in demonstrations and political profile; the extent of their participation (including regularity of attendance); the publicity which a demonstration attracts; the likelihood of surveillance of particular demonstrations; and whether the person is a committed opponent. In the case of such a person, this would mean that any additional risks that have arisen by creating a Facebook account containing critical material of, or otherwise inimical to, the Iranian authorities would not be mitigated by the closure of that account, as there is a real risk that the person would already have been the subject of targeted on-line surveillance, which is likely to have made the material known.

93. We accept Mr Thomann’s submission that any assessment of risk caused by social media activity needs to be on a nuanced and fact-sensitive basis, analogous to the nuanced assessment of risk factors in relation to physical sur place activity. We regard the first headnote of the Country Guidance case of BA as remaining accurate, namely:

“1. Given the large numbers of those who demonstrated here and the publicity which demonstrators receive, for example on Facebook, combined with the inability of the Iranian Government to monitor all returnees who have been involved in demonstrations here, regard must be had to the level of involvement of the individual here as well as any political activity before the individual might have been involved in Iran before seeking asylum in Britain.”

94. We also refer to the second headnote:

“2(a). Iranians returning to Iran are screened on arrival. A returnee who meets the profile of an activist may be detained while searches of documentation are made. Students, particularly those who have known political profiles are likely to be questioned as well as those who have exited illegally.”

95. We also conclude that headnotes (3) and (4) of BA remain accurate, namely that the following factors remain relevant when assessing risk on return having regard to sur place activities: the level of political involvement and the nature of any sur place activity, including the theme of demonstrations; the role of an individual in demonstrations and their political profile; the extent of participation; and the publicity attracted. All remain relevant and social media activity cannot be considered in isolation. All will be relevant to where a person fits into a “social graph,” which in turn impacts on the level of surveillance to which they may be subject.

96. We make the observation that in terms of evidence produced by those seeking protection, to the respondent or a Tribunal, social media evidence is often limited to production of printed photographs, without full disclosure in electronic format. In view of what we have found, as a general matter, production of a small part of a Facebook or social media account, for example, photocopied photographs, may be of very limited evidential value in a protection claim, when such a wealth of wider information, including a person’s locations of access to Facebook and full timeline of social media activities, readily available on the “Download Your Information” function of Facebook in a matter of moments, has not been disclosed. It is easy for an apparent printout or electronic excerpt of an internet page to be manipulated by changing the page source data. Where a decision maker does not have access to an actual account, purported printouts from such an account may also have very limited evidential value.

Will the fact of having no Facebook account on arrival in Iran cause the Iranian authorities to have suspicion or prompt further investigation?

97. Contrary to Dr Clayton's view (which he accepted was not given as an expert on Iranian matters, but his experience of UK/US use) we conclude that where an Iranian national of any age returns to Iran, the fact of them not having a Facebook account; or having deleted an account, will not as such raise suspicions or concerns on the part of Iranian authorities. We reach this conclusion for the following reasons:

(i) There are competitors to Facebook, for example Instagram and Telegram, to name but two. The use of media is rapidly changing, and the Iranian public is highly IT-literate generally, with the respondent's CPIN of February 2021 referring to a conservative estimate of 36 million, or 42.6% of the population in Iran, being social media users, (page [138] CB) with higher estimates in other reports, such as the Open Doors International Report below.

(ii) Mr Marchant accepts that any social media profile needs to be considered in the round and not simply by reference to one isolated social media account.

(iii) Even noting Mr Marchant's evidence that Facebook remains an important avenue for the diaspora community, and noting Dr Clayton's assertion, which was not based on any experience of the Iranian diaspora, we note the apparent decline in Facebook usage in Iran, from 60% in 2015; to 47.6% in December 2019, referred to in the Open Doors International Report of 2021 (page [193] CB).

(iv) Given the sophistication of the Iranian authorities' operation, their assessment will be nuanced, considering all an individual's circumstances, including not only alternative social media providers, but also, for example, whether a person is illiterate or from a rural community, where social media activity is reported as less common, such as in the appellant's case. Put another way, the absence of a Facebook account would be entirely unsurprising, if a person was illiterate, as the appellant was before he came to the UK.

To what extent can a person be expected not to volunteer the fact of having previously had a Facebook account, on return to his country of origin?

98. Our answer is in two parts. The first is whether the law prevents a decision maker from asking if a person will volunteer to the Iranian authorities the fact of a previous lie to the UK authorities, such as a protection claim made on fabricated grounds, or a deleted Facebook account. We conclude that the law does not prevent such a question, in this case. Whilst we consider Mr Jaffey's suggestion that Lord Kerr had specifically counselled against asking the question at §72 of RT (Zimbabwe), that was in a very different context, namely where political loyalty, as opposed to neutrality, was required by the Zimbabwean regime. In that case, the relevant facts included the risk of persecution because of the activities of ill-disciplined militia at road blocks. The means used by those manning road blocks to test whether someone was loyal to the ruling Zanu-PF party included requiring them to produce a Zanu-PF card or to sing the latest Zanu-PF campaign song. An inability to do these things would be taken as evidence of disloyalty, where even political neutrality (as opposed to opposition) would result in a real risk of serious harm (§16). In that context, Lord Kerr regarded an analysis of whether a person could avoid persecution by fabricating loyalty as unattractive. He raised practical concerns in evaluating whether lying to a group of ill-disciplined and unpredictable militia would be successful (§72) but made clear that his comments were by way of "incidental preamble," as the critical question was whether the appellant in that case had the right to political neutrality (§(73).

99. The key differences in our case are that the Iranian authorities do not persecute people because of their political neutrality, or perceived neutrality; and a returnee to Iran will not face an unpredictable militia, but a highly organised state. In our case, a decision maker is not falling into the trap of applying a test of what a claimant "ought to do," in cases of imputed political opinion. That was counselled against by Beatson LJ in SSHD v MSM (Somalia) and UNHCR [2016] EWCA Civ 715.

100. Instead, in deciding the issue of risk on return involving a Facebook account, a decision maker may legitimately consider whether a person will close a Facebook account and not volunteer the fact of a previously closed Facebook account, prior to the application for an ETD: HJ (Iran) v SSHD [2011] AC 596. Decision makers are allowed to consider first, what a person will do to mitigate a risk of persecution, and second, the reason for their actions. If the person will refrain from engaging in a particular activity, that may nullify their claim that they would be at risk, unless the reason for their restraint is suppression of a characteristic that they have a right not to be required to suppress, because if the suppression was at the instance of another it might amount to persecution. It is difficult to see circumstances in which the deletion of a Facebook account could equate to persecution in this sense, because there is no fundamental right protected by the Refugee Convention to have access to a particular social media platform, as opposed to the right to political neutrality.

101. The second part of our answer relates to Lord Kerr's concern about whether an analysis of what a person will do is too speculative or artificial an exercise. We accept Mr Jaffey's submission that there may be cases where the exercise is too speculative, particularly in the context of a volatile militia. That is not the case here.

102. We consider that it may be perfectly permissible for a decision maker to ask what a returnee to Iran will do, in relation to a contrived Facebook account or fabricated protection claim. Whether such an inquiry is too speculative needs to be considered on a case-by-case basis, but factors which may point to that question not being impermissibly speculative include: where a person has a past history of destroying material, such as identification documents, or deception or dishonesty in relation to dealings with state officials; whether the government has well-established methods of questioning (in the Iranian state's case, these are well-documented and therefore predictable); and whether the risks around discovery of social media material, prior to account deletion, are minimal, because a personal's social graph or social media activities are limited.

What difference does a critical Facebook account (whether deleted or not) make to the risk faced by someone returning to Iran?

103. Closure of a Facebook account 30 days before an ETD is applied for will, in our view, make a material difference to the risk faced by someone returning to Iran, who has a "critical" Facebook account. The timely closure of an account neutralises the risk consequential on having had a "critical" Facebook account, provided that someone's Facebook account was not specifically monitored prior to closure. In contrast, where a critical account has not been closed, the application for an ETD is likely to prompt a basic Google search of a name; and may prompt more targeted surveillance of that Facebook material. Discovery of material critical of the Iranian regime on Facebook, even if contrived, may make a material difference to the risk faced by someone returning to Iran. The extent of the risk they may face will continue to be fact sensitive. For example, an Iranian person of Kurdish ethnic origin may face a higher risk than the wider population.

Does the appellant have a well-founded fear of persecution?

104. The appellant gave oral evidence in Kurdish Sorani, via an interpreter. He is unable to read or write any Kurdish Sorani. His ability to read English is limited. He endeavours to understand certain passages of written English where they are of particular interest to him but requires a friend to help where he is unable to read something in full. On his own account, his English is self-taught via “You Tube” material or supplemented with limited help from his friend.

105. In terms of his Facebook account, he produced printed “pages” from it in his supplementary bundle. We do not doubt its existence, not least because Dr Clayton has accessed it, with the appellant’s consent, to check its setting, and his solicitors (who are under professional obligations relating to disclosure) have assisted.

106. We find that the appellant has been substantially assisted in the setting up and running of his Facebook account by the unnamed friend. He was unable to explain how or why his account settings had been set so that facial recognition of his photograph is switched on (which requires a positive step). His account settings have been set with the privacy settings as fully public; and automatic translation from Kurdish Sorani to English has been switched “off”, despite the appellant being unable to read Kurdish, and claiming affiliation to a Kurdish political party, whose Kurdish material he might be expected to have a particular interest in.

107. We are conscious that we do not have the full picture of the appellant’s Facebook account, (on the appellant’s own narrative, he has other social posts unconnected with his political activities) and we do not have his “DYI” material. However, we have a sense of how the account has been set up, as Dr Clayton has examined it personally and explained it to us.

108. Having reviewed the Facebook material that was in addition to what was before the FtT Judge, the new photographs are broadly in the same vein as those available to the FtT Judge. They include photographs reposted by the appellant of demonstrations or events he has not attended, but which he claims to support; and events which he claims to have attended. Beyond the photographs, the appellant adds limited commentary or written messages, and any Kurdish Sorani posts have been written by the appellant’s friend.

109. However, in contrast to the material before the FtT Judge, the new Facebook material also shows his attendance at identified locations, with banners or holding the PJAK flag, and include photographs of him in close proximity to a prominent member of the PJAK. He has also attended, for example, a demonstration celebrating the death of the Quds Force Commander, Qasem Soleimani in January 2020.

110. We consider the credibility of the appellant’s claimed genuine motivation in engaging in sur place activities in the UK since February 2018. The appellant has, since then, built up a Facebook profile of 2,983 “friends.” He accepted any friend requests made to him and sent friend requests where he likes people’s Facebook posts or activities. He does not know how many of these friends are Kurdish, despite claiming to have met most of them at demonstrations. His alternative evidence is that he has only met 10 or 20 of them. We accept that he has attended demonstrations outside the Iranian Embassy in London, including during “lockdown”, one of which was filmed by BBC Persia (but the appellant was not filmed personally) and has done so carrying the PJAK flag and other banners in a highly visible way. He has reposted on his open Facebook account material that would be regarded as highly inflammatory by the Iranian authorities, which it is unnecessary for us to repeat.

111. While we accept the fact of his activities in the UK, as outlined above, we find no reason to disturb the findings of the previous FtT Judge that the appellant's motive in engaging in these activities is entirely contrived, for several reasons.

112. First, we do not find it credible that he has built up such a number of friends because of a genuine support for the PJAK, noting the inconsistency of how many of the "friends" he has met or knows anything about. He suggested that he acquired these friends based on them sharing his views and having met most of them, but then suggested that he knew only 10 to 20 of them.

113. Second, the appellant's explanation that the translation facility on his Facebook account from Kurdish Sorani to English has been switched off and instead, he asks a friend to translate and if necessary to write on his behalf, is not consistent with a genuine interest in the aims of the organisation which he professes to support.

114. Third, despite travelling hundreds of miles to attend demonstrations in London (including during lockdown) he describes no other specific activities, whether by way of organisational support, other than attending the demonstrations at which he might be photographed.

115. We find that his posing with the PJAK flag and banners at specific demonstrations and his photographs of the PJAK leader in a highly visible way are designed to draw attention to himself via visual imagery, for the purposes of creating the impression of political loyalty to the PJAK, when in reality, he has no genuine interest in, or loyalty to, the PJAK. Whether his sur place activities have nevertheless resulted in a well-founded fear of persecution based on imputed loyalty is a separate question, with which we deal below.

116. Mr Jaffey invited us to consider that he would be at risk, even taking three points against him as follows:

(i) that his sur place activities have been entirely contrived in the sense that the activities had taken place, but they were not because of any genuine belief in the political ideology of the PJAK and were instead solely to bolster a fabricated protection claim;

(ii) that the appellant would delete his Facebook account prior to his application for an ETD;

(iii) that if returned to Iran, if questioned, the appellant would not volunteer his previous Facebook history, although Mr Thomann accepts that if presented with Facebook material obtained prior to deletion, he will not deny the existence of that material.

117. These three assumptions answer two questions, namely: (1) whether to depart from the preserved findings on the sur place activities being contrived (or not, based on our findings); and (2) whether he would delete and not volunteer the fact of the contrived sur place activities.

118. We turn to the final question of whether the appellant nevertheless has a well-founded fear of persecution. Given his attendance at events; and the prominence of the person he has secured a photograph with, we conclude that there is a real risk that he has been the subject of targeted (as opposed to general) surveillance by the Iranian state already. There is no need for the Iranian authorities to have "hacked" his account or "scraped" his "DYI". His carefully curated (albeit contrived) social graph is, in this particular case, just sufficient in our judgment to establish a risk that he has been subject to surveillance in the past that would have resulted in the downloading and storing of material held against his name. Put another way, he has drawn enough attention to himself by the extent of his "real world" activities, to have become the subject of targeted social media

surveillance. Deletion of his Facebook material and closure of his account before he applied for an ETD would serve no purpose, as his profile is such that there is a real risk that he had already been targeted before the ETD "pinch point." On return to Iran, there is a real risk that he would be presented with that material, of a highly provocative and incendiary nature. The nature of the material, although contrived and even if seen as contrived, combined with his Kurdish ethnic origin, would result in a real risk of adverse treatment, sufficiently serious to constitute persecution. He is analogous to the appellant in the well-known authority of Danian v SSHD [1999] INLR 533.

119. In the circumstances, it is unnecessary for us to answer the question of whether the appellant would or would not delete his Facebook account prior to an application for an ETD. He is already at risk. While the appellant has contrived a sur place claim, he has done so in such an extreme way that his is one of those cases where that the nature of his bogus activities puts him at real risk of persecution, for reasons imputed to him. The context is not because of some complex IT surveillance, "scraping", or computer algorithms; rather, his activities are sufficiently high profile to have raised his social graph. Even a brief, targeted search of Facebook, prompted by his profile because of "real world" sur place activities, is sufficient to reveal his on-line activities.

Country Guidance

120. The cases of BA (Demonstrators in Britain – risk on return) Iran CG [2011] UKUT 36 (IAC); SSH and HR (illegal exit: failed asylum seeker) Iran CG [2016] UKUT 00308 (IAC); and HB (Kurds) Iran CG [2018] UKUT 00430 continue accurately to reflect the situation for returnees to Iran. That guidance is hereby supplemented on the issue of risk on return arising from a person's social media use (in particular, Facebook) and surveillance of that person by the authorities in Iran.

Surveillance

121. There is a disparity between, on the one hand, the Iranian state's claims as to what it has been, or is, able to do to control or access the electronic data of its citizens who are in Iran or outside it; and on the other, its actual capabilities and extent of its actions. There is a stark gap in the evidence, beyond assertions by the Iranian government that Facebook accounts have been hacked and are being monitored. The evidence fails to show it is reasonably likely that the Iranian authorities are able to monitor, on a large scale, Facebook accounts. More focussed, ad hoc searches will necessarily be more labour-intensive and are therefore confined to individuals who are of significant adverse interest. The risk that an individual is targeted will be a nuanced one. Whose Facebook accounts will be targeted, before they are deleted, will depend on a person's existing profile and where they fit onto a "social graph;" and the extent to which they or their social network may have their Facebook material accessed.

122. The likelihood of Facebook material being available to the Iranian authorities is affected by whether the person is or has been at any material time a person of significant interest, because if so, they are, in general, reasonably likely to have been the subject of targeted Facebook surveillance. In the case of such a person, this would mean that any additional risks that have arisen by creating a Facebook account containing material critical of, or otherwise inimical to, the Iranian authorities would not be mitigated by the closure of that account, as there is a real risk that the person would already have been the subject of targeted on-line surveillance, which is likely to have made the material known.

123. Where an Iranian national of any age returns to Iran, the fact of them not having a Facebook account, or having deleted an account, will not as such raise suspicions or concerns on the part of Iranian authorities.

124. A returnee from the UK to Iran who requires a laissez-passer or an emergency travel document (ETD) needs to complete an application form and submit it to the Iranian embassy in London. They are required to provide their address and telephone number, but not an email address or details of a social media account. While social media details are not asked for, the point of applying for an ETD is likely to be the first potential "pinch point, " referred to in AB and Others (internet activity – state of evidence) Iran [2015] UKUT 00257 (IAC). It is not realistic to assume that internet searches will not be carried out until a person's arrival in Iran. Those applicants for ETDs provide an obvious pool of people, in respect of whom basic searches (such as open internet searches) are likely to be carried out.

Guidance on Facebook more generally

125. There are several barriers to monitoring, as opposed to ad hoc searches of someone's Facebook material. There is no evidence before us that the Facebook website itself has been "hacked," whether by the Iranian or any other government. The effectiveness of website "crawler" software, such as Google, is limited, when interacting with Facebook. Someone's name and some details may crop up on a Google search, if they still have a live Facebook account, or one that has only very recently been closed; and provided that their Facebook settings or those of their friends or groups with whom they have interactions, have public settings. Without the person's password, those seeking to monitor Facebook accounts cannot "scrape" them in the same unautomated way as other websites allow automated data extraction. A person's email account or computer may be compromised, but it does not necessarily follow that their Facebook password account has been accessed.

126. The timely closure of an account neutralises the risk consequential on having had a "critical" Facebook account, provided that someone's Facebook account was not specifically monitored prior to closure.

Guidance on social media evidence generally

127. Social media evidence is often limited to production of printed photographs, without full disclosure in electronic format. Production of a small part of a Facebook or social media account, for example, photocopied photographs, may be of very limited evidential value in a protection claim, when such a wealth of wider information, including a person's locations of access to Facebook and full timeline of social media activities, readily available on the "Download Your Information" function of Facebook in a matter of moments, has not been disclosed.

128. It is easy for an apparent printout or electronic excerpt of an internet page to be manipulated by changing the page source data. For the same reason, where a decision maker does not have access to an actual account, purported printouts from such an account may also have very limited evidential value.

129. In deciding the issue of risk on return involving a Facebook account, a decision maker may legitimately consider whether a person will close a Facebook account and not volunteer the fact of a previously closed Facebook account, prior to application for an ETD: HJ (Iran) v SSHD [2011] AC 596. Decision makers are allowed to consider first, what a person will do to mitigate a risk of persecution, and second, the reason for their actions. It is difficult to see circumstances in which the deletion of a

Facebook account could equate to persecution, as there is no fundamental right protected by the Refugee Convention to have access to a particular social media platform, as opposed to the right to political neutrality. Whether such an inquiry is too speculative needs to be considered on a case-by-case basis.

Notice of decision in respect of XX's case

For the reasons set out above, the appeal is allowed on asylum grounds.

Signed J Keith Date 20 th January 2022

Upper Tribunal Judge Keith

TO THE RESPONDENT

FEE AWARD

While we have allowed the appeal, because no fee has been paid or is payable, we have decided to make no fee award.

Signed J Keith Date 20 th January 2022

Upper Tribunal Judge Keith

ANNEX: ERROR OF LAW DECISION

Upper Tribunal

(Immigration and Asylum Chamber) Appeal Number:

THE IMMIGRATION ACTS

Heard at North Shields (Kings Court)	**Decision & Reasons Promulgated**
On 19 July 2019	

Before

UPPER TRIBUNAL JUDGE DAWSON

Between

XX

(ANONYMITY DIRECTION MADE)

Appellant

and

THE SECRETARY OF STATE FOR THE HOME DEPARTMENT

Respondent

Representation :

For the Appellant: Ms M Cleghorn, Counsel instructed by Halliday Reeves Law Firm

For the Respondent: Mr P Stainthorpe, Senior Presenting Officer

DECISION AND REASONS

Direction Regarding Anonymity – Rule 14 of the Tribunal Procedure (Upper Tribunal) Rules 2008

Unless and until a Tribunal or court directs otherwise, the appellant is granted anonymity. No report of these proceedings shall directly or indirectly identify him or any member of his family. This direction applies both to the appellant and to the respondent. Failure to comply with this direction could lead to contempt of court proceedings.

1. The appellant, who is a national of Iran, and of Kurdish ethnicity from a village in the District of Mariwan, appeals with permission a decision of First-tier Tribunal Judge Myers. For reasons given in her decision dated 8 April 2019, the judge dismissed the appellant's appeal against the Secretary of State's decision dated 14 February 2019 refusing his asylum and humanitarian protection claim. The appellant had left Iran in October 2017 and made his way through Europe via Greece, Italy and France to the United Kingdom where he arrived clandestinely on 4 December 2017. He claimed asylum the same day. The judge set out the appellant's case at paragraphs [9] to [17] of her decision as follows: -

"9. He is an Iranian Kurd from Drgasykhan village in the district of Mariwan. He lived with his parents and sister. He did not go to school and cannot read or write. He worked as a farmer and also as a smuggler of goods over the Iran Iraq border. He was aware of discrimination against Kurds but did not realise there was anything he could do about it.

10. In 2015 his friend and neighbour, Ayub volunteered for military service. On his return in 2017 he started to tell the Appellant more about the oppression of the Kurds and the activities of PJAK.

11. Over time, Ayub told the Appellant that he was a member of PJAK, and on Ayub's encouragement the Appellant also became involved on about six occasions by helping PJAK to distribute leaflets and materials.

12. On 23/10/2017 the Appellant met Ayub to deliver leaflets. After doing so he went to the Iraq border to collect some goods to take to a delivery point. In the early hours of the morning his mother telephoned him from a neighbour's house to say that Etela'aat had raided their home and were looking for him, she also told him that Ayub's house had been raided and that he had been arrested.

13. The Appellant did not go home but instead phoned his uncle who advised him to go to a house owned by a relative of Ayub where the next day his uncle met him and arranged for him to leave Iran with the help of an agent.

14. He travelled to the UK via Greece, Italy and France. He was arrested and fingerprinted in France but did not claim asylum because the agent told him that it was not safe to do so because Iranians were deported from France. On the instructions of the agent he said that he was Iraqi and gave a false name and date of birth.

15. Since living in the UK the Appellant has continued his involvement with PJAK activities by attending meetings and demonstrations and also posting messages on his public Facebook account. He believes that he has been photographed from inside the Iranian embassy when he attended demonstrations.

16. He has asked to join PJAK in the UK but has been told that he must first act as a supporter for two years in the UK before he will be accepted as a member.

17. He is at risk on return to Iran because he would be identified as a supporter of PJAK. He believes that his family have been under surveillance by Etela'aat."

2. The judge summarised the Secretary of State's position at paragraph [18] as follows:

"18. The basis upon which the Respondent has rejected the Appellant's claim on asylum, human rights grounds, and humanitarian protection is set out in detail in the reasons for refusal letter. In essence, the Respondent casts doubt on the overall credibility of the Appellant's claim and does not accept that he has a well-founded fear of persecution for a Convention reason. In doubting the Appellant's credibility, the Respondent relies on inconsistencies and implausible statements in his account."

3. The judge found the appellant had fabricated his account and considered his involvement and activities in the United Kingdom to be "merely opportunistic" but nevertheless considered whether his sur place activities would put him at risk on return. The judge's conclusions on this latter aspect was set out at paragraphs [31] and [32] as follows:

"31. In conclusion, I find that the Appellant has fabricated his account and that his involvement in activities in the UK are merely opportunistic. Despite this, I must now consider whether his activities even if manufactured could put him at risk on return. In **BA (Demonstrators in Britain – risk on return) Iran CG [2011] UKUT 36 (IAC)** the Tribunal held that (i) Given the large numbers of those who demonstrate here and the publicity which demonstrations receive, for example on Facebook, combined with the inability of the Iranian Government to monitor all returnees who have been involved in demonstrations here, regard must be had to the level of involvement of the individual here as well as any political activity which the individual might have been involved in Iran before seeking asylum in Britain; (ii) (a) Iranians returning to Iran are screened on arrival. A returnee who meets the profile of an activist may be detained while searches of documentation are made. Students, particularly those who have known political profiles are likely to be questioned as well as those who have exited illegally. (b) There is not a real risk of persecution for those who have exited Iran illegally or are merely returning from Britain. In my judgment the Appellant would not be at risk because he would not be known as a committed opponent or someone with a significant political profile. He was not leading or organising demonstrations and although there are photographs showing him carrying banners and on once [sic] occasion was photographed with a noose round his neck, I do not find that these photographs place him at risk because it is unclear where they were taken and there is no evidence that the demonstrations attracted media coverage in the United Kingdom or in Iran.

32. In any event, having found that he lacks credibility in my judgment the Appellant would not place himself at risk of having his Facebook post and photographs still available to the Iranian authorities on his return. The Upper Tribunal heard expert evidence in the case of LKIK which confirmed that "information, media and all settings/data relating to the deleted Facebook account, including user IDs and names are not accessible once they have been deleted; in other words any such entries by that particular user account will no longer be visible online and within a matter of days will be permanently removed from the service. The original Facebook posts and any copy shared by other

users cannot be viewed after being deleted. Upon deletion of a Facebook account all comments likes and shared content is removed. This content is no longer visible to users of the Facebook service or members of the public. The fact that a Facebook user my set their privacy settings to the public. The fact that a Facebook user may set their privacy settings to public does not mean that the content will be automatically disclosed to other Facebook users. The setting means that anybody conducting a search against the Appellant's name to an article with this privacy will be able to see the article whilst it remains in existence, no more."

4. As to the appellant's ethnicity and any consequent risk, the judge concluded at paragraph [36] after directing herself in accordance with HB (Kurds) Iran CG [2018] UKUT 00430 as follows:

"36. The Appellant's Kurdish ethnicity is likely to result in questioning on return, but I do not accept that he will be regarded as having been involved in any low-level political activity and neither do I find that any of the other factors identified in **HB** apply to him. Having found him to lack credibility in my judgment if he was returned to Iran, he would ensure that he had no materials in his possession which would put him at risk, and I do not accept that there would be any likelihood that the photographs submitted at the hearing would be available to the Iranian authorities. Consequently, I do not find him at risk on return."

5. The grounds of challenge are threefold. The first asserts a failure by the judge to take into account HK v SSHD [2006] EWCA Civ 1037. It is argued that the findings made were based on speculation as to the way in which the appellant would have behaved and the judge had failed to take into account the warnings of Lord Neuberger in the cited authority.

6. As to ground two, it is argued in paragraph [11] of the grounds:

"11. In light of the country guidance setting out the high level of attention shown by the authorities to protests and to social media, the evidence before the judge was sufficient to show that these protests had come to the authorities' attention. It is not plausible that a protest in front of the embassy was not something the authorities were fully aware of and were monitoring. It is submitted that it was reasonably likely that the Appellant's participation had come or would come to the authorities' attention. The case of BA indicates that the prominence of the individual's role in a demonstration is relevant to risk on return (headnote para. 4)."

7. Finally, in relation to ground three it is argued at paragraphs [13] and [14] of the notice of appeal:

"13. Following the error set out in Ground 2, it is averred that this fails to take into account the possibility of the Appellant and/or on-line activity associated with the Appellant having already come to the authorities' attention – see in particular the provisions of AB, paragraphs 9 and 10 above.

14. It is further submitted that taking into account the expert evidence contained in LKIK, that "all 'comments,' 'likes' and shared content is removed does not take into account the possibility that photographs on other public Facebook accounts would remain."

8. In granting permission to appeal First-tier Tribunal Judge Swaney considered it was arguable that the assessment of credibility was flawed because the judge had speculated how the appellant would have behaved (if genuine) without regard to his particular circumstances, being his limited education and poor literacy. He did not limit the grant of permission however.

9. Ms Cleghorn opened her submissions with an additional issue in relation to ground three with reference to the reported decision of the Tribunal in AB (internet activity – state of evidence) Iran

[2015] UKUT 0257. She argued that even if the appellant took down his Facebook account the authorities may already have a record of what was said before. She also sought to enlarge ground one with reference to a comment by the judge that the appellant had been vague and evasive in giving his evidence. The decision did not contain all that the appellant had said in his witness statement. Mr Stainthorpe had nothing to say on the matter. I declined the application. It has been readily open to the appellant to seek to amend or enlarge his grounds prior to the hearing.

10. In relation to ground one Ms Cleghorn argued the judge had imposed a westernised idea of what a person would do in her approach to the evidence, in particular in connection with how the appellant would have behaved drawing on the judge's own experience.

11. As to ground two, she argued that the issue was twofold. The first was whether the judge had genuinely grappled with the photographs of the appellant's protest activity in the United Kingdom. Time was spent in the course of submissions examining the photographs. The second limb of the ground was the reliance by the judge on the unreported decision in LKIK . Although Ms Cleghorn accepted that there had been compliance with the Practice Direction by the Secretary of State, the decision and accompanying note in respect of compliance with the Practice Direction had only been served on the day of the hearing. She acknowledged that there was no record of any protest by Ms Mottershaw and acknowledged that this aspect had not been raised in the grounds of challenge. She contended nevertheless that the judge had not given adequate reasons why she had relied on an unreported decision and whether she had considered all the evidence. A further issue related to people being presented with printouts when they arrive in Iran which went beyond checking people not just on arrival. As to the third ground, Ms Cleghorn argued this involved further consideration of the weight placed on an unreported case which was never meant to be country guidance. Specifically it is argued in the grounds:

" It is further submitted that taking into account the expert evidence contained in LKIK that 'all 'comments,' 'likes' and shared content is removed does not take into account the possibility that photographs on other public Facebook accounts would remain ".

12. By way of response Mr Stainthorpe submitted that, when read as a whole, the judge had provided context and reasons for her factual findings when her conclusions were read in their entirety. As to the second ground the judge had dealt adequately with the appellant's UK based activities and whether these would place him at risk. It had been accepted that LKIK had been served in accordance with the Practice Direction and in any event a large part of that decision had been considered by the Court of Appeal in AM (Iran) v SSHD [2018] EWCA Civ 2706. The appellant would not be expected to lie and would say on return that he had falsified an asylum claim. AB (Iran) had been displaced by the judge in holding that the appellant would be expected to delete his account. An argument as to whether his details would appear elsewhere was not before the judge. He considered these submissions also covered ground three.

13. I take each ground in turn. The judge's findings are set out relevant to the grounds of challenge in paragraphs [24] to [26] as follows:

"24. I have found the Appellant vague and evasive in giving his evidence and I do not accept the core of his account. His claims that he was a lifelong friend of Ayub who was like his brother. He also said that he was aware it would be very risky to undertake work for PJAK. In that context I would expect the Appellant to find out as much as possible from his close friend Ayub before agreeing to participate. However, the Appellant's lack of interest in any details simply beggars belief. He told me that he did not think to ask Ayub how long he had been working for PJAK, or whether he had delivered

the leaflets and been working for PJAK or whether he had delivered the leaflets and materials alone before the Appellant started to help. Despite being given the opportunity on numerous occasions to clarify his evidence all he would say was that “I did not ask him, it’s not an easy job… Not easy to do it on your own.” He told me that it was necessary to have one person distributing the materials and one acting as a lookout, however he had no idea how Ayub had previously done the work.

25. Furthermore, when asked why he decided to take the risk of helping PJAK, he was vague and lacking in detail, all he could say was that the party was striving for the Kurdish cause and his neighbour told him that he had to be careful and patient.

26. I do not accept that he has not asked his uncle in Iran what has happened to his family, and I find the Appellant is merely speculating when he says that his family would be in danger if he tried to contact them. In evidence he told me that he had not asked his uncle whether the authorities had been to his home to look for him, he just asked how his family was and then hung up. I find this lacks credibility, in my judgment this would be one of the first things he would ask about if he was genuinely concerned that he was wanted by the authorities because of his political activities.”

14. Thereafter the judge reached findings in relation to the appellant’s activities as a supporter of PJAK in the United Kingdom which she considered “merely opportunistic”. She also considered the appellant’s credibility undermined by the fact of his illiteracy having set up a Facebook account on which he shared messages supportive of Kurdish rights. She also considered at paragraph [29] that had Ayub been arrested and the appellant involved with PJAK activities, it would have been possible to obtain confirmation of this event from the party. The judge considered the appellant had given inconsistent evidence when seeking to explain this aspect.

15. Before turning to the conclusion cited above in paragraphs [31] and [32] the judge addressed evidence of the appellant suffering from PTSD, but here too the judge considered inconsistency between the appellant’s account as to the cause and his evidence that he had not encountered any direct threats from the Iranian Government.

16. In my judgment the findings by the judge were open to her on the evidence and I do not accept that she imposed her own idea on how someone would behave, but instead drew reasonable inferences from the evidence. Ground one is no more than a challenge to a credibility assessment properly open to the judge having heard the appellant’s evidence and having considered that evidence in the round.

17. I am not so confident that the judge did not err in relation to the issue raised in ground two with particular reference to the findings in the closing paragraph of [31]. It is in my judgment questionable whether the judge was correct to rule out risk because of the absence of clarity over where the photographs were taken in the light of the numbers evidently involved and the absence of media attention having been attracted. The sophisticated surveillance considered by the Tribunal in AB (Iran) points to a real possibility that even absent media coverage and doubts over the location of the gathering does not rule out the possibility of the Iranian authorities being aware of the event and having made a record. This feeds into ground three which considers the impact of the closing or deleting of the appellant’s Facebook account. Although it was open to the judge to have regard to the unreported decision in light of compliance with the Practice Direction, she was nevertheless required also to give reasons for doing so in the light of the reported decision in AB (Iran) in which expert evidence was given of an archiving process by the Iranian authorities. Further, the question that the judge did not ask, although acknowledging the hair trigger approach identified in HB (Kurds) Iran CG [2018] UKUT 00430 was how the authorities would react to the appellant explaining truthfully that he

had taken down his Facebook account on the basis that a tribunal in the United Kingdom had decided that in providing support for PJAK, the appellant had been merely opportunistic. The issue in the light of the guidance given in HB (Iran) is whether the authorities would accept the appellant's honest disclosure and have no further interest in him. Put another way is there a risk that, despite the disclosure, the authorities would nevertheless regard the appellant was a supporter of PJAK.

18. The Court of Appeal in AM (Iran) v SSHD [2018] EWCA Civ 2706 considered a similar situation where an appellant had been found as not credible as to his conversion to Christianity. Simon LJ recorded the approach of the Upper Tribunal Judge to the appellant's Twitter activities. The judge had concluded that the appellant could be expected to tell the Iranian authorities that his Twitter postings were simply an attempt to gain status in the United Kingdom and that he was not a genuine Christian convert because that was what the First-tier Tribunal had found. The judge had also found that this might however not be accepted by the Iranian authorities, although they knew that many Iranian asylum seekers were economic migrants. The judge had concluded that it would not be a leap too far to conclude that the Twitter postings which had been extensive would be seen. The court was also concerned with a concession by the Secretary of State which had not determined the entire appeal. Simon LJ concluded at paragraph [57] (5):

" However, the concession plainly did not 'determine the entire appeal', to adopt the phrase of Jackson LJ in A K (Sierra Leone) . The UT regarded the crucial issue which bore on the particular risk to AM on his return was not his apparent (but false and deceitful) Christian beliefs; but the expression of such beliefs in his Twitter posts. The UT Judge was entitled to his view of the facts, which I have summarised in [49] above, so far as they went. However, he relied on the decision in AB and others (2015) which was not a case dealing with Twitter posts, and did not consider the questions whether the posts could be deleted and what the effect of deleting them would be? When giving leave to appeal, the single Lord Justice considered that the possibility of deletion was 'a common-sense consideration' and that the UT's omission to consider these questions was one of the factors that satisfied the second appeal test, the other being the failure to have regard to the two CG cases FS and others (2004) and SZ and JM (2008). I accept that this point should have been raised on behalf of the Secretary of State, but in my view the matter should plainly have been investigated ".

19. I have referred to this case as it was relied on by Mr Stainthorpe, however, unlike the position in AM , the First-tier Tribunal in the appeal before me had before it a reported decision, albeit not a country guidance one which arguably covered the issue of the knowledge of the Iranian authorities rather more comprehensively than in the unreported decision of LKIK .

20. In my judgment grounds two and three are made out on the basis above. The decision is set aside solely in relation to the appellant's sur place activities and any risks that he would face as a consequence. The judge's findings as to the basis of the appellant's support for the PJAK in the United Kingdom (recorded at [27] and [28]) are preserved and, for the avoidance of doubt the judge's findings on the appellant's pre-flight activities are also preserved. Directions for a further hearing for the remaking of the decision in the Upper Tribunal will be issued in due course.

Signed Date 20 August 2019

UTJ Dawson

Upper Tribunal Judge Dawson