



**Upper Tribunal
(Immigration and Asylum Chamber)**

AB and Others (internet activity – state of evidence) Iran [2015] UKUT 0257 (IAC)

THE IMMIGRATION ACTS

Heard at Field House

On 28 January 2014, 29 January 2014, 30
January 2014 and 31 January 2014

Determination Promulgated

On 19 March 2015

Re-Promulgated on 30 April
2015

Before

**UPPER TRIBUNAL JUDGE WARR
UPPER TRIBUNAL JUDGE PERKINS**

Between

AB

CD

EF

Appellants

and

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Respondent

Representation:

For the Appellants:

AB

Mr P Haywood, Counsel instructed by Duncan Lewis Solicitors

CD

Mr T Hodson, Counsel acting for Elder Rahimi Solicitors

EF

Ms S Harrison, Solicitor from Halliday Reeves

For the Respondent:

Mr B Rawat, Counsel instructed by the Treasury Solicitors

The material put before the tribunal did not disclose a sufficient evidential basis for giving country or other guidance upon what, reliably, can be expected in terms of the reception in Iran for those returning otherwise than with a “regular” passport in relation to whom interest may be excited from the authorities into internet activity as might be revealed by an examination of blogging activity or a Facebook account. However, this determination is reported so that the evidence considered by the Upper Tribunal is available in the public domain.

DETERMINATION AND REASONS

1. The appellants in this case are citizens of Iran. In very broad terms they each claim they are refugees because of their “blogging” activity on the internet. The word “blogging” will be readily understood by a contemporary reader but for the avoidance of any possible misunderstanding we mean the practice of publishing on the internet written articles, reports, film clips, pictures, or links to the same, whether produced by the person responsible for the blog or another. They each appeal against decisions of the Secretary of State on the grounds that they are refugees or otherwise entitled to international protection.
2. Pursuant to rule 14 of the Tribunal Procedure (Upper Tribunal) Rules 2008 we make an order prohibiting the disclosure or publication of any matter likely to lead members of the public to identify any or all of the appellants. Their cases depend in part on their risking persecution because of things that they have done since leaving Iran, including criticising the government of Iran. The significance of their activities is disputed by the respondent. Publicity that identified them to the Iranian authorities might lead to the absurd result of their needing protection solely because an otherwise unfounded claim for asylum had attracted attention. Breach of this order can be punished as a contempt of court. Although the order must be followed strictly it is not intended to stifle reporting of the issues in the case and our findings on them.
3. As well as determining the three separate appeals that are before us we have endeavoured to give general guidance on a range of related issues. In an effort to make our decision easier to read we do not consider below each strand of evidence or argument in the order in which we heard it. For similar reasons we identify the appellants by their initials rather than their place in the title.
4. We confirm that we have considered all of the several volumes of evidence before us even though we do not mention each document or submission specifically. We reached no conclusion before considering the evidence as a whole. We have decided each appeal on its own merits and we have reminded ourselves that although the appellant in each case must prove his or her case the standard of proof is low. It is sufficient to show only a real risk of persecution or other serious ill treatment in the event of return to Iran to qualify for protection.
5. The appellant, AB, was born in 1989. He appeals a decision of the respondent on 25 March 2011 to remove him as an illegal entrant. He entered the United Kingdom on 3 March 2011.
6. His appeal was dismissed by the First-tier Tribunal in a decision dated 11 May 2011. He appealed to the Upper Tribunal which found that the First-tier Tribunal had erred in law and made fresh findings of fact. The Upper Tribunal dismissed the appeal on 20 August 2012 but the appeal comes before us pursuant to an order of the Court of Appeal on 27 June 2013. The Court of Appeal ordered by consent that the appeal be remitted to this Tribunal to be decided again with the other appeals determined here, on a particular basis. This was explained at paragraph 1 of the consent order dated 27 June 2013 where the Court said:

“The Appellant’s appeal be allowed by remittal of the limited grounds of appeal on which permission was granted by Sir Richard Buxton in his Court Order of 7 February 2013 (identified in sub-paragraph 2 of the “Events in the UK” paragraph, relating to the blogging in the UK) to the Upper Tribunal of the Immigration and Asylum Chamber for reconsideration pursuant to paragraph 12 of Schedule 4 to the Transfer of Functions of the Asylum and Immigration Tribunal Order 2010 (SI 2010/21) and section 14 of the Tribunal, Courts and Enforcement Act 2007”.

7. The appellant, CD, was born in 1975 and so is now 39 years old. She appeals a decision of the respondent of 25 March 2011 to refuse to vary her leave to remain in the United Kingdom. She arrived in the United Kingdom in September 2010 with permission to enter as a student and claimed asylum on 4 March 2011. Her appeal was dismissed by the First-tier Tribunal but permission to appeal was given by Upper Tribunal Judge Gleeson because she found it arguable that insufficient weight had been given to the appellant’s blogging activities, the expert evidence on which she relied about how bloggers might be identified and treated in Iran and her political activities.
8. Before us there was little argument on the point and we are satisfied that the First-tier Tribunal erred in law for the reasons identified by Judge Gleeson as arguable. The First-tier Tribunal did not engage adequately with the background and expert evidence presented to it. We therefore set aside its determination and decide the appeal again ourselves.
9. The appellant, EF, was born in 1972. He appealed a decision of the respondent on 22 November 2011 to remove him from the United Kingdom. His appeal against that decision was dismissed by the First-tier Tribunal but the Upper Tribunal, in a determination promulgated on 12 May 2013, found that the First-tier Tribunal had erred in law and set aside the decision in that case. Although the reasons have already been sent to the parties we formally incorporate the decision into this determination and set it out at Appendix 3.
10. These cases raise common questions and the parties had suggested a “list of issues” to be determined in the appeal which the Tribunal agreed to adopt. We set these out below:

List of Issues

- (1) The use of social and other internet-based media (including the posting of articles, comments or web links on a website; maintaining or contributing to a blog; uploading/streaming photographs or videos; the use of Facebook by Iranian nationals located in the United Kingdom to make actual or perceived criticisms of the Iranian state)
- (2) Whether such use is reasonably likely to come to the attention of the Iranian authorities because those authorities have the capability to detect and monitor such activity
 - (a) the capability of the Iranian authorities to monitor and/or restrict the use within Iran social and/or other internet-based media;
 - (b) the capability of the Iranian authorities to identify individuals in Iran who use (as in (1)), above, social and/or other internet-based media in a way that is critical or perceived as being critical of the Iranian authorities;

- (c) the capability of the Iranian authorities to monitor the use social and other internet-based media by Iranian nationals based outside of Iran;
- (d) the capability of the Iranian authorities to identify Iranian nationals based outside Iran who make use of social and/or other internet-based media to criticise the Iranian government and/or express views which are likely to be considered critical of the Iranian state;
- (e) the level of public interest within Iran in views posted on social or other internet-based media by Iranian nationals living in the United Kingdom and which may be considered critical of the Iranian state;
- (f) the capability of the Iranian authorities to restrict access to social/internet-based media operated by Iranians in the United Kingdom and is critical or deemed to be critical of the Iranian state.

(3) The additional factors that may be relevant to an assessment of the risk on return to an Iranian national who, while in the United Kingdom, has used social and/or other internet-based media to express views that are, or are deemed by the Iranian authorities to be critical of the Iranian state, including:

- (a) the use of social and/or other internet-based media, prior to departure from Iran, in a manner considered to be critical of the Iranian state;
- (b) the nature of any “profile” with the authorities that the returnee might have had before leaving Iran;
- (c) other “sur place” activities in the UK;
- (d) the immigration history of the returnee, including whether the returnee has left Iran illegally;
- (e) the possession of a laptop and/or other equipment that may be used across the internet.

(4) Whether and by what means the Iranian authorities would be able to link a returnee to social media and/or other internet-based activity conducted in the United Kingdom.

(5) Would the treatment received by an individual on return be affected by the nature and extent of their use of social and other internet-based media?

(6) The relevance, if any, of the opportunistic use of social and/or other internet-based media.

11. Each of the parties has provided us with a skeleton argument which we have found very helpful.
12. The appellants CD and EF each gave evidence before us. In each case their evidence is summarised in the appendices. Our findings on that evidence are obvious from the case summaries below.
13. We consider Mr Rawat’s closing submissions later but we found his skeleton argument a particularly helpful guide to the points of contention in these appeals and we summarize it now as an introduction. Unsurprisingly it outlined the respondent’s case in respect of each appellant.
14. He was careful to emphasise that adverse credibility findings had been made in the case of AB and these had not been disturbed by reason of the Court of Appeal’s decision. Both Mr Rawat and Mr Haywood (for AB) accepted that the

Court of Appeal did not regard the anonymous blog attributed to AB as being significant because it could not be traced to him.

15. Concerning AB, the respondent says that AB is a male Iranian national of Kurdish ethnicity born in 1989. He entered the United Kingdom in March 2011 and claimed asylum the same day. He said he had attended four demonstrations in favour of a Kurdish self-government and had been a member of the Kurdish Democratic Party and the authorities had raided his home and shop and taken his laptop. This had political writings that he had placed on the website and a picture of an Iranian banknote defaced with a political slogan. He left Iran and made his way to Turkey on foot. His claim for asylum was refused.
16. The respondent accepted that AB had recorded a rap album released on the internet in 2008.
17. The First-tier Tribunal did not believe part of AB's evidence. It found that AB could not be identified from the website on which he had uploaded his rap album. It found that AB had not proved that he was the author of the contents of the blogs of which he claimed ownership. Permission to appeal to the Upper Tribunal was granted on a very narrow ground but the Upper Tribunal conducted a full re-hearing and heard evidence. It did not accept that AB had told the truth about what he had done in Iran and that there was nothing about AB's activities in the United Kingdom to bring him to the attention of the Iranian authorities. His online activities were conducted under pseudonyms and the blog was only accessible with his permission. There was no original material. The Tribunal decided that his activities had been conducted to bolster an asylum claim. The Court of Appeal set aside the decision by consent because the First-tier Tribunal failed to engage with the material about the consequences of blogging.
18. In the case of AB we were directed to consider how the appellant might be at risk as a consequence of his UK-based activities and, by implication, if his activities were opportunistic. Evidence of his conduct in Iran was rejected. There is evidence before us from the KDP-I. It was not before the First-tier Tribunal and it confirms that he was an active member of the party and remains an active member in the United Kingdom.
19. The Secretary of State has accepted that AB put music on his website (its name was given in evidence) and the songs clearly have a political content.
20. Before leaving Iran he had "blogged" and had blogged since coming to the United Kingdom via a web site he used first posted in 2011. The second of the blogs bears his photograph and full name and shows him to be in the United Kingdom. He also has a Facebook account and hosts a room on Facebook known as [name redacted] which includes videos and satires of the Iranian regime. Copies of some of the appellant's songs and photographs were on YouTube. In the United Kingdom he has been involved with the KDP-I and attends meetings but does not play a prominent part. A search in Google against his name brings up music that he has posted including YouTube links, his Facebook page and his blog.
21. We were shown "Mr AB's YouTube" handouts. These appear to have been found by searching for the appellant's name. The response was headed "did you mean:

AB". Of particular interest was a song identified as a political song about the situation in Iran and about the system of government being a dictatorship. Another was identified as a song in Kurdish, also a political song, translating roughly as "for the sake of my homeland". One was identified particularly as a song by "TT" (we have disguised the name), described as a Kurdish and English rapper. AB said that he wrote the song and music with the help of the Welsh guy who was one of the three singers identified elsewhere from the website.

22. Concerning CD the respondent said that she is a female national of Iran who was born in 1975. She is a political science graduate who was employed in various positions before getting a permanent job in Iran as a translator with the state broadcaster. She entered the United Kingdom in 2010 on her own passport with valid entry clearance as a student and claimed asylum about three months before her leave lapsed. The appeal was dismissed by the First-tier Tribunal and permission to appeal was given to the appellant because:

"insufficient weight had been given to her blogging activities; that she was a genuine political activist; and that insufficient weight had been given to her expert evidence about blogging and the way bloggers are identified and treated in Iran".

23. Although we received, and noted, additional evidence we have no reason to go behind the findings of the First-tier Tribunal. It follows that this is a case of a person who was awarded a first-class masters degree at [university redacted] in Tehran in political science in the year 2000. She started work as a teacher but she was stopped working as a teacher because she objected to the contents of some of the books from which she was required to teach and she was not sufficiently diligent in promoting and encouraging students in the ways of Islam. Nevertheless she was able to get a series of short-term jobs with the Islamic Republic of Iran Broadcasting Corporation with a particular interest in the analysis of the political news and events in the Middle East. She was stopped getting a full-time job by the actions of Herasat because she was not thought to be sufficiently loyal to the supreme leader or to Islam and in the presidential election of 2009 she campaigned for the Green Movement.
24. In the case of EF the respondent says that he is a male national of Iran born in 1972. He travelled from Iran to Turkey where his passport was stamped and returned to him. He entered the United Kingdom illegally in September 2011 and claimed asylum on arrival. He relied on his having co-founded a Facebook group called [WEBSITE]. The group had 1,500 members. Before the First-tier Tribunal he relied on his interview given to [company redacted], an internet-based telecommunications company which was placed on YouTube. The Tribunal granted permission to appeal and an error of law was found and it was observed that none of the findings about his activities in Iran were directed to stand.
25. We have reflected carefully on EF's evidence and the way it was challenged. We found him a substantially truthful witness. He makes no claims that are extravagant or otherwise inherently beyond belief and the reasons for disbelieving him do not, we find, amount to very much. The point most energetically pursued against him was that he was unable to identify the make of his computer. He has given two different explanations but they are not inconsistent. At interview he said that the computer was given him by his

brother and on a later occasion in his statements he explained that computers in Iran tend not to be bought as an entire unit from one manufacturer but assembled from parts. It is within our knowledge that computers tend to have common design features and the manufacturers put much emphasis on interchangeability and compatibility of components.

26. We really cannot accept that EF is unbelievable because he does not know the name of the main maker of his computer or because he has given different but not inconsistent explanations for his ignorance.
27. We accept that EF had helped establish a group called [name redacted] with the help of four friends and this group expressed opposition to the Islamic regime. The group is identified on Facebook and they showed some discernment before they allowed someone to be a member. We accept that a cofounder of [name redacted] was arrested, that this was seen by a friend who warned the appellant who decided to leave. He left Iran irregularly for Turkey. After he had gone he had been told his computer had been seized. We accept that he had saved illicit material on his computer of a kind that would concern the authorities. His explanation of being able to obtain news filter codes from Voice of America is, we find, wholly consistent with the background material and inherently believable.
28. We accept further that he has established the website [WEBSITE] in late 2009 or 2010 and had used no privacy settings. He did have some security in that a person joining the account was, usually, checked. That account was hacked by "Soldiers of Islam". This is apparent because of a posting in that name purporting to close the account. They also established a new group [new group redacted] but this was a closed group and had at the time of writing over 5,000 members. He had used YouTube as a means of broadcasting his activities and uploaded twelve videos onto that site. He was twice interviewed by [company redacted] which is accessible via the YouTube account and so recordings of the interviews could be seen. These interviews were when he was in the United Kingdom.
29. The appellants called expert evidence.

Mr K G

30. Mr "KG" gave evidence before us. His identity is known to the parties and the Tribunal but is disguised here to protect his safety. Although called by appellant CD he gave substantially unchallenged evidence about the internet in Iran and we set out his evidence first because it illuminates the rest. We set out his evidence first because he was the witness best able to describe the ways in which the Iranian state monitors computer activities and how some computer users respond.
31. He adopted his report dated December 2013. It includes the customary expert direction and an explanation that he had worked as an IT specialist with knowledge of computer forensics for more than eight years. He had worked in Iran for five years in that capacity and had some experience working for governmental organisations as a contractor. He had personal experience of setting up a small network to bypass Iranian filtering systems. He had also read the statements from other papers provided by CD about her case.

32. His curriculum vitae showed that he had worked as a forensic specialist and a network administrator and has designed computer systems for a major insurance company in Tehran and has worked as a network administrator involved with the transport industry in Iran. He holds a university degree and he has been a Microsoft Certified Systems engineer since 2002. We regard these as the qualifications of a graduate level computer technician and we found his evidence helpful, clear and in accordance with his experience.
33. He had answered written questions arising from his statement. We do not find them particularly significant in themselves but we have noted them and evaluated them with the rest of his evidence.
34. He said that internet censorship began in Iran in May 2001 at the initiative of the then supreme leader Ayatollah Khomeini who dictated the policies of the Iranian Ministry of Telecommunication and Information Technology. President Khatami opposed adopting measures without the approval of parliament but the Supreme Council of the Cultural Revolution mandated Regulations concerning internet use, the most important of which concerned filtering.
35. In the early days the operation of the filtering and monitoring systems was neither substantial nor extensive but it developed over time. Filtering is a process whereby activity on the web is electronically checked for particular content, typically but not exclusively, certain words or patterns of words that interest the body organising the filter.
36. Ayatollah Khomeini introduced the Supreme Council of Virtual Space which was tasked with safeguarding the revolution against potential harm in the growing distribution of information and communication technology. The report then included a detailed explanation of how filtering can work. The internet service in Iran is unusual, probably unique, in that the design priority is ease of interception. The quality and speed of service provided are not important.
37. There were at the time of writing over 600 internet service providers in Iran offering various subscription services. These included a few internet service providers run by the Iranian government. The rest are private companies, chiefly parsonline.com, phishgaman.net and laser.ir.
38. However, one of the major internet service providers is TCI.ir operated by Iranian Telecommunications Company. The internet service provided by TCI (Iranian Telecommunications Company) is slow and expensive. For example, in the United Kingdom a typical internet service provided by British Telecom of 16 megabytes per second is available to the end user for £16 a month. In Iran a service offering half that speed (8mps) would cost the end user the equivalent of £600 per month. This is approximately six times the minimum monthly wage in Iran but even then additional payments would be needed to get a meaningful service. TCI provides infrastructure and cabling to the end user but charges for a faster service than it has any intention of providing. It owns and operates the entire Iranian telecommunication and internet infrastructure and allocates bandwidth to ISPs. It is a government agency affiliated to the Ministry of Telecommunication and Information Technology.

39. All internet traffic converges at TCI before being routed into the worldwide internet. The most common kind of internet access was “dial up” using an ordinary telephone line.
40. The maximum permitted internet speed was set at 128 kilobytes per second for home users. This compares with a UK average of 8,601 kilobytes per second. The Iranian parliament in January 2011 announced that it would not increase the maximum internet speed for householders and a maximum internet speed of 128 kilobytes per second gives a download speed of only 16 kilobytes per second. The minimum needed to watch low quality television on line is 52 kilobytes per second. He suggested that this was done quite deliberately to facilitate state control.
41. Nevertheless by 2012 Iran had 42,000,000 internet users.
42. The Iranian parliament has prohibited websites carrying a range of content from political and social subjects to pornographic material. However, there are many different government organisations involved in filtering and controlling the internet. These include the Supreme Council of Virtual Space, the Committee for Determining the Criminality of Web Content, the Iranian Cyber Army and the Information Exchange Police. The Iranian supreme leader has authority over appointing officials to all of the aforementioned government bodies. It is believed that the Supreme Council of Virtual Space has the most important role in devising internet management strategies.
43. However, the Committee for Determining the Criminality of Web Content is the ultimate decision-maker on what is legally permissible and what is not and is responsible for creating a list of banned websites. Sites can be banned because, for example, they have inappropriate social content, being against Islamic principles, being a threat to national security or having taken any action to bypass internet filtering. The Supreme Council of Virtual Space and the Committee for Determining the Criminality of Web Content have a close relationship and share committee members including the intelligence minister, the minister of science, research and technology and the head of the Islamic Republic of Iran Broadcasting. The Iranian prosecutor general monitors all the bodies involved in controlling and filtering the internet in Iran and is responsible for submitting the list of banned websites to the Iranian Telecommunications Company and other organisations in charge of distributing web content.
44. In 2007 a new law required all website owners and blog publishers to register and in the same year the Iranian parliament enacted a provision that all web content contrary to Islamic values and traditions is prohibited and banned. The Regulating of Internet Websites Act introduced a total of sixteen categories of restricted content. Some of these were directed to restricting criminal activity such as money laundering or disclosing military secrets. Others restrain the distribution of pornographic material. However, others were vague and to western ears rather sinister. For example, “insulting the supreme leader or the late Ayatollah Khomeini”, “misinterpreting the revolution”, “encouraging pessimism and weakening popular confidence in the government”, “showing methods of bypassing internet filters” and “atheistic assertions” are all restricted. Punishment for violating the consequent Rules can attract a fine of up to £20,000

and a maximum prison sentence of fifteen years. Web use known to have attracted filtering includes peer to peer communications, websites serving foreign media and conservative websites as well as active critics in the domestic media. The following are given as examples of undesirable content: Voice of America, the BBC, web blog and websites reflecting news, pictures and videos such as YouTube relating to political protest as well as sites with immoral content and guidance on anti-filter utilities, proxy servers, Virtual Private Networks servers, sites dealing with gold valuation and currency exchange and even websites connected to the former President Rafsanjani, President Khatami and the British Embassy.

45. Notwithstanding the high degree of Regulation, web content filtering is an arbitrary affair so that even registered unauthorised websites can be closed down or filtered without notice. For example, during President Ahmadinejad's re-election campaign many opposition activists turned to social network and internet news websites and the government responded by filtering and then banning almost all social network sites and disabling all instant messaging ports such as Yahoo Messengers and Google Talk.
46. The report then explains the methods of filtering in Iran. It is not for us to comment on the mechanisms involved. The point is that it is possible to block IP addresses so that traffic is stopped, to limit internet bandwidth, to permit detailed scrutiny, to pick up key words such as "anti-filter", and to classify certain traffic as unacceptable. Thus, for example, all activity with "Skype" could be stopped, and data could be subject to both deep packet inspection and shallow packet inspection as it is transferred. Shallow packet inspection could throw up something of interest and divert the data for deep packet inspection. In this way a relatively quick and broad examination of data can be used to identify areas of particular interest which can then be examined still more thoroughly.
47. All filtering and monitoring in Iran was done through a single location in Tehran using a combination of different local and imported filtering and monitoring appliances from major manufacturers. Much of this equipment has been obtained through third parties to avoid international sanctions. The equipment has the ability to oversee traffic from instant messaging such as Yahoo, MSN and others, emails, internet telephoning, receiving and sending email, transferring files, web traffic and secure web traffic. The filtering could be done very quickly and make a record which can be inspected later.
48. There are ways around this equipment. The most common method is "tunnelling". It is not necessary to understand it in detail for the purposes of this determination. It essentially depends on the little parcels of data that have been transferred being encrypted at their source and decoded at their destination so there is only nonsense to intercept between delivery and arrival. Commonly the tunnelling server is outside Iran so filtering systems within Iran cannot know both the source and destination of a particular piece of data. However, such systems are imperfect.
49. Further it is believed that individuals associated with the Iranian security apparatus have deceitfully provided Virtual Private Networks with anti-filtering tools so that people who think that they are making their data secure are

actually sending it directly to the government. By using devious means the government agencies have managed to hack into servers and decode user names and passwords for Google, Yahoo and Skype users.

50. The Iranian government are also believed to have been involved in “DNS spoofing and phishing”. These are ways of copying the log-in pages of well-known websites and so deceiving users into disclosing their identities to the Iranian state when the user thinks that he or she is logging into the real product. In a similar way government-sponsored hackers present themselves on the web as attractive women in an effort to stimulate a victim’s sexual interest and so disclose personal details to the hacker, thinking that they are attempting to contact the woman.
51. In 2004 a number of bloggers in Iran were detained and held in isolation and then interrogated with the result that they gave away information about their own websites and the people who use them. In response to pre-hearing written questions from the respondent, Mr KG referred to the following websites: <http://resources.infosecinstitute.com/social-engineering-a-hacking-story/> and <http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>. The “infosecinstitute” appears to link to a serious website dealing with internet security. Symantec is a well known supplier of internet security and although we could not find the particular link relied upon we regard this as a serious and responsible source of information and the link give weight to Mr KG’s views.
52. Government agents also feign support for anti-regime political groups in an effort to be allowed access to their websites. Techniques such as this can reveal information which individually, or collectively, can be used to trace the identity of bloggers. It is believed that many Iranian pornographers were deceitfully convinced to return to Iran by Iranian officials and then arrested on arrival.
53. It was Mr KG’s strong opinion that the Iranian security apparatus was capable of tracking down individual internet users and bloggers operating in Iran to their IT address and then positively identify them to get their full home address, national identity card number and even telephone numbers in Iran. All Iranian internet service providers had to disclose the identity of any given subscriber on request.
54. Additionally the authorities will lure bloggers back to Iran to arrest them. Skilled Russian hackers and Chinese security equipment has been made available so that US Navy computer networks were hacked in September 2013 and SSL certificates from Comodo were stolen in 2011. This claim was sourced by reference to an article on Gizmodo which is an international technology based website which we find is worthy of respect. All of this was disclosed before the hearing and considered by the respondent. KG was not cross-examined on the basis that he was making up his evidence or depending on notorious sources.
55. Mr KG then considered CD’s case specifically.
56. He believed she had done several things to increase the likelihood of her coming to the attention of the authorities.

57. Some of her shared posts on [website redacted] were matters of intense public interest in Iran so some might have attracted the attention of officials. The presence of keywords and phrases such as [X], [Y] and [Z] may come to light during monitoring of the internet traffic to and from Iran.
58. The publication of her web blog name and link on the [journal redacted] along with other well-known web logs such as [redacted] and links to [redacted] and the murdered web blogger Sattar Beheshti may well be grounds for detection.
59. Finally the sharing of her web blog links on Facebook called “Amazing Videos” holds 145,000 members. He listed ten ways in which detection was possible. These are listed as follows:
 - (1) any attempt to log onto the admin page of a web blog from Iran without using a secure connection;
 - (2) any comment concerning the web blog or the sending of links to web blogs on IM (instant messaging) software such as Yahoo, Messenger, to an individual in Iran would enable the Iranian authorities to identify her email address and the address of anyone with whom she communicated on IM, typically her friends and family;
 - (3) any comment concerning the web blog or the sending of links to the web blog through SMS to an individual would enable the Iranian authorities to identify her telephone number and that of her family;
 - (4) any comment concerning the web blog or the sending of links on chat and internet telephone software would enable the authorities to identify her telephone number and that of her friends and family;
 - (5) any response to emails from an unrecognised source may disclose the geographical location by passing on her IP address to the receiver;
 - (6) chatting with unrecognised individuals or sources can disclose her geographical location;
 - (7) opening infected links may introduce spying and monitoring software;
 - (8) opening emails that were infected by spying and monitoring software;
 - (9) establishing friendships with unrecognised individuals and sharing personal data;
 - (10) sending personal information by the website manager of blogdoon.com at the request of the Iranian authorities.
60. He had examined CD’s web blog and described the security as “quite low”. He was particularly concerned that there was no encryption on the link during the sending and receiving of data so it would be easy to monitor and check internet traffic from Iranian users on the web blog.
61. It would also be possible to hack into the web blog. He explained how he had managed to capture a packet of data which contained user credentials belonging to the web blog administration who wanted to log into the web blog. He explained that this was done by arrangement with permission and had not as far as he was aware been done in any way unlawfully. He was able to set a trap so that when http communication was detected it was captured and the packet contained the sender’s and receiver’s IP addresses. Also the contents of the body were seen and it was possible to obtain the user word and password necessary to log in.

62. Additionally she had explained to him that she had been sending her web blog link through SMS using free text websites to friends in Iran. The websites were using her real telephone numbers to send a message to the recipient address. If she used the same telephone number to call her friends and family it would be easier for officials to intercept her phone conversations and thus identify her. She had also been using instant messaging (IM) software to promote her web blog but all IM communications were monitored in Iran and incorporated into database records. Officials can search keywords by phrases and the database records can be searched for keywords and if she had ever used her web blog link in any conversation, for example to update or check a web blog with anyone in Iran officials would be able to detect the web blog on the database records and get her email address and view its whole contents. He regarded her real identity as “highly prone to detection”.
63. In conclusion he believed that people who were not well-informed and astute about internet operations in Iran would find it difficult to be aware of all the necessary security measures or to remember to use them every time. He said that even individuals with considerable knowledge of internet security had eventually identified themselves and been arrested. He said by way of example one Shaygan Esfandiari operating in Vandar Abbas who was the web blog manager of gameron.wordpress.com had his identity detected by security officials because of one simple mistake which brought him to their attention. After purchasing an item from a television channel from abroad and having had a telephone conversation with the company he expressed his discontent with the product on his web blog and was eventually traced back. This illustrated the ability and determination of the Iranian state to identify bloggers of whom it did not approve.
64. Having identified his report he was asked questions by Mr Hodson.
65. He confirmed that filtering a website is “really easy to do”. The Virtual Private Networks created a supply of encrypted and decoded data and the word “Private” in VPN could be properly understood as virtual encrypted network. He described the constant battle between the government and the people as encryption and interception software vied for supremacy. He believed that the Iranian authorities could find anything because they have full access to all communications.
66. He was taken to page 21 of 22 of his report under the heading “Summary on Filtering” and the example of the web blog in CD’s case. Under the heading “A Web Blog” he listed four ways in which her blog would be attracting the attention of the Iranian officials. He explained that those four things were things he identified from the web blog name by intercepting and examining the web blog.
67. He was then cross-examined.
68. He confirmed that he had never worked for a government body gathering data and was not involved in purchasing software for the Iranian state. But he did know what software the Iranian government had and arranged with a friend to enable him to test the security.

69. He said that the Virtual Private Network connections are a common tool in Iran. It is not something that is bought but is something that is paid for as a service. He explained that the Virtual Private Network was a way of bypassing the Iranian internet service. Essentially computers are linked together so that they communicate with each other but without using the services of an internet service provider in a way that can be detected easily.
70. He had explained in his answers to written questions that he had produced a screenshot of an instant messaging monitoring tool. He did not mean to imply that the tool he had used is the one that would be used by the Iranian authorities. Rather he had used one commonly available to illustrate how easily it intercepted things.
71. His report referred to an article on a Reuters website dated 10 March 2013. This explained how the Iranian authorities had blocked most Virtual Private Networks so that only legal and registered Virtual Private Networks could be used. This theme was picked up from a report from Cenet. Virtual Private Networks were still allowed to operate. He had not accepted that it was simply a case of them having been infiltrated and operated as a lure. Rather it was a constant battle between people and the government. The government could not shut down everything.
72. He was shown a report entitled "Freedom on the Net 13" at tab 17 and page 622 of the respondent's bundle. This confirmed that customers of cyber cafés must provide personal information before using a computer and that the café owners were required to keep such information as well as browsing histories for six months.
73. The report continued:
- "In addition, the CCL obliges ISPs to record all the data exchanged by their users for a period of six months, but it is not clear whether the security services have the technical ability to process all this data. When purchasing a mobile phone subscription or prepaid SIM card, users must present identification, facilitating the authorities' ability to track down the authors and recipients of specific messages."
74. He explained that the data that would be kept would be of limited value. For example, if he was ordering a Digital Video Disc the record would not show the film that he had ordered but it would show the address he had contacted. The information would be stored at least for a time so that it could be searched later. He was then shown a report entitled "Enemies of the Internet" dated 12 March 2013. In the section on Iran it noted that Virtual Private Network technology can be used to circumvent content blocking and censorship in Iran. Indeed the Iranian state sells that kind of technology in order to profit from the demand but the report advised people not to use Iranian VPNs and also warned that the Iranian government's surveillance resources are constantly changing, so advice which might be good when given will not be good for long.
75. However, the report said that the regime "does not yet have the resources for keeping millions of internet users under surveillance". He was asked if he agreed. He believed that all activity could be recorded although not all could be constantly analysed.

76. He was then asked about social engineering techniques. He said the example of Mr Esfandiari was an example of a person who was well-informed getting caught because of a momentary act of carelessness. It illustrated the extent of the monitoring and how easy it was to come unstuck.
77. In re-examination he corrected a minor mistake in his antecedent history which did not seem to have concerned anyone. He then referred to a screenshot at page 24 of the bundle (23 of the report) indicating how easy it was to access a web blog and net information. It was easy to extract a password and get an email address and profile.
78. He was asked questions arising from that. He confirmed that the evidence was that the internet was slowed down in Iran. If you bypass it you could not surf the web except very slowly. A person who bypasses filtering gets a better speed.

ANNA ENAYAT

79. Ms Anna Enayat then gave evidence principally adopting her report dated 8 December 2013.
80. Ms Enayat's short curriculum vitae was included in the papers. She has given evidence about conditions in Iran on several occasions and her evidence has generally been well received. From 1966 until his death in 1982 she was married to an Iranian and has lectured in economic sociology at Tehran University. She is presently a Senior Common Room Member at St Anthony's College, Oxford University.
81. Her report is supported by published material which it identifies fully and is frequently supported with detailed extracts. A few inconsequential errors were discovered by written questions posed by the respondent before the hearing and these were corrected.
82. She began by reflecting on how the use of electronic media hugely facilitated the social unrest following the revolt against the 2009 election coup. She described a "heroic exercise in grassroots organisation/mobilisation/citizen journalism". The authorities understood very well the potential power of the internet to frustrate social control and determined to curtail it. The government of Iran has set out to censor and restrict internet activity by increasingly sophisticated surveillance and legislation. It declared itself intent on constructing an "intranet" on the Chinese model but implementation, although much talked about, has not happened.
83. Iran had also been damaged by the Stuxnet Trojan which did much to damage Iran's nuclear installation in 2009 and 2010. Here the internet was used by an enemy of Iran to infiltrate, control and destroy apparatus used in Iran's nuclear programme so that the programme was significantly delayed. Thus forewarned the government set out to limit the impact of globalisation on Iranian society and culture, described by the regime as the "soft war waged by the West" and to stop opponents taking advantage of the internet to further their own ends.
84. An Israeli study concluded that Iran had allocated US\$1,000,000,000 to develop technology and expertise in using and controlling the internet. Considerable resources were being invested in designing the architecture of the Iranian

internet to make it particularly conducive to widespread surveillance. Considerable business was being done with a joint venture between Finnish and German companies trading as Nokia Siemens Networks.

85. Ms Enayat referred particularly to an article published in “The Atlantic” by Chris Good entitled “Internet Surveillance and Iran: a Primer”. The article posed a conundrum:

“If Iran puts so much effort into monitoring its citizens, how come we keep seeing cell phone videos of protests and violence; how is so much information coming to us via Twitter?”

86. The simple answer was that the Iranian groups who use the internet were themselves very “tech-savvy” who were well-versed in using decryption and proxies and other devices and there was a considerable gap between identifying an IP address and tracing that to a particular known user.
87. Ms Enayat was inclined to accept the view that at least in 2009 the authorities did not have the resources to tackle every net-based activist. Nevertheless the 2009 demonstration spurred the authorities to be still more vigilant. In 2010 Nokia Siemens Networks acknowledged it had sold equipment capable of tapping telephone calls to the Iranian Telecommunications Company but said it had not provided the software necessary to intercept and monitor internet usage. That denial was contested.
88. Creativity Software Limited (UK) and Ericsson AB had provided location monitoring assistance. AdaptiveMobile Security Limited (Ireland) had provided equipment capable of intercepting text messages at the rate of 10,000 messages per second and storing them for six months. Further the government had acquired via Denmark Israeli-supplied filtering software and in December 2010 a US\$130,000,000 deal was concluded with a Chinese corporation to supply telephone and web surveillance systems described as “extremely powerful”. According to a Reuters report a former telecommunications project manager in Iran said that the Chinese-made system was “countrywide” and “far more capable of monitoring citizens than I have ever seen in other equipment”. It claimed to be able to locate users by their voice, text messaging, emails, chat conversations or web access.
89. As well as necessary equipment the Iranian authorities had established appropriate bureaucracy. The Centre for the Surveillance of Organised Crime was, from its inception in 2007, effective at actively tracking, identifying and then arresting “netizens”. Having operated discreetly in March 2009 it broke the news that it had destroyed over 90 pornographic websites and 45 people were detained in connection with that operation. Photographs and alleged confessions of the people detained were posted and some broadcast on state television. Five of the group were sentenced to death.
90. In late 2009 there was another round of arrests of cyber activists including one Hossein Ronaghi Maleki, who was reputed to be expert at setting up proxies to bypass filtering. He was sentenced to fifteen years’ imprisonment for spreading propaganda against the regime and allied offences. These arrests were all

attributable to the work of the Centre for the Surveillance of Organised Crime, which is better known by its website “Gerdab”.

91. In 2012 Gerdab initiated a project called “Eye of the Fox”. Its declared purpose was to punish alleged BBC Persia contacts operating clandestinely in Iran and several journalists were arrested and later confessions appeared. In 2009 and 2010 Gerdab’s commanding officer boasted of the organisation’s technical skills.
92. The Revolutionary Guard also controlled the “Cyber Army” established in 2009. Its function was to destroy networks and arrest hundreds of netizens. Originally it was comprised of highly skilled Iranian hackers. There is some uncertainty about its precise organisation. It may be a rather loose arrangement of computer technocrats working for IRCGC or Basij units. According to the Wall Street Journal in March 2012 the Cyber Army was far larger than previously believed. It claimed to have trained 120,000 “cultural soldiers to combat a soft cyber war against Iran”. Their function was to monitor online activity of opposition groups and dissidents and bombard websites with comments supporting the regime. It also hacked into emails and computers.
93. Ms Enayat then quoted one Ali Jamshidi whom she described as a Malaysian-based telecommunications expert working for the opposition Green Movement. He said:

“These strong measures to confront the internet recently prove two things: the internet has been an extremely effective way of distributing information and the regime is frightened by it”.
94. He said that the strong measures proved both the efficacy of the clampdown and the government’s fear of internet activity.
95. From 2011 the Iranian authorities have announced the formation of the Cyber Police generally known by the Persian language acronym Fata. This was conceived as an anti-revolutionary organisation that would oppose dissident groups on the internet. The organisation was raised because of the effective use made by dissidents and anti-revolutionary groups contacting each other both within Iran and other countries. The Cyber Police have announced their successes reporting arrests and crackdowns on virtual private networks.
96. Ms Enayat quoted a March 2013 report of the UN Special Rapporteur for Human Rights in Iran dealing with the case of the blogger Sattar Beheshti. According to this report:

“Mr Beheshti was reportedly arrested by the Iranian Cyber Police Unit on 30 October 2012 on charges of ‘actions against national security on social networks and Facebook.’ His family was reportedly summoned to collect his body seven days later. During an interview for this report, an informed source communicated that Mr Beheshti was tortured for the purpose of retrieving his Facebook user name and password, that he was repeatedly threatened with death during his interrogation, and that he was beaten in the face and torso with a baton. The source also stated that Mr Beheshti reported chest pain to other prisoners and that authorities were made aware of his complaints, but no action was taken. A domestic report released in January 2013 by the Majles’ National Security and Foreign Policy Commission criticised the Tehran Cyber Crimes Police Unit for holding Mr Beheshti in its own (unrecognised) detention centre, but fell short of alleging direct wrongdoing in his

death or of calling for an investigation into the apparent widespread maintenance of illegal detention centres, operated by branches of Intelligence services, in contravention of Iranian law.”

97. In December 2008 the Special Prosecutor’s Office for Computer Crimes was established in anticipation of ratifying the computer crimes law. It was intended to be dedicated to the further restriction of internet freedom and was part of a “broader project”. The July 2009 Computer Crime Law was said to be “saturated with provisions that criminalised legitimate expectation”. Further the government was given an unfettered discretion. The range of activities were objectionable including content which offends public virtue, content offensive to the sanctities of Islam, content undermining security and “social peace”, content against state officials and institutions, content encouraging the commission of cyber crime, and “content encouraging other crimes”. Clearly these things are widely drawn. Insults to Imam Khomeini would be offensive to the sanctities of Islam. Republication of banned material or providing links to other sites would come under the heading of encouraging other crimes. Content against state officials and institutions included mocking public officials. Other offences were extremely vaguely worded and included “disturbing public opinion”.
98. Ms Enayat could not provide data on the number of sites currently blocked by Iranian government filtering processes but extravagant phrases such as “tens of thousands” or even “millions” were frequently used.
99. Ms Enayat drew attention to the tension between the determination of the Iran authorities to restrict the internet and the extensive use of the internet made by Iranian citizens. Notwithstanding this extensive use, Iran is believed to have the most sophisticated form of website filtering available using a “key word” system currently used only by China, Iran and Tunisia. Of the estimated 25,200,000 Iranian citizens who have access to the internet about 30% of internet users were thought to use Virtual Private Networks (“VPNs”) to circumvent controls. Tor and Hotspot Shield were also frequently used. Until March 2013 when it was discontinued extensive use was made of Google’s RSS reader but that has now stopped.
100. VPNs are necessary for Iran to remain connected with the internet to conduct commercial and financial transactions and it is understood that VPNs are used extensively by government agencies, banks, media companies, research institutions and even the Islamic Revolutionary Guard Corps (“IRGC”). From time to time the government rails against VPNs. Gmail from Google was regarded as the only secure email service and it has been blocked by the government on occasions. However, when it is blocked there is vehement protest, not only from ordinary users but from parliament and government officials. However, the government has made extensive use of phishing and it is thought that in the summer of 2011 as many as 300,000 computers, primarily in Iran, were penetrated.
101. At part 2 of her report Ms Enayat looked particularly at the use of social media by Iranian nationals in the United Kingdom. Although radio and television broadcasts remained important the overwhelming proportion of writing critical about the Islamic Republic of Iran was produced on the web. Save for a few sites

such as www.iranianuk.com and www.stockholmian.com which are determinedly parochial serving the needs of local Iranians, diaspora web activity is transnational.

102. There have been three particularly respected studies (two of them academic, one by a journalist) concerning the use made by the Iranian people of the internet and the overall picture is of widespread and diverse use. Every conceivable topic appears to be covered including cooking, sport, poetry and religiously conservative views as well as secular and reformist views. A study by Harvard University in 2008 showed that notwithstanding the use of the internet by secularists and reformers internet blogs on the whole were not blocked. Although, perhaps unsurprisingly, blogs by secular reformists were more likely to be blocked than ones that were clearly benign.
103. There is also significant interaction between political blogs inside and outside Iran. Following crackdowns within Iran a “high value” is placed on maintaining the flow of cross-border information. There is clear evidence of numerous arrests for unacceptable comments made on blogs within Iran and at the end of 2010 and the beginning of 2011 around 70 Christians were arrested in coordinated dawn raids within Iran. These were all people who had converted to Christianity from Islam under the influence of the UK-based “Elam Ministries” and they were believed to have been exposed by way of Facebook. Perhaps the mechanism of their being exposed is unimportant. It is clear evidence that the authorities were able to link people to their Facebook activities.
104. Certainly in 2011 eight people were sentenced to between five and eight years’ imprisonment for engaging in unacceptable religious debate in an internet social network. They were detained in solitary confinement for prolonged periods as intelligence agents tried to link them to European embassies and countries even though the discussions that had attracted attention had been purely religious.
105. A report by Freedom House in April 2011 referred to the Iranian authorities interrogating protesters and activists and confronting them with copies of their emails and asking them for passwords to their Facebook accounts. They were also asked about their “friends”.
106. A later report from a journalist confirmed the first thing that the Iranian forces seek when a person is detained is the password to the email and Facebook accounts. As a countermeasure such information is now shared with trusted friends who have a duty to change the passwords in the event of a person being arrested.
107. There are also reported cases of Iranians returning to Iran being interrogated at the airport and asked to give their Facebook passwords. One person who claimed untruthfully not to have a Facebook account watched his guard conduct a Google search which revealed he did have an account. His passport was confiscated but he was allowed to leave the country after several rounds of interrogation in a month.
108. Although the authorities are believed to have sophisticated software for the surveillance of Facebook activity some observers believe that the most common method of tracking identities is to become a false friend. Several student

activists had reported approaches from people with identities that turned out to be spurious. One reporter explained how his interrogator during detention demanded to be made a friend on release. He was threatened with further imprisonment if he did not cooperate and had to advise his real friends not to make any contributions to the website. He speculated that many people did not know of the risks posed by false friends. Ms Enayat pointed out that there is little enthusiasm to return to Iran amongst the diaspora and particularly not amongst those who have views critical of the government. She referred to two cases of people who had returned believing things would be all right and finding that they were not.

109. Thus Rojin Mohammadi, a Kurdish medical student at Manila University in the Philippines, described herself as a human rights activist who kept a blog. She was arrested on her arrival in Iran in November 2011 and taken to Evin Prison. She was released on bail after 24 hours but five days later security agents attended her father's house seeking to re-arrest her. She was not there. Two days after that she was summoned by telephone to attend Shahid Moghadisi Revolutionary Court in Evin Prison. Her belongings including her computer were confiscated. She was interrogated over three days and arrested again on 23 November 2011. She was eventually charged and then released after five months awaiting trial. She fled the country in 2013. She said that the authorities seemed interested in her contact with the Green Movement. Ms Enayat was unable to say exactly what had caused the difficulties but pointed out that the complainant was an educated woman who returned to Iran not expecting any difficulty.
110. The second concerned Bahar Alinia, who was arrested a week after she arrived at Tehran. She fled the country.
111. Ms Enayat made the point that although censoring has to be done instantaneously surveillance can be done stealthily. It is easy to record electronic data and peruse it later. In that way it is not difficult to assimilate a great deal of material which might on scrutiny incriminate someone. Although it is not difficult to establish a blog or Facebook page without a name or using a pen name the author can often be identified by friends and acquaintances and also on a background investigation in the event of a person's return. Questions about internet activity are part of the standard stock of questions speaking to someone at the airport.
112. Ms Enayat was emphatic that the evidence does not support the conclusion that only people with a big following outside Iran attract attention on return. According to an Associated Press article one Beheshti was on the fringe of Iranian online opposition. His blog had fewer than 30 followers in October 2012, yet he was warned the day before his arrest that if he did not stop communicating information he would be killed. He was described by Radio Free Europe as a "minor figure of the blogger sphere" but he was tortured and killed.
113. Secondly one Omidreza Mirsayafi was seen as a minor figure of no known influence, yet he was so ill-treated that he died. He was arrested for his blog in April 2008 and sentenced to 30 months' imprisonment for "insulting religious leaders and engaging in propaganda against the Islamic Republic". He suffered a

complete nervous breakdown and died as a result of medical neglect in prison. He was a middle class intellectual whose blog was primarily devoted to cultural subjects, particularly traditional Persian music. Occasionally he included posts of a political nature. He described himself as a cultural rather than a political blogger. He had no intention to insult anyone and did post perhaps as many as three to six satirical comments over a number of years. His blogs were in his minds “completely private”. They were read by only a few of his friends. According to his lawyer there was insufficient interest in his writing for it to be regarded as publication. The Computer Crime Law allows for mitigation only if it can be shown that less than ten people have seen something complained of. In short, the Iranian state might be fearful of something that seems to attract little popular attention.

114. The authorities appear to be concerned by the influence of satellite television channels broadcasting into Iran. Although there are occasional raids resulting in mass confiscation of equipment at least 25% and possibly as much as 60% of Iranians watch satellite television. Satellite television is provided not only by internationally known major organisations, such as BBC Persian, but also by smaller groups supported by members of the diaspora. Thus an academic running a serious website with a few followers might be perceived as the kind of person who would support “damaging” satellite TV.
115. It was reported that members of the BBC Persian staff had false Facebook accounts created in their name which contained blogs wrongly attributed to the real journalists and used to discredit them and present them as spies. The director of Voice of America described a similar pattern. It was said to be a source of considerable frustration to the Iranian authorities that they spend “millions, if not billions” of dollars every year to perpetuate the regime’s official story only to see it undermined very swiftly by independent internet-savvy dissident journalists. The website did not need to be based in Iran to attract attention or to be blocked. Anything that could be accessed from Iran (bearing in mind that circumvention software and proxies are commonly available) could be seen as a threat to Iran.
116. There was considerable uncertainty in the diaspora about the kind of conduct that could create difficulty. The example was given of one Mohammad Reza Pourshajari who wrote under the assumed name of Siamak Nehr. He was arrested in Iran in September 2010. He had used the Google blog spot platform to post serious articles, many critical on religion and politics. This attracted no obvious sign of concern from the authorities until he attacked the ruling of Shia clergy in a particular matter. He was quickly identified and arrested. He was sentenced to four years’ imprisonment for insulting the supreme leader, actions against national security and blasphemy. It is not known how the authorities identified Siamak Nehr as Pourshajari.
117. This suggested that anyone engaging with political activity may, potentially, be punished on that account. Activities (to western eyes) as trivial as attending meetings, distributing fliers in the street or taking part in demonstrations could be enough. Human rights activity is seen as propaganda against the state. Dissenting religious activity such as that carried out by evangelical Christian

communities is also a route to persecution. A web blog or Facebook page or similar activities supporting any of these things can give rise to persecution.

118. Ms Enayat had detected a sea change in attitudes to returnees in about 2009. Before then there was a policy of encouraging Iranians overseas to return but after the 2009 presidential elections and the following political crisis there was a “marked shift in the Iranian establishment’s attitude to the Diaspora of refugees”.
119. A retired Iranian High Court Judge explained how there were existing laws that enabled the judiciary to bring charges against Iranians for conduct committed outside Iran and another unnamed Iranian judge spoke of the need to stop people who would try to destroy the reputation of Iran. Essentially returnees were held for a few days awaiting the police to prove they had done nothing political. An unnamed airport official said that all returned Iranians would be interviewed and detained. A person who had not been involved in helping foreign powers or engaged in propaganda against the Islamic Republic would be allowed home but these things can take time to determine. These things were not new but were more overt since 2009. Several cases of returnees being detained and interrogated are documented in detail. Airport security is the responsibility of the Ministry of Information and Security (thought of as the Intelligence Ministry) rather than Immigration Officers. The Revolutionary Guard also has a presence at the airport and there is an apparently efficient watch list so that people known to be of interest to the authorities are intercepted on return.
120. The report referred to the Gozinesh records which are state-managed files containing information about a citizen. These include notes on the person’s political and ideological profile and that of his family members. Any activity on the web that has come to the adverse attention of the Revolutionary Guards monitoring unit would be made available to Ministry of Information and Security officials.
121. The interest of Iranian security organisations in email and Facebook accounts has been frequently reported. An interest in Facebook and email passwords has been reported during security checks.
122. If it comes to the attention of the authorities in Iran that a person has been returned there is “a near certainty” that the person will be interviewed. A person returned without travel documents would have to obtain them from the Iranian Consulate before return was possible. Clearly this would attract attention. Similarly a person travelling on temporary travel documents of a kind that could be obtained voluntarily without the involvement of, for example, British officials, would attract attention on return. There are Regulations concerning enquiries to be made of documents produced when a person seeks a travel document to return to Iran. This will require an account of the applicant’s last exit from Iran and the basis of entry into the United Kingdom. In reality it will emerge if the applicant has sought asylum. There was anecdotal evidence that the Iranian Consulate specifically asked for a letter of confirmation from the Home Office that the person returned had asked for asylum in the United Kingdom. Ms Enayat was satisfied that this echoed practices from other countries and she was inclined to think that the anecdotes were well-founded.

123. Further, although the rules provided for a person who had status in another country but who had exited Iran illegally to atone for that error by payment of a small fine before return there were no analogous provisions for those without status.
124. Ms Enayat was not able to establish what happened to people who were returned to Iran having left illegally without making good their position before departure. The offence of illegal departure appeared to be compounded with other matters for the purpose of punishment and much appeared to depend on the discretion of a particular judge. By way of example she drew attention to cases, typically but not exclusively of Kurds who were sent to prison for illegal exit and a political offence.
125. A returnee arriving at airport security with a computer can expected to be examined.
126. Ms Enayat referred to the “high likelihood” of internet activity being discovered during background investigations even if the person being returned was not already known to the authorities. The Iranian regime would expect asylum seekers to have “spread lies” and such behaviour is taken seriously and would attract punishment.
127. The report then turned its attention directly to AB’s case. She had seen evidence from senior KDPI officials in the UK confirming AB’s claim to be a member of the Kurdish Democratic Party of Iran both before and after he left Iran. AB’s blog written in Iran between November 2009 and January 2010 identifies him as a KDPI supporter.
128. This included a post published on 22 January 2010 marking the anniversary of the foundation of the short-lived Mahabad Republic on 12 February 1946. The post is a statement from the new youth of struggle and resistance in Kurdistan which is a pro-KDPI youth group which AB recognised in his screening statement. The same blog includes a link to pictures of the persecution of the Kurds in late 1979 including executions at Sanandaj Airport. There are also photographs of AB attending two meetings in the United Kingdom which were posted on the KDPI website. AB was clearly visible in several other photographs.
129. Ms Enayat believed that it was “likely” that these photographs would have been seen and archived by the Iranian security forces.
130. Since arriving in the United Kingdom AB has used a second blog to publish KDPI statements and events.
131. Ms Enayat profoundly disagreed with the finding in the determination that his attendance at KDPI meetings in the United Kingdom was not sufficiently threatening for his presence to be noted. In Iran low level KDPI activists like other pro-Kurdish activists, are regularly arrested in Iran and often severely ill-treated. Ms Enayat could see no reason why people active in the United Kingdom should not be just as interesting to the authorities in Iran who, presumably, would be keen to know who was joining the KDPI. The current regime regards even peaceful Kurdish activists as dangerous separatists threatening the Iranian state. She believed there were “many cases” of Kurds being arrested and convicted of offences simply because of contact with or

cooperation with an opposition party. It is not necessary to be a member of a party to attract persecution in Iran. Even low level activities such as demonstrating or distributing leaflets and no more can attract punishment.

132. The report then drew attention to a fact-finding report by the Danish Immigration Service published in 2009 about low level activism amongst Kurds. This refuted completely any suggestion that low level activism was somehow safe or tolerated by the authorities. An example was given of a person acting as a courier without any understanding of the items being carried but carrying them out of family obligation. Such a person may well know nothing about a political opponent organisation but would still be treated as a political opponent. The report recognised that a high profile activist was “sure to be persecuted” but there was a prospect of persecution for a low level activist innocent of any political commitment.
133. Amnesty International had reached a similar conclusion, again giving the example of a person carrying leaflets in Kurdish that could be seen as opposing the government risking maximum penalties available to the judge.
134. The appellant AB had authored two blogs. One used from November 2009 to January 2010 had 22 entries and another used from March 2011 had over 400 entries. They were written in Persian and Kurdish. Ms Enayat had read all of those written in Persian and some of those written in Kurdish. All that she had read contained political subjects, including many political cartoons and occasional social problems. The first blog written in Iran was particularly critical of the Islamic Republic depicting it as “cruel, dictatorial, self-serving and corrupt”. The blogs particularly rejected the theocratic political order and called for its overthrow by peaceful means. The blog showed a good knowledge of politics but also expressed a childlike rhetoric which Ms Enayat found to be characteristic of Iranian political satire. The cartoons were of a kind widely available on Iranian opposition website but the content of the blog could not be tracked to another source causing Ms Enayat to conclude they were indeed written by AB as he claimed. She suggested that the tone of the blogs and particularly the strong criticism of Ayatollah Khomeini put AB at the risk of facing the death penalty.
135. AB’s criticisms of the Iranian regime are wide-ranging and severe. He attacks the Constitution, foreign policy, the truthfulness of the leaders and accuses them of bloody suppression of demonstrators and mass murder of Kurds. One posting included an image said to have been created by AB of an Iranian banknote with obscenities written in English and Persian on the forehead of Khomeini. There was also a slogan “death to the Velayat-e Faqih” which she translated as the “guardianship of the religious jurisprudence”.
136. The second blog was a collection of over 400 items in Persian and Kurdish. The content was exclusively political consisting largely of statements and reports and notices from the Kurdish Democratic Party of Iran but also including Amnesty International and Human Rights Watch Reports on Iran, some of them translated into Kurdish. There were also a number of political cartoons. Unlike the first blog it is predominantly a collection of existing material but exhibits the same themes of anti-clericalism, a commitment to the overthrow of the

government, a commitment to a freely democratic future for Iran as well as Kurdistan, a desire to expose rights violations and so on.

137. The appellant AB's Google Plus account was linked to one of his blogs. When his proper name is typed into Google the Google Plus page appears with AB's photograph and his blog immediately afterwards.
138. He had a Facebook page in the name of [FB redacted] which translates as [FB redacted]. The Facebook room was devoted to satire and mainly comprised cartoons, jokes and videos making fun of the Islamic Republic. There were also links to satirical comedy videos which were clever and professional in their content. Many of the clips came from a comedy channel run by "Iran National TV". The link was obvious to anyone with an interest in Iranian affairs because of the distinctive logo and this would attract the attention of intelligence agents. It was produced by the Mujahedin which the Islamic Republic had always seen as its archenemy. It is severe in its punishment of those it regards as Mujahedin supporters. Reposting of Mujahedin material may not lead to AB being suspected of being a Mujahedin activist or member but it would reinforce the conclusion that he actively promotes the overthrow of the state.
139. The Facebook page is linked to one of the blogs and the appellant's hip hop albums with the result that any regime monitor who came across it will have access to the rest of the internet profile.
140. The report then considered AB's YouTube channel.
141. When his name was keyed into Google the appellant's music albums and photographs appeared even though he uses different names on his albums and photograph. There were eighteen items on his YouTube account. One was a 1980s marching song of Kurdish guerrillas. The description refers to the "Islamic Republic of Iran's holy war against Kurdistan and the Kurdish people". Use of Yahoo and MSN search engines produced similar results.
142. She then considered AB's rap/hip hop album on the internet. AB sings in Kurdish but the song was described by Sheri Laizer as a "very deep-rooted political song against Iran mullahs' regime of over 30 years". Ms Enayat believed that the musical genre would be just as objectionable as the content. Rap/hip hop is immensely popular amongst young Iranians as an underground musical genre. Rap groups cannot sell their music on the open market and release them over the internet. They can of course be blocked by filters. Performance is always secret and recording studio is underground. The state-owned media mention rap only to criticise it and often describes it to followers as a "satanic cult". Rappers are depicted as morally corrupt. In the eyes of the authorities rap music is part of the "soft war" promoted by the West.
143. She regarded it as "uncontroversial" that the Iranian authorities attempted to suppress rap. She then gave examples of the difficulties faced by rap artists. One Aria Aramnejad, whom she described as a "pop singer", was held in solitary confinement for 44 days, tortured, sexually humiliated and, *inter alia*, obliged to walk barefooted on the blood of AIDS patients. He was sentenced to nine months' imprisonment and then a further twelve months for other songs. Other examples were given.

144. She believed that the appellant AB had been a political, cultural and internet activist. He had produced a regularly updated blog carrying “explosive political material” and resumed activity when he came to the United Kingdom. He has composed and performed hip hop songs which he has placed on the internet. One of the songs has obvious political content. This form of music is reviled.
145. Ms Enayat suggested that there was a “considerable likelihood” that he would have come to the attention of the authorities already by reason of his internet activities, especially the second blog that carries his full name and by observation of his Facebook page which is public and leads to the blog and music uploaded and by observation of the music on the internet and identifying him as a Kurdish dissident and by his presence at KDPI meetings. Certainly for a time there was reason to believe that the Iranian authorities could not access the Google blog spot platform but she did not know if that was still the case.
146. In any event the blog would come to light during interrogation.
147. The report then listed a variety of offences that might be used to prosecute the conduct identified. Punishments included imprisonment, in extreme cases for up to ten years, and his being lashed.
148. The report then drew attention to cases of known persecution.
149. One Sonayeh Tohidlou described as a blogger and activist was given 50 lashes for insulting the president. A twelve month prison sentence was not enforced. It was reported that her blogs were printed out and put to her during interrogation.
150. Then Laleh Hassanpour was sentenced to five years’ imprisonment for “weighty crimes and social conspiracy, propaganda against the regime, blasphemy and insulting the president”. Sakhi Rigi, a blogger and political activist and member of the opposition leader’s campaign staff, was sentenced to twenty years’ imprisonment by a revolutionary court. Deyman Aref was sentenced in March 2010 to a year in jail for propaganda against the regime by speaking to foreign media. He was also lashed 74 times for insulting Ahma Dinejad.
151. Under the heading “General Conclusion” Ms Enayat explains that Iran is unashamedly an Islamic state. It follows that criticism of the state is criticism of Islam and any political party advocating a secular state is proscribed. The legal mechanisms used to enforce oppression including peaceful dissent are typically vaguely phrased offences such as conduct incompatible with Islam. The Iranian government has set its face firmly against independent civil society organisations including student organisations, women’s right organisations, trades unions, journalists, lawyers and human rights defenders so such people cannot meet or otherwise advocate their cause. Religious groups other than their own are regarded as deviant and thus Sufis, Bahais and converts to Christianity as well as Shia Muslims who advocate an interpretation of Islam other than that approved by the government are denied a right to associate and express themselves freely.
152. Anyone arrested for having crossed one of these ill-defined “red lines” faces incommunicado detention often in solitary confinement and no access to a lawyer until investigation is complete.

153. The internet is seen as an instrument of cultural invasion which is part of the soft war conducted by the West and although there are clearly many in the Iranian establishment who believe in the benefits of a more open policy there is little sign of any change.
154. The mindset of the state officials is that anyone who has fled abroad and applied for asylum should be treated with deep suspicion because they are potentially agents of a foreign power.
155. We find paragraph 156(iii) of Ms Enayat's report particularly apposite and we set it out below:

“An enforced return means that there is a high likelihood that the returnee will be ‘interviewed’/interrogated at the airport and that, given the interest in determining whether or not they have engaged in political or another form of critical activity, their internet presence will be investigated (2b and 3d) – There is a high risk that critical web activity will be picked up on return, given statements by IRI officials and current practice by the security forces where detainees are concerned.”

156. She also opined that there was “a reasonable likelihood” that websites carrying substantial criticism or religious provocation would have been monitored. Understandably there was uncertainty about the extent of surveillance of Iranian nationals outside Iran but the government of Iran was proud of there being no opposition politics in the western sense and in 1996 a court in Berlin was satisfied that there was a deliberate policy of murdering political opponents outside Iran. However, there are no confirmed reports of assassinations in European cities since 1997. The German authorities are concerned that Iranian citizens were being watched when they attended demonstrations in Germany and issued a warning in 2009. There was a case in Norway of an Iranian diplomat who had defected after the election. He said that he had been approached by Iranian intelligence agents who threatened him for certifying results favouring an opposition candidate and asked him to be an informant on Iranian ex-patriots including his own son. When accused of making tape recordings of demonstrators in Norway an Iranian official said “there is no need to record them. We already know who they are.”
157. According to a statement reported in April 2010 the minister of justice, Morteza Bakhtiari, announced that the overall policy concerning Iranians abroad was to create the means for them to return. Individuals who did not have a political file in Iran who had introduced themselves as a political activist solely to get residence abroad would be investigated by the office. In 2011 it was confirmed that charges could be brought against returned Iranians for conduct outside Iran and that included the criminal offence of “propaganda against the system”. Amnesty International's Middle East adviser in London found it in keeping with what was known about the Iranian state not to publish any formalised policy to deal with such people. However, the prosecutor general, Gholamhossein Mohseni E'jei, said her people who were “shamefully cooperating with the Americans and the British and act against their own people, which is a dark stain for them”. Such people could be pursued and punished in the event of return. 270 people were officially executed in 2013 and Iran continues to be one of the world's biggest prisons for journalists and netizens.

158. Ms Enayat then explained how the Iranian president has no direct control of the armed forces or the security apparatus, the radio and television network or the judiciary and all is under the direction of the supreme leader which at the time of writing remained uncompromising.
159. Ms Enayat then responded to questions brought by the respondent. She dealt courteously with the implied criticism for giving opinions beyond the scope of the appeal ordered by the Court of Appeal. She emphasised that it was her view that AB was at risk of persecution in the event of his return to Iran because of his electronic media activities in the United Kingdom apart from any other consideration.
160. The answers consisted essentially of detailed responses to questions raised for clarification. We have considered them and see no need to say more about them here.
161. After adopting the report into her evidence Ms Enayat was asked for any further recent evidence postdating the report (self-dated December 2013).
162. She referred briefly to the case of an Iranian student studying for a PhD at the University of Liege in Belgium and being arrested in Iran on return and being sentenced to several years' imprisonment for espionage although as far as she could ascertain he was not in any way politically active. The account included reference to his being detained in solitary confinement and pressurised to produce Facebook and email passwords. She believed it was very common for there to be coercive requests for passwords.
163. She was cross-examined extensively.
164. She did not agree it was possible to draw a sharp distinction between journalists and netizens. For example, many people who were paid for their reports as journalists also wrote as netizens on their own blogs. She was also satisfied that people were arrested for private comments made on their blogs and often things they had said publicly. However, she was happy to describe a "blogger" as someone who wrote a web blog.
165. Her attention was drawn specifically to paragraph 23 of her report under the heading "The Cyber Army". The IRGC public relations department had announced it had trained and recruited 120,000 cultural soldiers to combat a soft cyber war against Iran. She was asked if the figure was an exaggeration. Ms Enayat could not elaborate on the figure. She was quite satisfied that something called the Cyber Army clearly existed although it seemed to have different skill bases. Her point was that there was a Cyber Army and it was controlled by the Revolutionary Guard. Initially the Revolutionary Guard did not want to admit that it existed.
166. She did not regard the IRGC as the most accurate source of information on activity in Iran. She also accepted that there were bloggers active in Iran in non-political ways, for example, writing about cooking or gardening. She referred to a study done. She accepted that a Harvard University study had commented on the "exceptional flowering of the media numerically and its exceptionally rich content". However, she also said that the blogger sphere had changed since the reported studies had been completed. This was a result of the 2009 crackdowns,

“Freedom House” reporting that widespread arrests and harsh sentences on reporters, activists as well as perceptions of pervasive surveillance had made journalists and bloggers more afraid. Many had abandoned online activities or used pseudonyms.

167. Ms Enayat accepted that there was no reason to think that the state had the ability to monitor all internet users in Iran. However, it did not wish to do that. It wanted to monitor dissenters and there were fewer of them to watch. She emphasised again that governmental sensibilities extended to banning poetry and music of certain kinds and social and cultural activities would be labelled “political” in Iran in a way that they would not normally be so called in western countries.
168. She accepted that millions of Iranians use the internet and that the use of Virtual Private Networks had spread. Ms Enayat did not know the extent to which the Iranian authorities could carry out internet surveillance. She understood there was a Reporters Without Borders report suggesting the state can monitor a million activists.
169. She was asked about people passing through Tehran Airport but she did not know the number. She was nevertheless satisfied from the sources that asylum seekers who are returned are interrogated. This came particularly from the Country of Origin Information Service quoting Amnesty International Reports. She accepted the evidence did not refer to all asylum seekers but just “asylum seekers” being questioned. She said that there had been very few returns from the United Kingdom in recent years and so very little chance of producing data about how many of them were detained. She accepted that her reports were based on 29 returns over a twelve year period. We just do not know how many other people have been returned safely in that time, if any. Nevertheless she maintained that all people who were removed with temporary travel documents were interviewed. She pointed out that there seemed to be similar procedures, possibly centrally controlled and guided, at all embassies about obtaining travel documents and she believed these would create interest leading to scrutiny, and she had anecdotal evidence passed on by someone who was returned on a special travel document because he or she had lost his or her passport and they were detained on arrival and rescued by an important person who was organising a conference.
170. The Ministry of the Interior would be suspicious and interested for example to see if someone had converted to Christianity. The spur was return on a temporary travel document. Attempts had been made to return people on Iranian identity cards but the Iranian authorities did not accept them. That is why returns are only possible with a passport and passports lead to enquiries that could lead to interrogation and persecution.
171. She was asked to comment particularly on the examples that she had used to illustrate her report. It was possible that the Christian couple removed from Norway were in trouble because they possessed a Bible. It was possible that the man removed from Norway was in trouble because he had a false identity document. None of this undermined Ms Enayat’s opinion that people returned to

Iran will by reason of their return attract attention and it is only a short step from being returned to being seriously ill-treated.

172. She was then asked to explain a footnote to paragraph 103 in her report from the Christian Science Monitor of 7 January 2010 entitled “How Iranian Dissidents slipped through Tehran’s Airport Dragnet”. This article appears at page 600 in the bundle of reference materials. Ms Enayat was quick to explain that the article referred to people leaving Iran and how several people believed to be on a watch list were able to leave Iran because of bureaucratic inefficiencies. Ms Enayat said the article showed the extent of interest by the authorities in the activities of its citizens. The fact that several people were able to leave despite the interest the authorities appeared to have in them was not an indicator that people would be all right on return when different procedures operated. She was then asked to comment particularly on the appellant AB. She agreed, as was plainly the case, that much of the material on his blog was not original but was reposted material. She accepted that the records indicated that the blog had only been looked at 81 times in a whole year. In re-examination she reminded us that the penal code required proof of only 10 views for web posting to be sufficiently well published to be capable of being an offence.

ROYA KASHEFI

173. We have reports from Roya Kashefi dated 9 December 2013 and a response of the same date. We refused an opposed application to produce a further report because it was produced too late.
174. Ms Kashefi has studied Iran since 1989 and is the head of the Human Rights Committee and works as an associated researcher for the association Description Chercheurs Iraniens (ACI) which she identifies as an international non-profit organisation dedicated to the unbiased study and objective study of Iranian issues. She built her expertise particularly from studying daily newspapers from Iran and from consulting an extensive and regularly updated library and archive.
175. In her capacity as head of ACI she has presented papers at international conferences and seminars including the United Kingdom Parliament, the United Nations and the European Union. Her report begins by appropriate reference to the Ikarian Reefer guidelines. She has also read the papers in the case. Helpfully her report is divided into three parts. Section 1 looks at the Islamic Republic’s governing structure and ideology. That is helpful but probably not the most important part of the report as far as this case is concerned. Section 2 looks at the Islamic Republic’s attempt to curb free flow of information. This is potentially the most useful part of her report. Section 3 concentrates on this appellant’s case.
176. She begins by explaining that the Islamic Republic of Iran was established by popular mandate after the overthrow of the Shah. There was 98% popular approval although little prerequisite debate on the nature and meaning of an Islamic Republic.
177. Iran follows the Shi’a form of Islam which, although making up only about 10% of the world’s Muslims, is emphatically the form of Islam adopted in Iran. The

President is an elected office but is the second highest office in Iran. The highest is the absolute supreme leader which is a clerical appointment.

178. The revolutionary guard are seen as the guardian army of the Islamic Republic. The Islamic Revolutionary Courts still operate and seek to safeguard the revolutionary ideals of the Islamic regime. Anti-revolutionary activities carry long custodial sentences and sometimes even the death sentence. The regime fears cultural invasion and is particularly suspicious of intrusion from the United States of America or the United Kingdom. Any action against the Islamic Republic in any form is punishable by three months to a year in custody and longer sentences await those who insult Islam or disseminate false information or rumours. It is very firmly her view that “anything is considered low-level dissent”.
179. Further the Islamic Courts are the personal domains of judges and there is no interest in consistency of sentencing with the result that people who have committed apparently similar offences might face very different punishments. Cyber crimes have been particularly addressed by Article 19 of the Criminal Code and are described as “the latest edition to the Islamic Republic of Iran’s vast censorship apparatus”. It is targeted particularly at bloggers and journalists expressing themselves through electronic media. The computer crimes law is not necessary to punish dissidents who can be dealt with adequately by the existing law. Rather it provides a legal mechanism for restraining internet activity and thereby minimising legitimate discussion and criticism.
180. Illegal access to data, computers and telecommunications systems is punishable by 91 days to a year’s imprisonment, a cash fine of five million to twenty millions Rials or both. There are other offences for other activities. Press Law Article 6 prohibits a huge range of activity including publishing atheistic articles, publishing reports against the constitution, spreading rumours or untruths, objectifying men or women, creating discord between people, insulting Islam and other matters. It is broadly and imprecisely drawn.
181. In the section of a report “Freedom of opinion and expression” Miss Kashefi explains that one of the most important tools of the Islamic Revolution was the audio cassette. These could be mass produced cheaply and distributed easily in a society where freedom of speech and freedom of the press were extremely limited. Persian language radio broadcasts into Iran were also respected and useful in informing the public about the growing revolutionary movement. It is hardly surprising that a regime brought into power by the exploitation of such methods should be very sensitive to others using them or their modern equivalents against them. Thus at different times in post-revolutionary Iran fax machines, video recorders and players were banned or licensed or their use restricted.
182. Satellite dishes and receivers met a similar fate. In November 2012 it was understood there were at least 120 Persian language satellite TV channels broadcasting into Iran. Censors sought to jam the signals. This shows both the determined efforts of the Islamic regime to impose censorship and restrict its population but also its inability to achieve that end.

183. Unsurprisingly the arrival of the internet compounded the government's difficulties. The first internet service provided began operating in Iran in 1994 and it is thought there were in excess of 150 ISBS by 2013. However they are all subject to a degree of government control and the leading firms are closely linked to the government and remain accountable to it. All private ISPs must be vetted by the Data Communication Company of Iran (DCI) and the Ministry of Culture and Islamic Guidance (MICG) before they can be considered for a licence. The DCI is the largest ISP in Iran and most other ISPs get their internet connection through the DCI. The DCI is a subsidiary of the Telecommunication Company of Iran (DCI) which is owned by the Islamic Republic Revolutionary Guards and run by the Ministry of Information and Communication Technology (MICT). It is a level of centralisation that allows the government to monitor, filter, slow down or shut off all internet use in the country.
184. Nevertheless Iran has one of the most vibrant "webs" in the world. Research in 2009 estimated there were as many as 700,000 Iranian blogs and websites so that some scholars referred to Iran as "blogistan".
185. The report then gives a detailed account about one Hossein Derakhsahn who was credited with setting up the Unicode framework for Persian language blogging in 2001 after he had moved to Canada from Iran. He visited Iran in 2008 and was arrested from his home and later sentenced to nineteen and a half years' imprisonment. This was reduced to seventeen years on appeal. The offences were vague but accused him of cooperating with hostile states and insulting the holy sanctities as well as spreading propaganda.
186. Similarly one Hossein Ronaghi Maleki, an Iranian computer expert who had been supporting the Persian blogger sphere by beating filters while living inside Iran was convicted of similar-sounding offences and sent to fifteen years' imprisonment.
187. In the 2005 elections surveillance of the internet was tightly monitored but she gave an account of how the wife of a prominent blogger and journalist was able to use the internet to arrange an online petition when she became concerned about her husband's absence.
188. The Ministry of Islamic Culture and Guidance required all bloggers to register with the ministry and this was met with a resistance movement of people refusing to register. By July 2007 many blogs had been hacked, destroyed or closed by the ministry.
189. The arrival of Facebook, which was available to anyone over 13 years of age with a valid email address in September 2006, provided yet another way for even complete strangers to share and exchange ideas almost instantaneously. It is the nature of Facebook that national boundaries become irrelevant and membership of Facebook opens the possibility of accessing up to 4,000,000,000 people. This easy exchange of information and free expression is perceived as worrying for authoritarian dictatorships.
190. Much of the use made of Facebook in Iran would be described as non-political in western countries.

191. As well as the Cyber Crimes Law criminalising a great deal of web activity the law recognised the need for a working group to assess the contents of websites, blogs and social networking sites to make sure it conformed to required standards.
192. Although denied officially, a Wall Street Journal report claimed that there was a cyber army of such people with 120,000 cultural soldiers established in 2009. It seems uncontroversial that the working group for determining criminal content comprised six ministers, two members of parliament and was headed by the office of the prosecutor general. The group decides what is acceptable to the Islamic regime and prosecutes anyone who does anything that is not. It also identifies sites that should be filtered or censored to protect the user in Iran.
193. Following the disputed 2009 elections the website of the Cyber Defence Command of Sepah Pasdaran repeatedly posted images of demonstrators taken by traffic and security cameras and asked members of the public to identify them.
194. Since 2002 the committee responsible for determining unauthorised sites has been established to identify unauthorised websites and block specific domains without judicial authority. In May 2001 the first official order to censor the internet was given by Ayatollah Khomeini bypassing both president and parliament.
195. The cyber police known as Fata have been responsible for the arrest and detention of various bloggers and Facebook users. One, Sattar Beheshti, died after sustaining serious injuries during interrogation in November 2012. The chief of disciplinary forces described Google as not merely a search engine but a tool for spying.
196. She then gave examples of the death sentence being imposed (although not apparently carried out) against a person who had developed a photo-sharing tool that had been used by pornographers and against a person categorised as a web developer and humorist. Reporters Without Borders had counted 27 arrests between March 2011 until March 2012. Eleven had been sentenced to periods of imprisonment of between three and six years.
197. The internet was slowed down in times of national tension or leading up to election, presumably with the intention of frustrating the free exchange of information.
198. Miss Khashefi then explained how the growing influence of social media was a growing perceived threat to the government of Iran. By way of example, President Obama had asked "Twitter" to reschedule planned maintenance so that its sites remained open at a time when Iranian people could be expected to be awake.
199. She then gave an account of her own use of Facebook. She maintained two Facebook accounts. The one she described as her professional account attracted just over 1,000 friends. She had not met many of them but they were bound by a common interest, in her case women's and minority rights. For their safety she would only accept friends in Iran who had been recommended to her. This was because she believed that security agents posed as activists with fake identities in order to gain access. They used closed groups as well as open groups. She

explained that she used Facebook to gather firsthand information for the reports submitted to for example the United Nations Human Rights Council. She believed that everyone in Iran who had any contact with her Facebook page risked prosecution for threatening national security, disturbing public order, disseminating propaganda or similar offences. She explained that Fata arrested people throughout Iran and not just in Tehran.

200. Those in Iran who used anti-filtering system and VPN (virtual private networks) could be charged with additional offences.
201. Miss Khashefi certainly risked prosecution in the event of her return to Iran.
202. She asked herself directly if Facebook was legal. It was not possible to give a simple answer to that question because of the imprecise nature of internet-based crime. However, it was her view that accessing Facebook is an offence but having a Facebook page or profile is not of itself an offence. However, she said again in her report how in Iran pages devoted to fashion or music, for example, could very easily be seen as political statements and attract punishment. Notwithstanding that prominent Iranian figures including cabinet members and the president have Facebook pages it is very easy for all but the most anodyne of content to attract sanctions.
203. She was aware of the tension between her belief that accessing Facebook was always considered to be illegal and the practice of Iranian cabinet ministers, for example, running Facebook accounts. This appears to be a tension in Iranian society that has to be recognised.
204. Efforts to establish the acceptable alternative to Facebook had met with little success. Nevertheless she was satisfied the authorities did create false sites to identify those using anti-filtering software. In November 2013 the Islamic culture and guidance minister, Ali Janati, called for the removal of filtering from Facebook. High-ranking officials and religious leaders spoke out against his request. No major changes could come without the approval of the supreme leader who had shown no inclination whatsoever to reduce his opposition.
205. The government remained active in its opposition. In her report dated 9 December 2013 she said how 24 people had been arrested by Fata since 26 November 2013. Clearly that may not have been representative of every two week period throughout the year but is indicative of continuing serious opposition to Facebook and similar activity.
206. She then addressed her report specifically to the question of whether the use of social media and similar internet-based activities were reasonably likely to come to the attention of the Iranian authorities. There was no doubt that there was will and capability to set up surveillance systems that monitor, control and censor. That is why specific offences had been created and why a specific police force, Fata, had been created. Nevertheless the greater control of the internet seemed to come through limiting access by slow speed or filtering sites. According to the UNSR's most recent report made available in October 2013 67 internet cafés had been closed in July 2013 and the authorities announced that 5,000,000 websites are blocked. In April 2013 officials estimated that some 1,500 antireligious websites were blocked per month as well as those dedicated to news,

music and women's rights. Some 936 pages in the Persian language version of Wikipedia were blocked. It was believed that much of the removed material was critical of Iran's human rights record.

207. She also explained that since 2012 internet café users had to register their full personal details every time they used a computer and the internet café was responsible for monitoring their online activities.
208. She explained that the use of virtual private networks and anti-filter software made identifying internet users a difficult and time-consuming task but it was clear that some people were detected and punished. Further it took only "the smallest lapse in security" to make identification possible. At 99.2 she explained how the operator of a popular website, "Gameroon", Shaygan Esfandiari, had posted critical items for many years but gave themselves away because of a minor slip. It appeared that Esfandiari posted on his blog a criticism of a satellite station that had supplied him with a defective component. The authorities were prompted to make enquiries and were able to identify the supplier who identified the customer and this led to his being discovered. She explained that identifying "internetizens" was not just a matter of using technology but also monitoring content and thinking about what was said.
209. By way of example she told how a Christian group had been discovered because it made contact by Facebook leading to the arrest of about 300 people.
210. Further the regime's equipment was getting better. It had upgraded its filtering technology and was blocking particular types of traffic.
211. Iran's diplomatic missions were known to have operatives from the Ministry of Information and Security attached to them. This was seen as proof that the Iranian authorities were interested in internet activity outside Iran's borders. She related how a young male student working for the Embassy of the Islamic Republic of Iran had approached her and explained how the unit searched the net for intelligence purposes checking up on local Iranian sites and international groups with a UK presence to stay informed about dissident activities. There is a large Iranian community in the United Kingdom and the United Kingdom is viewed with particular suspicion by Iran. The Islamic Republic also has a presence in London through the Islamic Centre in Kilburn and the mosque network in the UK.
212. She did not refer to any specific evidence but pointed out how it was a clear incentive for security officials to get into closed Facebook groups by deceit because it could be seen as a way of opening many doors. She believed that setting up fake identities by intelligence and security agents was common practice. It did not much matter if they were eventually discovered. Much could be discovered before then. She described it as a "running joke among Iranian Facebook users" to attribute any technical glitch on the site to the activities of Iranian government officials.
213. She was asked to consider the capability of Iranian authorities to identify Iranian nationals outside Iran who make use of the internet. She suggested that the Facebook circle of friends was an obvious route. Further some public figures had public fan pages which were open and could be read easily. She was aware from

her own experience how many of her “friends” would only accept friendship requests from people who used identifiable real names. This was a step against infiltration.

214. She found it difficult to comment on the level of public interest within Iran in views posted on social media and similar places but she was aware of the significant level of public trust shown by high audience figures extended to the BBC Persian Television and BBC Persian website and the regime’s overt criticism in the BBC and UK government. She referred to a slightly self-congratulatory article by Peter Horrocks, the World Service director who thought it “clear that crude attempts to discredit our journalists are failing and ordinary Iranians are increasingly turning to the BBC and independent news they can trust”.
215. He went on to say how the audience reach of BBC Persian TV had gone up to 11,400,000 and Persian TV had a weekly reach of 19% of the overall population of Iran.
216. She was quite satisfied that the Iranian authorities have the capability to block access for Iranians inside Iran to undesirable sites. There seemed to be an ongoing battle. For example, Persian language satellite and internet sites such as Voice of America and Radio Farda offered daily proxy addresses to circumvent censors. Many other sites did the same thing.
217. Miss Khashefi then dealt with the risks faced by a person returning to Iran who had been involved in internet use in a way that annoyed the authorities.
218. It was pointed out that since 2006 or 2007 many blogs had been closed down on judicial orders because of unacceptable content. She suggested that anyone who had come to the adverse attention of the authorities through such activities would not be forgotten. If a person was “wanted” a file would be opened and remain open until investigations were complete. A period of inactivity would not bring to an end the interest. She also pointed out that it was easy to get a profile that was of interest to the regime. There was a heavy presence of intelligence and security agents and their associates in universities and public sector spaces in Iran. It was not difficult for a person who is in any way critical of the government to say something or do something which sparks interest. Even discussing human rights issues can be enough. She was confident from her own contacts in women’s and minority rights activists that such people are often contacted when they have settled out of Iran. Typically if they have already been interrogated in Iran the interrogator makes contact in their new country of residence. Contact typically is through Facebook or email but occasionally by telephone. Similarly those legitimately present in the United Kingdom on student visas can be the subject of interest if they are known to the security forces for their human rights activities. She gave a detailed example of a person known personally to her who had been studying in Manila on a government grant paying her tuition fees. This was suspended until she agreed to cooperate with the agent contacting her for information about other women’s rights activists. She was frightened (the word used was petrified) of returning to Iran because she had been feeding them false information. She deactivated and then deleted her Facebook account about two months before she was due to return and changed

her email address. It made no difference. On her return to Iran in August 2013 she was arrested and detained. She was then confronted with printed copies of her Facebook posts and threatened again that she must cooperate or be imprisoned. The person concerned remained free but under pressure and was required to make weekly reports to agents who contacted her. She presently lived in a small village away from her previous contacts and so had no information that would be of interest if it was passed on. This was described as “not an isolated case” and the writer was aware for another fifteen people who had chosen to return to Iran and who were now being subject to surveillance.

219. Any contact with the media in the United Kingdom on for example radio or satellite television or newspapers or internet news sites receivable in Iran would be likely to have come to the attention of the embassy’s agents as would attendance at dissident activities such as even participating in, never mind organising or leading demonstrations and rallies and attending meetings.
220. Leaving Iran illegally is not of itself a reason to risk persecution. If false documents were used that would be taken more seriously. The problem was that if a person who had left Iran in those circumstances had a profile then there was in her view a real risk of arrest and detention at port. Merely leaving without permission was a punishable offence.
221. This point was made emphatically in the January 2013 COI Report at paragraph 32.22 in the following terms:

“If an Iranian arrives in the country, without a passport or any valid travel documents, the official will arrest them and take them to this court. The court assesses the background of the individual, the date of their departure from the country, the reason for their illegal departure, their connection with any organisations or groups and any other circumstances. The judge will decide the severity of the punishment within the parameters of Article 34. This procedure also applies to people who are deported back to Iran, not in the possession of a passport containing an exit visa; in this case the Iranian Embassy will issue them with a document confirming their nationality ... illegal departure is often prosecuted in conjunction with other, unrelated offences. Such a methodology appears to suggest that it is the investigation into the facts surrounding the easily observable and provable offence of illegal departure, namely the motive for such an act (as a decision to depart illegally suggests a desire to escape prosecutorial/police detection for past illegal deeds), that eventually results in the discovery of the underlying offence, leading to a combined prosecution.”

222. The same approach applies to those who have been identified as having a critical profile by reason of activities such as blogging. Miss Khashefi considered it “highly likely” that someone who was wanted by the authorities or who had come to their adverse attention would be detained on arrival. Their mobile phone and laptop would be confiscated for further investigation and all passwords would have to be revealed to interrogating officers. She considered it again “highly likely” that a person forcefully returned to Iran would be asked to explain their dealings out of Iran and to provide Facebook passwords and checks online against their name would be made. The ease with which a person’s internet-based activity in the United Kingdom would be discovered on return depended to a considerable extent on how they conducted themselves. If they had used their

own name then they would be easy to track down and friends or followers or posted photographs would be a good link either directly to their activities or to things that would reveal their activities. Their treatment would depend to some extent on what they have been doing. However, there was no reason to think that the authorities would make any allowances for the possibility that a person had engaged in activity insincerely in order to improve his claim for asylum in the United Kingdom. Anti-Iranian activity for whatever reason would be dealt with harshly.

223. Miss Khashefi then directed herself expressly to the case of EF.
224. She believed that anyone born a Muslim who renounced his faith to adopt another religion could face the death sentence. She recognised that this was not spelt out in the draft penal code. She attributed that to international pressure and suggested that respect for Ayatollah Khomeini would cause an Islamic judge to follow his wishes and pronounce a death sentence. There was no reference in the report to any example of this being done and her comments might be best understood as speculation albeit by an informed person.
225. She then turned to the [WEBSITE] Facebook profile. She confirmed that this translates loosely as [redacted] and is therefore a challenge to the fundamental identity of Iran which styles itself an Islamic republic. She said that this of itself is contrary to Article 498 of the Islamic penal code facing a maximum of ten years' imprisonment. She accepted that EF had managed to gather about 1,500 supporters. She said that if the profile had come to the attention of the security intelligence forces, as might happen through confession of an arrested friend, the appellant EF would be traced and would be at risk.
226. She said that by possessing anti-filter software EF had committed an offence which could be punished by a fine or three months' to a year imprisonment and that by reason of organising meetings to discuss political views looking for a change in the political structure of the country he risked being charged with incitement, threatening national security, gathering [information] to conspire against the regime and other similar-sounding offences which could be punished by up to 74 lashes and custody for up to two years. The fact that the meetings were small was not an important consideration.
227. She had seen an interview on [company redacted] involving EF dated 14 December 2011 where he publicised his Facebook profile and undermined the revolution by saying that the revolution was orchestrated by the West rather than representing a unified view of the Iranian people.
228. She said that she could see when she visited his [WEBSITE] profile as a member of the public that there were some 935 photographs and 109 mutual friends that they shared. Enquiry of one of those friends showed that on 9 December 2013 a little over 4,000 people were friends with a profile. She described the public posts as "of clearly political nature". Several posts about the "Iranian People's Freedom Front" and an invitation to participate in a gathering about executions in Iran at the beginning of December. She regarded almost every post she could find (as a member of the public) as being punishable under Iranian law.

229. The profile photograph shows the appellant EF and she had seen the same person clearly identified standing next to a “graphic reading” from the [group name redacted]. As far as she is able to ascertain the appellant’s name did not appear on the profile until he was in the United Kingdom. After he came to the United Kingdom he became linked to a YouTube channel in his name.
230. She confirmed that the appellant EF had identified himself as the administrator of [group name redacted]. This was a Facebook page created in February 2012 and is described as an open group. In December 2013 he had had 1,310 “likes”. The posts are open to all members of the public who would care to look.
231. The posts included anti-Islamic rhetoric, mockery of the ruling clergy and an advertisement for a demonstration against executions in Iran on 5 December that was advertised on the page. She understood from a YouTube post that EF was also the secretary general of that particular group. There was a website saying the group’s aims were to unify and organise nationalist groups based the history, culture and love of Iran. On the Saeed Ghahremani dedicated YouTube channel there is video of the group calling for a boycott of the presidential elections. The text is read by the appellant.
232. She also looked at the [group name redacted]. This was also a Facebook page with 7,492 “likes” in December 2013. It had an open public page commenced in 2008. The appellant EF said that he became part of the administrative team in October 2011. She said there was a general news and current affairs page. It was said to be dedicated to unity amongst Iranian people and the territorial integrity of Iran and does not support any political party. It bases its work on universal human rights and values and identified itself as a subsidiary of the Azarbaijan Movement for Democracy and Integrity of Iran. She said that the appellant had support letters from the chairman of the Iran-Azarbaijan movement Zeinali Lohrasb and she identified its website.
233. She had also studied the [group name redacted] which she said had a closed group page so that the administration had to approve membership of the group and posts were not public. In December 2013 its membership was in excess of 5,000. For the purposes of the report she asked to join the group and her request was approved by [WEBSITE]. There were four administrators of the group. The content was general.
234. The webpage indicated that the owner was [WEBSITE]. The last post showed that it had been taken over by “Soldiers for Islam”.
235. She described Jebhe Iran Azad Artesh Areae [WEBSITE] as an open Facebook group which was “most outspoken in its opposition to the Islamic regime”. She described the regime as “monstrous” and “bloodthirsty” and numerous other equally unappreciative adjectives. It invited all freedom-loving Iranians to unite under the banner of the great King Cyrus of Persia who was identified as the founder of secular government and human rights. The pages were news analysis with a nationalist flavour and a membership of 1,636 people. There were posts by members of the group that clearly insulted Islam, the prophet and the Islamic regime.

236. Additionally she had seen a membership payment slip and support letter identifying the appellant EF as a member of [group name redacted] in January 2012 when his appeal was heard but she understood him to be no longer a member.
237. Jebhe Iran Azad Artesh Areae [WEBSITE] and [group name redacted] are particularly relevant because they are identified on Persian Wikipedia as two of the organisations who were initial supporters of the Iranian National Council created by the joining of the Iranian People's Freedom Front and the Azarbaijan Movement for Democracy and Integrity of Iran. This was an organisation created to support the Iranian National Council which was called for by Reza Pahlavi, the son of the late shah. Over 16,000 individuals and groups had signed to show support for the Iran National Council. Over 20,000 people appeared to have taken part in the voting and the founders met in Paris. One Reza Pahlavi was selected as the council's spokesperson and he has attracted international media attention. The Iranian National Council has a Facebook page that has been liked by 31,885 people in December 2013. EF said that he no longer supports the council because of "administrative irregularities" but he is identified as one of the original signatories. The Iranian People's Freedom Front is also listed as a supporting group.
238. She also said that she had seen postings on the YouTube channel clearly identifying the appellant as one who organised and led demonstrations on his YouTube. He had read declarations and given several satellite interviews. He mostly did it on behalf of the Iranian People's Freedom Front. Stations can be picked up anywhere outside Iran.
239. She summarised his *sur place* activities as one who had organised and participated in demonstrations. Photographs and video recordings of those were posted on YouTube and the Iranian People's Freedom Front website, Facebook and [WEBSITE]'s page. They could have been seen by thousands of people.
240. She suggested that his links with Reza Pahlavi and his support for the Iran National Council were ways in which he could have been identified as someone who opposed the regime even if his Facebook profiles had not come to the attention of the authorities.
241. She drew attention to the fact that the audiences for his YouTube posts were limited. No more than 301 viewers were recorded. However, she pointed out that we do not know the identity of those people. She suggested that it could have been officials from the regime.
242. Miss Khashefi then conducted a Google search in the appellant's name using both English and Persian characters. The search in Persian characters identified his YouTube channel including an announcement of his appointment as secretary general of the [group name redacted], a link to the [group name redacted] website announcing the appellant's appointment as spokesperson and deputy secretary of the [group name redacted] including his photograph and a link to a Facebook page with a group of 174 members called the [group name redacted] movement in union with the Iranian People's Freedom Front. There was also a link to a condolence video message to survivors of the earthquake in North West Iran in

2012. The cover photograph is of a group of about twenty people holding the nationalist flag of Iran with a central lion and a rising sun. There were placards reading “Free Iran” and “Dear Khomeini go to hell”. The appellant was shown holding the flag. There was also a photograph linked by [WEBSITE].

243. The English search identified other people with the same name and also led to this appellant’s YouTube channel.
244. Miss Khashefi suggested that in the event of return a simple search by intelligence officers at the airport would identify the appellant as an opposition figure even if he was not already known in that capacity.
245. She pointed out that Iran’s “dissent laws” have extraterritorial effect and the appellant would be punished upon return.
246. She then dealt with punishment for claiming asylum.
247. Miss Khashefi referred to a newspaper article quoting a senior Iranian judge published in February 2011 suggesting that asylum seekers could be prosecuted for “dissemination of false propaganda against the Islamic Republic of Iran” and punished accordingly. Punishment could be assumed to be akin to false witness and that typically attracted a custodial term of between three months and two years or a fine. If the prophet had been insulted then there could be the death penalty and if false or forged documents had been used the offender could be lashed.
248. She drew attention to the Country of Origin Information Report of January 2013 quoting an Amnesty International Report with the disturbing and clear headline “We are ordered to crush you”. There was a report by Swiss refugee agency quoting an unnamed judge complaining that people had been attacking the reputation of Iran by political activities against Iran from abroad. It was explained that a person who was returned would be detained for a few days while the police made enquiries. The report continued:

“If the police can prove that the person was not active and has not done or said anything that could damage the reputation of the Islamic Republic, then they are released. If the person was either politically active in Iran before leaving, or has been active abroad, they must be tried and receive a punishment appropriate to their activities.” (Report paragraph 134).
249. We note that the burden of proof was apparently on the police to prove the innocence of the detained person.
250. Miss Khashefi then examined the returns procedure. Unless the person to be returned admits to having a valid current Iranian passport there can be no question of return without contacting the Iranian authorities to establish the identity and nationality of the person to be returned. This would generate considerable paperwork and gives the authorities an opportunity to make enquiries. A person who had exited Iran illegally would be given a particular form entitled “illegal exit”. Unsurprisingly the form requires the full name, birth certificate, date of birth, the father’s name, United Kingdom address, Iranian address, date of illegal exit, place of illegal exit and reason for illegal exit. The subject is also required to identify their level of education, whether or not they have been conscripted, their telephone and residential address and place of work

and telephone and address in the United Kingdom and details about their spouse and children. A photograph also has to be affixed. Plainly this information gives abundant opportunity to make enquiries about the subject's political activities in Iran or the United Kingdom. Further if any questions are not answered then the subject can expect to be detained on return when more enquiries will be made.

251. Although at the time of writing Mr Rouhani was a relatively new president Miss Khashefi explained that in Iran a person is not allowed to stand for political office without the approval of the guardian council. There really was little opportunity for a person with radically different views being able to stand for election and there was no reason to assume that his election as president would provide for a major change. Undoubtedly there were some encouraging signs. Some prisoners of conscience were pardoned. President Rouhani had chosen women for three important cabinet positions. These things did not change the fact that people were still being arrested for working as journalists or human rights defenders.
252. Her opinion about the risks facing a person returning to Iran was not changed. In her concluding paragraphs Miss Khashefi emphasised that Iran has the inclination and the resources to invest in the best available technology to monitor and control internet use within Iran and that its legal system does intend to criminalise and punish out of country activities that could be seen as being against the interests of Iran. Returning from the United Kingdom had some added difficulty because of British interference with Iran's internal affairs over the last century or so. Whilst appreciating the possibility of a person engaging in online activity insincerely she saw no reason to think that the insincerity would be recognised or found significant by the security forces in Iran.
253. She emphasised how simple use of Google produces enough information to cause difficulties for the appellant EF. Anyone returning to Iran would be "highly likely" to be interviewed and that is the process that can so easily trigger persecution.
254. Miss Khashefi had responded to requests for further information made by the Secretary of State after her evidence had been disclosed. The questions were asked in part to test the sources on which Miss Khashefi relied. In response to further questions about the working of Facebook she said there are "high privacy settings" which are not searchable. These can only be accessed by someone patient enough to work their way through the operational requirements but she had direct experience of such a tightly restricted page. However, such groups are vulnerable if one member is arrested and she was aware of occasions of a group responding to the arrest of one of its members by finishing the group, deleting all reference to it and then having the computers "decleaned" to eliminate all traces. She knew that people did not always observe the security measures. She said that surveillance methods can be frustrated by the use of a pseudonym but she knew from personal experience how activists from Iran residing in the United Kingdom had been monitored because of surveillance of their friends and relatives in Iran.
255. As we understand her evidence it was suggested that surveillance of such people can create a pattern which enables a person's identity to be recognised. She

explained that contact by officials by email is more threatening than contact by Facebook. Email is personal and often carries a request for cooperation.

256. Miss Khashefi gave evidence before us and adopted her reports and answered some supplementary questions. This included confirmation that [company redacted] was an internet-based “television” channel and that [company redacted] was on the internet and on satellite and had a good following in Iran.
257. She was cross-examined.
258. She explained that she had no technical qualifications but had been a blogger and Facebook user since 2008. She explained that Facebook is often used to circulate things by people other than the post they have written.
259. She agreed that Iran was a country that took quickly to new technology and there was often tension between what the government required and what actually happened. For example satellite television was largely banned in Iran but was also widely available. Technology was frequently smuggled into the country and satellite dishes had become available that were smaller than those common in the United Kingdom and worked within the house.
260. She also accepted that condign punishment including lashing did not seem to make much impact on the easy, albeit illicit, availability of new technological products.
261. She also accepted that virtual private networks were seen as a popular way around government intrusion. Similarly the very high price of an internet connection and the deliberately slow speed did not stop people using the internet. International news sites such as BBC and Voice of America provided anti-filter software to overcome government restrictions. The question “is it your sense that there is an ongoing battle to circumvent restrictions” met with the pithy reply “yes, and we have several people in prison for finding ways round”.
262. She also recognised that the Iranian authorities were introducing an alternative to the World Wide Web which she knew as “Halal internet” and “Salaam World”. She accepted that it should not be necessary, for example, to go “outside” for banking. The regime had problems with mobile telephones. It had tried to stop ways of using modern mobile phones to upload photographs immediately.
263. She accepted that Facebook had been used as a survey of about 5,000 people including 2,500 from Iran most of whom had expressed their opposition to the death penalty. She did not know if it was possible to analyse Facebook to see where visitors were from.
264. Again she agreed that there was an active blogging scene in Iran and people were returning to blogging rather than the immediacy of Facebook. She also accepted that the requirement to register blogs was largely ignored. She also accepted that she had set up a Facebook in order to have a very large group of “friends” even though they were not people she necessarily knew. She had set up her account so people could see the news. The number of followers recorded would not necessarily be the number of people who visited the page. However, a follower would know every time a person made a posting.

265. The Iranian Cyber Army was affiliated to the Iranian National Revolutionary Guard. She believed that there was a website set up by Sepah. There were many factions within Sepah and setting up such a site was the kind of thing they did. She accepted that any link between the Cyber Army and Sepah was “opaque and tortuous”. Nevertheless Sepah had strong intelligence gathering units and arrested people.
266. Although Iran had considerable capacity to monitor the internet it also had a high number of internet users.
267. She was referred expressly to an article published in 2013 entitled “Freedom on the Net” from Freedom House. This confirms the considerable restrictions imposed on internet users in Iran. For example, it gave the statutory basis in Iranian law for registration and giving details to owners of cyber cafés. It quoted reports from Reuters and the Wall Street Journal about major Chinese firms providing surveillance equipment, with a presentation showing how Iran’s Mobin Net ISP would potentially have the capacity to utilise deep packet inspection to conduct real time monitoring and to block websites and track users and to reconstruct email messages as a means of its citizens. Thus Facebook accounts and other areas of activity were found to be hacked and defaced with a statement saying that the owner of the page had been placed under investigation by judicial order and other websites had been hacked to portray a meaning other than the one intended.
268. Nevertheless the authors of the report found the role of the Cyber Police or other security forces to be “unclear”, exactly what role the Cyber Police or other security forces had in such activity. There was no doubt that in the weeks leading up to the presidential elections there had been a significant increase in targeted cyber attacks against high profile activists and journalists being traced back to Iranian servers.
269. However, Miss Khashefi had to accept that none of these things were evidence that the state was always able to intervene when it might so wish to do. She also believed that the Iranian authorities did not have the capacity to monitor all activity to and from Iran. Quite literally millions of people wanted to use the internet in Iran.
270. She did not know how the Iranian authorities could monitor activities outside Iran if they monitor them at all. She did not think it far-fetched to suggest that embassy officials or Iranian citizens working under the guidance of their embassies would apply for jobs and she believed there was a media-monitoring unit run by Tehran in the United Kingdom even though there had been no embassy since 2011. She believed it operated from an Islamic centre.
271. It was put to her bluntly that it “must be right” that the internet runs so quickly that Iran cannot possibly monitor everything. She agreed with that suggestion. She did not agree that cyber attacks were limited to high profile targets such as the BBC Persian Service or Voice of America. She said that blogs had been attacked too.
272. She was then asked particularly about EF’s activity. She had looked for [WEBSITE]. Certainly things had been posted as long ago as 2011 and there was

no evidence of this site being hacked by December 2013. Neither was it apparent from looking at the site where to find EF or any names except those freely disclosed. However, there were over 4,000 friends. She was then asked about the website of the Iranian People's Freedom Front. She explained that an administrator or "admins" was the one person who controlled access to the page. Usually the person was the creator or someone to do with the administration of the site. She believed that some of the television sites were based outside Iran. She explained that different broadcasters bought blocks of time. Some broadcasted live. Some broadcast recordings.

273. She confirmed that one of the demonstrations photographed appeared to be a relatively small group of people demonstrating.
274. She was asked about returning people to Iran. She confirmed that Iranian affairs were managed by the Consulate of Oman in the United Kingdom and sometimes for certain things by the government of Sweden. There was skeleton staff at the former embassy where people could go. She understood that there were something of the order of 250,000 Iranians in the United Kingdom. Before the government of Oman was involved people used to go to Dublin from the United Kingdom to get help. The Home Office does not help.
275. Miss Khashefi was later recalled to give evidence. Miss Khashefi was asked about a report she prepared in the case of CD. The report is at page 322 in her bundle. Her main findings were to support CD's claim of having worked as a teacher. The story set out at paragraphs 5 to 15 of that statement including the reference to starting work on a temporary contract because she was unsuitable for full-time employment as a teacher was, in Miss Khashefi's experience, exactly what was done when a person was not known to be disloyal but was not trusted. She said it was particularly difficult for women to be out of work but as a qualified person CD could seek work with a private company. Support for an unsuccessful election candidate would not matter because the candidate would have to have been approved by the supreme leader before offering himself for election. She said that the president is a clever diplomat.
276. We summarise now that report. There is an appropriate expert direction and reference to the **Ikarian Reefer** guidelines. Miss Khashefi had looked at the statements and interview records and refusal letter and also documents from the IRIB (Iranian Broadcasting) and CD's own blogs and internet activities. This includes an article written by the appellant for the [journal redacted] in Iran.
277. Broadly Miss Khashefi understood it to be CD's case that she worked for the IRIB and took time off to get paid study leave in the United Kingdom. She became connected with the Green Movement and was discovered by Herasat. She said there are ways of being removed from state employment. One is exraj, which is simple dismissal. This method of terminating a contract of employment does not prevent future employment by the state. Another is enfesal, which is qualified as enfesal da'em or enfesal movaghat. Enfesal da'em is disqualification permanently and enfesal movaghat is disqualification for a determined period. These decisions are appealable. There was no evidence that the appellant CD had been subjected to enfesal and so she was not prohibited from being re-employed by the state. The employee number is consistent throughout her

payslips, employment documents and IRIB portal and the reference to her employment status being “undetermined – on leave without notice case referred to disciplinary division” seems wholly consistent with her case.

278. Miss Khashefi said that IRIB were in many ways good employers. A person employed with them would have healthcare cover and pension arrangements. Further it would advance her own career to have a long period of working for IRIB even on a continued temporary basis. There was nothing unbelievable about her claim that she was unable to take part in big political campaigns but was careful and considerate and did what she could.
279. Miss Khashefi then explained the operation of Herasat. She likened it to security officers in any public building in the United Kingdom but whereas in the United Kingdom security staff might be expected to be interested in matters relating to physical security and safety Herasat would additionally go a stage further and ensure, for example, that the Islamic model and religious code was enforced. Thus prayer times would happen as required and employees would participate. Similarly fasting would be observed in Ramadan and “un-Islamic behaviour” (such as people of opposite sexes sharing the same lift) would be stopped.
280. She was aware of a statutory entitlement given to state employees to have unpaid leave for up to three years to further their education and the possibility of this being extended for two years to a maximum of five years. Periods of leave could be subject to some local negotiation but there is a statutory entitlement to a holiday of two and a half days’ paid leave for the first month of employment and continuing until a person is allowed four months’ holiday a year. She was not aware of any mechanism whereby CD could have obtained six months’ paid study leave but four months’ paid leave was available to her and it was not inconceivable that a further two month period could have been negotiated locally.
281. Unsurprisingly, continued absence without leave is a disciplinary matter. The correspondence of a colleague claiming that she had seen documents saying that the appellant was about to be dismissed but could not provide copies was in accordance with Miss Khashefi’s understanding of processes in state companies. The person making the report had no right to see the correspondence nor to take an opportunity to find out something to pass it on. She considered it “highly likely” that Herasat would have carried out investigations on CD when she failed to return to work.
282. There would be no objection to CD having published writing before she was contractually employed by IRIB. She was an analyst and the credibility of her employer would be enhanced by appropriate publications. Anything that was published openly would not be too critical. However, any hint of rebellious views would be noted.
283. Miss Khashefi commented on the widespread use of the internet in Iran and how Iran ranked fourth in the world on the number of blogs. The extent of censorship become known only in 2004 when visual sites of organisations such as The Voice of America which were sponsored by national governments or Iranian opposition groups became filtered and unavailable in Iran. The authorities were not

prepared for the enormous explosion in internet use and introduced new laws to combat “internet offences”.

284. Notwithstanding the new laws it was possible for the contributor to remain anonymous. The authorities were threatened by this and from 31 December 2006 it was mandatory for bloggers to register their sites with the Ministry of Islamic Culture and Guidance. Very full details were required including family and contact details. Protest groups developed refusing to register. These included sites on “blogfa.com” and “Persianblog.com” and in July 2007 some of these sites had been hacked and destroyed. She understood that blogfa.com had been hacked, so many bloggers from Iran were experiencing problems. The blogfa management then set up “blogfa.ir” (and transferred blogfa.com over to blogfa.ir). Blogfa.ir was also hacked after the presidential elections. The “Allah’s Cyber Army” took responsibility for that and sites were closed by a notice from Allah’s Cyber Army on the leading page. Blogfa had to respond to the pressure by monitoring and closing questionable blogs. Again she considered it plausible that CD’s blog was of the kind that would have been shut down.

285. The report then dealt with CD’s activities outside Iran.

286. It seemed clear that any activity against the Islamic Republic committed outside the borders of Iran would be punishable within Iran. Since June 2009 the Iranian authorities have made it very clear that they will commence investigations within Iran and seek to use international arrest warrants to arrange a person’s return. Quoting the report, she said:

“this fear is fed by constant announcements from the authorities in Iran that anyone engaged in activities against the Islamic Republic outside Iran would be identified and prosecuted.”

287. Face recognition software has been used since June 2009. She opined that regular attendance at demonstrations was as risky as carrying banners or leading chants. The Islamic Republic believes that protests outside Iran are organised by dissident groups who are criminal. The faces of the “wanted” had been posted on a website set up by the Revolutionary Guard (Sepah Pasdaran), intelligence officers are known to gather in Iranian Embassies and so are ready to act.

288. She believed that, for example, the embassy in Iran had a special media monitoring unit that existed to scour the media reports and news on Iran in case a story emerged that required comment. The same unit worked with another that monitored the web-based activities of Iranian groups for intelligence. Unlike many sites iran-free.org places an emphasis on new writing rather than reposting other stories and for this reason alone could be of particular interest to the intelligence units. Miss Khashefi considered the Gheichi blog to be too new to attract too many readers but noted it was CD’s case that some of her articles had featured on [website name redacted], which she described as “one of the most visited news sites by the Iranian dissident community for dissemination of original writing and views”. Anyone wanting to know news or opinions from Iran would visit it and she had little confidence in the anonymity of a person being preserved in the face of serious enquiry by the well-funded and sophisticated Iranian intelligence service.

289. Public dissatisfaction with the declared results of the elections of June 2009 was so widespread that fear of recognition seemed to have evaporated. In the United Kingdom, for example, many people were second or third generation Iranians growing up outside Iran and they took part in public demonstrations without apparent concern of being identified. During demonstrations in June and July 2009 outside the Iranian Embassy in London there were examples of members of the crowd identifying people with cameras who, unlike apparently legitimate journalists, were not filming events but filming the faces of people in the crowd. Such people were asked to leave, sometimes with the help of the police.
290. Facebook had emerged as the preferred way of communicating between actual or would be demonstrators.
291. Miss Khashefi is well-known in the Iranian community and said how Iranians frequently confided in her their concern about being identified. One family told her that they had left identity documents at the Iranian Consulate and when they went to return them they were admonished for attending demonstrations. Miss Khashefi had no way of knowing if that story was accurate but she cited it as an example of many similar stories.
292. Iranians had also been recruited to infiltrate the community in the United Kingdom and report and this not only gathered useful information but encouraged an atmosphere of mistrust and suspicion that suited well the purposes of the Iranian regime.
293. A German television programme reported on people who had demonstrated in Germany against Iran reporting that they had been targets for intimidation by the Iranian regime. Notwithstanding emphatic and rather scoffing denials by the Iranian ambassador in Germany, Germany's security police had confirmed reports that there were Iranian agents amongst the crowds outside the embassy. She found it relevant that documents show that CD had been "protected from employment because of her unsuitability rather than because she is prohibited". This was consistent with her claim to have been in full-time employment with the IRIB when she came to the United Kingdom. It was plausible that Herasat would investigate her absence, her pro-reform politics and links with the Green Movement would make her unsuitable for work as a state employee. She would be of adverse interest to the security services in the event of her return. The political benefits of encouraging the Green Movement such as high voter engagement and turnout have passed after the election and conduct that would have been tolerated before the election would now be the basis of an offence.
294. Although at the time of writing she could leave the United Kingdom easily on a valid current passport the involvement of [redacted] at the very least created a risk of her being brought to the attention of the authorities on computer records in the event of her return. Even if she managed to clear the airport any re-engagement with her employer would attract the security forces. Her activities could attract a custodial sentence. London is a centre of political engagement against the authorities in Iran. Many meetings are publicised on Facebook and Twitter. These are the kind of features which will cause the authorities to take an interest in her. Potential interrogation tends to attract ill-treatment and even torture.

295. Miss Khashefi was careful not to overstate her case but said there would be no guarantees of the appellant's rights and in Miss Khashefi's opinion she would risk detention, ill-treatment and torture.
296. She was asked questions drawing attention to her view of the plausibility of the appellant's account. She explained that she did not claim any technical understanding of the internet and she could only write as a user but she was aware of things called Virtual Private Networks and there were privacy settings on Facebook which suppressed a person's identity but she had no idea how effective they were in the face of a determined enquiry.
297. She was cross-examined.
298. She was reminded that she had identified two particularly successful Iranian bloggers (57 and 58 in her report) named Hossein Derakhsahn and Hossein Ronaghi Maleki respectively.
299. There was a government department known as the Gozinesh that had to prove appointments and admission to university. There were private universities where people who failed the ideological test were able to be educated. However, the Gozinesh would be aware of people's failings. For example, she said that if CD had been expelled as a teacher because she was questioning and not sufficiently devoted to promoting Islam then these things could be expected to have come to the attention of the Gozinesh. She said that at the time that CD got her job she would not be excluded by reason of her views.
300. However, she was a contractual rather than full-time employee. She said a lot of competent people were sacked and had to be replaced and they were re-employed as freelancers.
301. She said a lot of things in Iran were done on a personal level. There was nothing unbelievable about the appellant having to attempt to renegotiate the terms of her employment or more accurately the terms of her leave of absence.
302. The article published supporting or at least not being too critical of the Revolutionary Guard is something that would be part of her profile. She was pressed about a letter confirming the appellant's dismissal. She could not find it and accepted that she did not appear to have listed it.
303. It remained her view that the appellant was not subject to enfesal because that was not mentioned in any of the letters rejecting her and so her dismissal as a teacher would not stop her getting work in government service. She had found a translation of the letter at page 303 in the bundle. It is impolite and refers to her application being unsuccessful because the application "has not met with the selection criteria and condition had a sensitive position". But she clearly had seen something that made her think in terms of dismissal which is why she expressed herself as she did at paragraphs 1.4 and 1.5 in the report.
304. She was then directed to page 328 of the report which referred to blogfa. There was a printout from blogfa announcing that it could not provide services for one of three reasons, namely, a violation of the laws and agreements in relation to the use of site services, an order from the legal authorities to block the web blog, publication of immoral content or content deemed to be unauthorised based on

the laws of the country. This was it was suggested rather all-embracing and did not for example have the reference to Soldiers of Islam that occurred in the blocking of EF's case.

305. It was suggested that it could simply be a failure to register the blog because that would be under the heading "Violation of the Laws". She said she would accept Ms Enayat's observations but she was not in a position to comment herself on subscription accounts.
306. She did not know if people who had claimed asylum were identified as such by the Home Office.

Submissions

307. Mr Haywood for AB addressed us first. Although representing his own client all three appellants had points in common and where this is relevant we have considered the submissions as a whole.
308. In very simple terms it was the AB's case that he was an Iranian of Kurdish ethnicity who risked persecution because of his political affiliations and activities just before leaving Iran and after arriving in the United Kingdom.
309. The skeleton argument very properly reminds us that his claim to have had computer material containing incriminating material was disbelieved when the case was first heard in the Upper Tribunal and the appellant therefore could not rely on that strand of evidence now.
310. He said that he, and indeed the other representatives, recognised the initial incongruity between claiming to be at risk because of blogging and allied activities when there was abundant evidence that the internet was widely used in Iran and the huge resources invested in controlling the use of the internet by the government of Iran were plainly less than wholly successful. However, he submitted that although internet use in Iran was widespread it would be wrong to assume that all internet activity involved political discourse. The number of people of interest to the government because of suspected political opposition was significantly smaller, he submitted, than the raw data suggested.
311. It is an important part of AB's case that he had arrived in the United Kingdom without documents. It was plain that he would have to obtain documents in order to be returned and part of his case that the process of claiming and relying on exceptional travel documents would add significantly to the risk of his being persecuted.
312. He particularly drew to our attention paragraph 5.4 of the Iranian Operational Guidance Notes, version 8, dated October 2012 being the most recent ones available. This drew on a "Freedom House" report saying how "the authorities sometimes stopped citizens at Tehran International Airport as they arrived in the country, asking them to log into their Youtube and Facebook accounts, and in some cases forced them to delete information."
313. It is also plain at paragraph 3.15.5 of the OGN that anyone who had left Iran irregularly and therefore could not show by an entry in a passport that he had had permission to leave could expect to be arrested and brought before a court. The sentence for leaving without a valid passport could be as high as three years'

imprisonment although the minimum available sentence was a fine equivalent to about £6. According to paragraph 3.15.5 “the court assesses the background of the individual, the date of their departure from the country, the reason for their illegal departure, their connection with any organisations or groups and any other circumstances.”

314. Mr Haywood submitted that it was clear that there was at the very least a real risk of such questioning exposing political activity either in Iran or after departure. He drew our attention to the Amnesty International Report dated 28 February 2012. This report recognised that there were examples of the Iranian authorities responding positively to campaigning on behalf of depressed people. The general trend was for an increase in restriction and ill-treatment. Further the report made plain that it was not necessary to be involved at a particularly high level to attract opprobrium. For example although the report referred to there being “over ten journalists, writers and bloggers” who had been detained the report continued, “hundreds of prisoners of conscience and political prisoners are currently imprisoned or detained, although it is difficult to provide accurate figures on the numbers held at any one time”.
315. We do not read this report as though the word “hundreds” was hyperbolic. It clearly supports Mr Haywood’s contention, shared by others, that it is not necessary to be a high profile activist to be persecuted in Iran. He then reviewed existing country guidance material which he submitted and that was now of limited value. Nevertheless it was well recognised that returning to Iran is always a potential pressure point. Illegal exit is an offence and an offence that interests the authorities so that people are detained, interrogated and returned. Nothing else happened in the recent past to diminish this risk.
316. This was particularly true in the case of SB (risk on return – illegal exit) Iran CG [2009] UKAIT 00053. The added factor now was evidence of the real risk of enquiry about internet activity and the possibility of that leading to persecution.
317. In SA (Iranian Arabs – no general risk) Iran CG [2011] UKUT 41 (IAC) it was decided that an Iranian Arab was not at risk because of his ethnicity but returning from London which was considered a centre of separatist activity, was of itself a risk factor. In BA (demonstrators in Britain – risk on return) Iran CG [2011] CG UKUT 36 (IAC) the Tribunal recognised that a returnee could expect to be screened on arrival and an activist could be the subject of further enquiry and possibly risk depending on all the circumstances. He submitted that we were now more aware of specific risks as a consequence of activity on Facebook or other media and we now have evidence of people being required to give access to their Facebook accounts. He also drew attention to the finding in BA that a person might pass through the airport but be “picked up” on their return home.
318. He then drew attention to a decision of the European Court of Human Rights in the case of RC v Sweden done at Strasbourg on 9 March 2010 Application No.41827/07. Paragraphs 44 and 45 emphasise that “the Iranian authorities frequently detain and ill-treat persons who participate in peaceful demonstrations in the country”. It emphasises that the evidence shows it is not only leaders who are high profile actors who are detained. A similar point was made in the decision of the New Zealand Immigration and Protection Tribunal in

the case of AP (Iran) [2011] NZIPT800012. This notes with approval a finding in a case reported to it that:

“Dozens of individuals in the US and Europe who criticised Iran on Facebook or Twitter said their relatives back in Iran were questioned or temporarily detained because of their postings. About three dozen individuals interviewed said that when travelling this summer back to Iran, they were questioned about whether they hold a foreign passport, whether they possess Facebook accounts and why they were visiting Iran. The questioning, they said, took place at passport control upon their arrival at Tehran’s Imam Khomeini International Airport. Five interviewees who travelled to Iran in recent months said they were forced by police at Tehran’s Airport to log into their Facebook accounts. Several reported having their passports confiscated because of harsh criticisms they had posted online about the way the Iranian Government had handled its controversial elections earlier this year”.

319. He submitted that it was clear that there would be scrutiny and questions about electronic activity. Mr Haywood then relied particularly on the Operational Guidance Notes to support his submissions that this appellant as an ethnic Kurd was at risk. This refers to a Freedom House report stating how Kurdish opposition groups and separatists are “brutally suppressed”. Amnesty International noted how members of Kurdish minority groups who express “any form of peaceful dissent are vulnerable to accusations of participation in banned Kurdish groups” and that such accusations bring with them a risk of human rights violations including the death penalty. Again according to the Operational Guidance Notes the degree of involvement that was proved did not have to be great to bring with it a real risk of persecution. Possessing a CD or pamphlet could be enough to be seen as acting against national security.
320. He then turned his submissions directly to the problems associated with blogging emphasising, as he had done already, that there was agreement that blogging was widespread. He particularly relied on the report of the death of Sattar Beheshti who was put to death because of “actions against national security and social networks and Facebook”. However, there was also reference to a blogger who was not particularly well-known, dying in custody, and another blogger who according to his sister had no political activities or membership of any group being detained. These were points echoed in the skeleton argument which we have also considered. We consider that skeleton argument now.
321. It is pointed out there was no doubt about the appellant’s links with the KDP. There was support from the organisation identifying him as an active member of the party both in Iran and in the United Kingdom.
322. It is also plain that he had been involved in producing songs which had been posted on the internet. This much had been accepted by the Secretary of State. The appellant was photographed on the site and it was plain that the songs or some of them were supportive of Kurdish independence.
323. It was also plain that the appellant is an active blogger. He blogged before leaving Iran and he blogged in the United Kingdom. The blog prepared in the United Kingdom has his photograph and full name and shows him to be in the United Kingdom. The appellant plainly has a Facebook account and hosts a

room on Facebook under the name [name redacted]. The contents satirises the Iranian regime. There are YouTube recordings of his songs and his photograph.

324. Since being in the United Kingdom he has been to party meetings and there had been no challenge to his evidence that he attended party meetings. He did not play a prominent part in them. The skeleton argument contended that there was a “striking” quantity of material.
325. There was then a very detailed analysis of the Operational Guidance Notes for October 2012. These notes emphasised the role of the Cyber Army and the Cyber command in monitoring internet communications and Freedom House since September 2012 reporting on internet users in Iran suffering from “routine surveillance, harassment, and the threat of imprisonment for their online activities, particularly those critical of the authorities.”
326. We note the use of the word “particularly”. The evidence points to the Iranian regime being sensitive to all kinds of internet activity.
327. The Operational Guidance Note says that Iran is not a country where people will be required to demonstrate loyalty to the government. Presumably this contrasts with the situation that was known to exist in Zimbabwe where there was a real risk of a person being made to show that he was a government supporter and persecuted if he could not. However the same note continues that the Iranian authorities “take serious action against individuals who they believe are critical of, or pose a threat to the state and this treatment may amount to persecution.”
328. Again we note the language that is used. Posing a threat to the state is more than sufficient. The risk comes to a person who is “critical”.
329. As indicated above the Operational Guidance Notes refer to Kurdish opposition groups being “brutally suppressed”. It was not the appellant’s case that a person or he in particular would be at risk simply because of Kurdish ethnicity. Rather it was a case there was a real risk of very grave persecution if someone was seen to be a Kurdish separatist. By the standards of the Iranian authorities he is a Kurdish separatist and returning him would create a real risk of this being discovered if it was not known already because of interrogation on return.
330. The skeleton argument summarises relevant country reports.
331. The US Department of State Report refers to the crackdown on civil society intensifying after the 2009 elections. There are reports of disappearances, cruel inhuman and degrading punishments, judicially sanctioned amputation and flogging, beatings and rape and other harshness. Although some prison facilities including Evin prison in Tehran, are notorious. There was evidence of there being unofficial secret prisons where abuse occurred and prison conditions generally being harsh and life-threatening. The point is made that although there are reassuring constitutional provisions in practice the authorities can and do detain people incommunicado, sometimes for weeks or even months, without trial or contact with their families. The “offences” attract attention are often vague by western standards and include such nebulous activity as “antirevolutionary behaviour”, “moral corruption” and “siding with global arrogance”. The point is that offences of this kind make it difficult to predict with any degree of accuracy just what kind of behaviour is going to attract

adverse attention. However, it is quite clear that journalists generally and Kurdish language newspapers in particular face harassment, opposition or worse.

332. There were 28 Kurdish prisoners in the country facing the death sentence.
333. The Human Rights Watch Report refers to harsh sentences being imposed on journalists and bloggers based on “vague and ill-defined present security laws”.
334. The skeleton argument then looks at the Danish and Norwegian FFM Report and the report from the Danish Refugee Council and Norwegian Landinfo. The same message comes. Human rights activists and reporters were ceasing to report. Many had left. Many were in prison.
335. The same report then noted how an individual connected with Kurdish activities who was caught with a leaflet would be likely to be arrested and tortured and forced to confess. They would be put through a “five minute trial” and the outcome of the trial was wholly unpredictable. There could be a mild sentence or they could be sentenced to many years of imprisonment. The comment was made that it was “impossible to say”.
336. This is an example from the Landinfo of the difficulty of seeing what brings a risk. Again according to the Landinfo Report in a time when political activity and demonstrations were banned criticism is emerged in the blogosphere. The control and censorship of the internet is extensive. The use of a virtual private network is widespread and easy. It is forbidden but it is not expected that use would lead to condign punishment.
337. The Freedom of Expression report was considered particularly with reference to the UN Special Rapporteur. Again the message is of tight press laws, generalised offenses and sharp crackdowns. One Mr Mehdi Khazali started a fourteen year sentence for criticising the government on his freelance blog.
338. The UN Special Rapporteur noted no signs of improvement.
339. It was advanced in July 2013 that five million websites had been blocked and about 1,500 anti-religious websites were blocked every month. It was reported that at least 40 journalists and 29 bloggers were serving sentences in Iran.
340. The skeleton argument relied particularly on Reporters Without Borders information describing Iran as “an internet enemy”. Nokia Siemens was thought to be working perhaps unofficially with the Government of Iran and was involved in the sale of internet surveillance technology. Mr Haywood emphasised how the Iranian Government had equipped itself with a wide range of effective tools for monitoring internet activity and how “posting illegal content or using round about methods to access blocked content is punishable by long jail terms” [911 – skeleton argument 13].
341. He particularly drew attention to the 2013 Freedom House Report which emphasises how the Iranian authorities “continue to restrict access to tens of thousands of websites, particularly those of international use sources, the opposition Green Movement, ethnic and religious minorities and human rights groups.”

342. These startling high figures were justified by further details in the same report which also emphasised the sophistication of the government filters for picking up words or strings of words that were of interest to them. In April 2013 a person described as “a prominent Cyber police commander” described Facebook as “the most disgusting spyware and the most dangerous warfare of the US”. The Computer Crime Law of 2009 identifies punishment for spying, hacking, piracy, fishing, libel, and publishing materials deemed to damage “public morality” or to be a “dissemination of lies”. Punishments are mandated and are severe. Offences against public morality or chastity are punished with death and long prison sentences and draconian fines and other penalties for other offences.
343. He particularly drew attention to the death in custody of the well-known blogger, Sattar Beheshti. Appalling as the death of one person always is, it is perhaps more of interest to us to see that “numerous bloggers remain in prison and are currently serving prison terms of up to twenty years”.
344. He relied very heavily on Miss Enayat’s report submitting that this was “powerful, commonsense reasoning”. Mr Haywood particularly drew our attention to studies that Miss Enayat made about the people who returned, Rojin or Rozhin Mohammadi who is described as a Kurdish medical student at Manila University in the Philippines. She was a human rights activist who kept a blog. On her return to Iran on 14 November 2011 she was taken to Evin Prison. She was freed on bail after 24 hours. However five days later security agents raided her father’s house to arrest her again. She was not there. She was summoned to attend Evin Prison for interrogation and personal belongings including her computer were confiscated. She was interrogated for three consecutive days before being released. On 5 December it was reported that she had been charged with crimes of propaganda. Members of her family were also put under pressure. On 2 January 2012 she was released on bail awaiting trial and she left the country some time in 2013. Eventually she was given permission to leave after five months of delay. Miss Enayat was not able to see her blog but enquiries led her to believe that it was not something that the writer thought serious enough to attract severe ill-treatment but according to Amnesty International both she and her brother were tortured.
345. Miss Enayat also looked at the case of Bahar Alinia. Miss Enayat had been able to see her blog. Miss Enayat described it as “mainly concerned with her personal philosophy on life and political only in the very broadest sense of the term.” Nevertheless on her return to Iran she was arrested on account of her blog in December 2011. After she had been released some time before February 2012 she fled the country regularly. In a subsequent blog Miss Alinia described this as one of the strategies of the Iranian Government. They banned people from leaving the country but also intimidated those who returned. The skeleton argument emphasises (paragraphs 45, 46, 47 and 48) that people who are known to have been in trouble are not people seen as particularly prominent.
346. The skeleton argument draws heavily on the Freedom House Report saying how the Attorney General Officer of Sirjan had warned internet users “to avoid any illegal online activities, such as publishing photos and women not wearing hijab, otherwise there would be legal consequences awaiting them.”

347. Enquiries by the UN Special Rapporteur suggested that Mr Sattar Beheshti's difficulties in custody followed his being severely beaten for the purpose of retrieving his Facebook username and password. He quoted a radio free Europe article stating that the Iranian authorities were able to access Facebook accounts without resorting to hacking but just by obtaining the passwords from detainees under torture. Miss Enayat had relied on a report by Freedom House quoting a number of protestors who were put on trial charged with offences relating to their use of Facebook or a comparable site that facilitated sharing news called Beheshti quoting a number of protestors who were put on trial charged with offences relating to their use of Facebook or a Persian site that facilitated sharing news called Balatarin. Many of those detained said the interrogators confronted them with copies of their emails and wanted the passwords to their Facebook accounts. They were then interrogated about their "friends".
348. Essentially the same points were made independently by a journalist with a particular interest in cyber dissidents. Ms Enayat also gave detailed accounts of people who had returned in circumstances that would not have been thought suspicious being asked about their Facebook activities. A person who said untruthfully that they did not have a Facebook account was detained when he saw a guard "Google" his name. A Facebook account was found and his passport was confiscated. He was allowed to leave the country after about a month but only after several rounds of interrogation. The Iran authorities also spied on citizens by using fake Facebook accounts.
349. The skeleton argument draws attention to the decision of the Australian Government Refugee Review Tribunal in Iran IRN 36407 acknowledging evidence that the Iranian authorities monitor from Iran the activities of overseas Iranians on social network sites as well as storming directly protests. The Swiss Refugee Council (OSAR) drew attention to the unpredictability of the Iranian authorities. It would seem clear that some people were received into the country without difficulty. It was also clear that some people were assumed to be involved in anti-government propaganda or activities because they had sought asylum abroad. However, the Swiss authorities were satisfied from two contacts in Iran that at least generally rejected asylum seekers are interrogated on return and detained whilst their cases are reviewed. The government is anxious about people who "are trying to destroy the reputation of Iran".
350. This Tribunal in BA (Demonstrators in Britain - risk on return) Iran CG [2011] UKUT 36 (IAC) acknowledged evidence of three dozen individuals who had been interviewed and said that they were questioned on their return and asked directly if they had Facebook accounts. Five of those said that they were forced to log into their Facebook accounts by police at Tehran Airport.
351. Mr Haywood submitted it was not easy to see who was going to slip through and who was going to be interrogated and ill-treated. He then focused his submissions particularly on the case of AB.
352. He fairly acknowledged that unfavourable or adverse findings of fact had already been made in this case. Nevertheless there was clear evidence that he had blogged from within the United Kingdom and had identified himself with pro-

Kurdish activities. His YouTube recordings were there to be seen and were sufficient for him to be identified as a separatist.

353. Ms Enayat's report pointed out that Sattar Beheshti was not a prominent blogger and had registered fewer than 30 viewers in the month of his arrest. Mr Haywood particularly drew attention to the appellant's visibility. Ordinary use of Google reveals a photograph of the appellant and a link to his blog. He hosts a Facebook room with satirical content and links to a blog where there are recordings uploaded by him. One of the recordings is of a Kurdish epic song. It came into prominence in Iran's war against the Kurdish people 30 years ago.
354. The "hip hop" posted by the appellant is described as a "very deep political song against Iran mullahs regime". Hip hop itself is reviled as a form of Satanism. He had quite clearly been involved in sufficient things to create at least the real risk of his being persecuted in the event of these things coming to light and there was a risk of them coming to light on return. He submitted the appeals should be allowed.
355. Ms Harrison for EF addressed us and relied on her skeleton argument.
356. This corrected a slip in the finding that there was an error of law by pointing out that the appellant arrived in the United Kingdom on the back of a lorry and it had never been suggested by the respondent that he had his own passport. His case was very simple. He is an ethnic Qashqai who speaks Farsi and Turkish. He is an enthusiastic and prolific user of social media on the internet, particularly Facebook and YouTube and has used these as a way of sharing and disseminating political aims and objectives that are objectionable to the government in Iran. If he is returned to Iran his internet activity both in Iran before he left and in the United Kingdom since his arrival will be discovered and each of them is sufficient to create a real risk of persecution. She submitted that the Country of Origin Information Report for January 2013 recognised that Qashqai people made up about 2% of the Iranian population and although not persecuted per se because of their ethnicity minority groups tended to be more likely to suffer the dispossession of their property and discrimination in education and employment. The government in Iran was engaged in "ethnic restructuring" to force Qashqais out of the oil and sugar-rich Khuzestan province. Their traditional grazing pasture was being sold off to the private sector. Ms Harrison submitted that these contentions were not controversial. They had not been challenged by the Secretary of State and were well-documented.
357. Particularly the appellant said he had been twice arrested and detained by the Iranian authorities. The first was during his third year in high school when he and two school friends were caught drinking homemade alcohol in the holy month of Ramadan. He spent 24 hours in the disciplinary detention centre before being transferred to Firoozabad Prison. He was then roughly treated and lashed with 80 lashes.
358. His second arrest was a year later when he was arrested by the Revolutionary Guard resistance for removing a picture at his school of the founder of the Islamic revolution. His punishment was 48 hours' detention.

359. He said that with four friends whom he named he had established a group aiming to establish a secular government in Iran in 2009. He set up an internet page about a month after the initial meeting of their group and there was an email address associated with that internet page. The appellant and his group became active on the internet, particularly Facebook. He believed that one of his co-founders had been arrested by Etelaat at his own place and had not been heard of since. These points are set out in the appellant's witness statements.
360. The skeleton argument relied heavily on the expert report of Ms Roya Khashefi. The change of leadership did not represent a sea change in Iranian society. The appellant was very much at risk.
361. The Iranian Constitution had developed to ensure that an Islamic state was entrenched and persons such as the appellant who favoured a secular state were its enemies. Internet and satellite broadcasts were received as significant opposition forces that had to be crushed.
362. There were available to various prosecuting authorities a range of imprecise offences against the revolution and these permitted condign punishment for activities of the kind in which the appellant had taken part. For example, the death penalty was a possible punishment for insulting Islam and a prison sentence of between two and six years was possible for insulting the supreme leader. The Iranian authorities did not understand the idea of "low level dissent". Any opposition could attract persecutory punishment. Cyber crimes such as "e-legal illegal access to data" were similarly vague. Any kind of involvement in the production and distribution of obscene material could attract the death penalty. The idea of obscenity in this context again is rather broad. The breadth and imprecision of restriction against internet-based activity would make the appellant's position intolerable if the authorities were aware of what he had done if he was returned.
363. Ms Harrison's argument submitted that the appellant would be very easy to locate. She relied on Roya Khashefi's report which showed that a simple Google search in Persian or English would identify him as someone who had acted against the regime. Although website administrators and Facebook operators tried to be careful it was known that there were intelligence and security agents who befriended, monitored and gathered information on Facebook users. The skeleton argument then moved on to look at the treatment of individuals perceived as a threat.
364. She relied particularly on the reports of the return of the journalist Saeed Razavi Faghieh who was arrested after returning to Tehran from France. He had been in France for seven years. He had previously been tried in absentia. The second report about individuals who blog particularly looked at Navid Mohebbi who gave away his email and blog passwords. The report in question comes from "the Green Voice of Freedom". It says how Saeed Razavi Faghieh was currently held in Evin Prison. This report is of limited value. We are not in a position to form a clear view about the reliability of the Green Voice of Freedom and the report is very short because it tells us little other than he was detained in 2009. Nevertheless, that is another example of a person of interest to the authorities being intercepted on return. The report about Navid Mohebbi is under the

headline “world’s youngest detained blogger on trial”. The report comes from Global Voices Advocacy. He was not allowed legal representation because the charge was of an offence against national security and also of insulting the Islamic Republic’s founder and current leader by means of foreign media. It was his case that he was arrested for no reason in the street. He was released when he gave away his email and blog passwords but required to report back. It seems he did and was arrested. By way of illustration of the nature of his behaviour the article said that in 2009 he wrote about sports he played and going to school and having a small operation on his nose. He also said how he read the book *The Second Sex* by Simone de Beauvoir. He had been accepted at Tehran’s Azad University to read political science. He clearly was perceived to be a risk.

365. The skeleton argument directed us particularly to the international campaign for human rights in Iran, an article entitled “more detained social network users: forced confessions feared”.
366. This is dated December 2013 and refers to the intelligence unit arresting two individuals who had been active on Facebook in “a continuing wave of arrests against internet and social media users and professionals”. This document refers to an earlier report confirming that access to Facebook pages is achieved not so much through hacking capability but by extracting access passwords from detainees under torture. The skeleton argument also emphasises the sinister nature of the closing sentence of the article “forced confessions – frequently obtained under torture – are often the only ‘evidence’ presented by Iranian security organisations when prosecuting Iranian civil society activists and dissidents.”
367. One of the people detained, Mohammad Amin Akrami had been living in India and returned to Iran. It appears that he was detained either on return or as a result of enquiries made on return. In short, this is an example of precisely the concerns raised by the appellants in this appeal.
368. We do not wish to be dismissive of the other points raised in the skeleton argument by summarising them as “more of the same”. They are summaries of background evidence reports which the Iranian authorities are involved in clamping down on dissidents and punishing severely those involved in internet activity. An article from Iran Human Rights dated 9 January 2014 illustrates the conflicting messages given out by different parts of the Iranian governmental structure. For example, in September 2013 Hassan Rouhani gave an interview in which he said that the government thought people should have access to international information although adding that “monitoring and observations should be in the framework of protecting our national identity and model values”. In the same interview he indicated that social networks “are important”. At different times the social media “WeChat” is both praised and criticised by different policy statements. The only thing that was clear is that free access to the internet as it would be understood in the West is not happening. An article from the same website, iranhumanrights.org, dated December 2013 commented on the activity of the Cyber Police in monitoring internet traffic. The police were boasting of their presence, particularly on Facebook, instagram and WeChat.

369. The skeleton argument then referred to the Tribunal's own jurisprudence and also S.F. and Others v Sweden, Application no. 52077/10 which accepted the argument that a person was at risk because of activities conducted in Sweden after a colleague in Iran had been arrested and, it was assumed, persuaded to divest details. The argument then summarised S G's case. It said that he had been prolific in his internet activities and the translations show that he had done enough to be at risk if his activities came to the attention of the authorities. These included his speaking out against the regime on [company redacted] and YouTube where his identity could be established easily. His Facebook page has in excess of 4,000 friends. Anyone accessing his YouTube page can see a video that would be found incriminating. The last few paragraphs of the skeleton argument are particularly pithy, taking the picture still further. It asserts that the appellant "has committed activities in the UK which can be interpreted as crimes in Iran. The Iranian authorities would punish him for these crimes. He is linked to a high profile political movement outside Iran which can reasonably be assumed to have attracted the attention of the Iranian authorities."
370. However, he goes on to say that he would be returned with an attention-grabbing travel document because he no longer has a passport and this would lead to interrogation which would lead to his internet activities being discovered and he is therefore at risk and entitled to international protection.
371. In her oral submissions Ms Harrison respectfully reminded us that we had to make our own findings about what this man had done in Iran or in the United Kingdom. She submitted that there was clear evidence of his involvement in [WEBSITE] and really no reason to doubt it. His internet activities were sufficiently political to create a risk and so the appeal should be allowed.
372. Mr Hodson for CD also relied on a corrected skeleton argument and oral submissions.
373. The skeleton argument suggests that CD's activities in the United Kingdom of posting items on her Facebook page and maintaining a personal blog are sur place internet activities that are to some extent representative of other Iranian asylum seekers. It is, however, a particular and aggravating feature of her case that she used to work for the Islamic Republic of Iran Broadcasting Service as a political researcher. The work she does might well be thought to have a strong political undertone. He submitted that conduct or views unacceptable to the Iranian government is a widely drawn concept. The appellant has been critical of the Iranian regime and expressed views about women and Islam which are sufficiently critical to make her a target. The argument summarised the facts of her case. She is an Iranian national born in 1975 in Najafabad. She entered the United Kingdom as a student lawfully in June 2011 and has remained since. She claimed asylum and was interviewed at the Asylum Screening Unit in March 2011. She was refused asylum. The application was appealed. The appeal was dismissed but the decision set aside with the consent of the respondent for error of law in 2012.
374. Put very simply, it is her case that she risks persecution because of the social and religious beliefs expressed on her personal blog and Facebook postings and other online activities. She was awarded a first-class degree in political science and

worked part-time as a teacher of history employed by the Ministry of Education but was sacked because she questioned the contents of courses and did not promote Islam satisfactorily. She worked for the political research section of the Islamic Republic of Iran Broadcasting Company on a series of temporary contracts and whilst doing that work also wrote freelance pieces of political analysis some of which were published in the Defence Journal Quarterly of the Revolutionary Guards. She made determined efforts to obtain a permanent position with IRIB but was always rejected because she was not sufficiently loyal and the Gozinesh did not approve her appointment. She campaigned on behalf of Mir Hussein Mousavi in support of the Green Movement at the time of the Iranian presidential elections in 2009 and took part in some of the major protests held in the second half of 2009 following the controversial election of President Ahmadinejad. After she arrived in the United Kingdom she was informed that the Herasat had been making enquiries about her and contacted her family objecting to her travelling to the United Kingdom and requiring her to return to face a disciplinary hearing.

375. But she later learnt that she had been sacked from her position with IRIB at the instigation of Herasat. She took part in demonstrations against the Iranian regime in London in February and March 2011 and stopped attending when she removed to Manchester.
376. She had started a blog in Iran and has shown evidence of postings in November 2009. Blogs were posted on blogfa.ir that were unpolitical and social topics without being overtly critical of the Islamic regime. She continued to blog after she came to the United Kingdom when she became more expressly political and openly critical. She then started a blog under the assumed name of [name redacted] which translates as [name redacted]. The blogs were on a variety of subjects inclusive of socialist views for women in Iran as well as expressing her atheistic convictions against Islam and opposition to the current regime. Similar points have been made in her Facebook account. She sees herself as a political analyst and journalist. She has published on the website iran-free.org and subjects have included the democratisation of the Arab world, the role of Facebook and Twitter as revolutionary tools in Egypt and the way ahead for the Green Movement in Iran. She has also given a talk to the National Black and Asian Writers Conference at a festival in Manchester in October 2013 entitled [redacted] drawing on her personal experience as a journalist and a blogger.
377. She is in contact with friends and family in Iran using a variety of well-known means of electronic communication.
378. The grounds draw attention to documentary evidence supporting the appellant's case. In particular (because this has been challenged by the respondent) she has produced copies of IRIB payslips and an IRIB identity card. Also letters confirming her failure to obtain a full-time appointment. There is also an email chain supporting her claim to have been dismissed. There are also photographs which she says are photographs of her at a demonstration or demonstrations in London.
379. Of particular interest are her blogs or summaries of her blogs. The blog purporting to be written on 7 December 2010 is somewhat equivocal. It states

“we don’t want a superstitious government” but does not indicate what government would be seen as superstitious. It continues though that “the biggest corruption is the government corruption” and it shows the reader that “we respect Revolutionary Guards – Vasij is who defend people’s rights”. The article dated 10 November 2010 approves of people who were protesting and praises the “bravery of these Green Movement women”. It concludes “Lady Iran will find her way with her hardworking daughters”. We agree with Mr Hodson that there is a detectable change in style after the appellant arrived in the United Kingdom. For example, the item written on 10 November 2010 is quite unequivocal when it talks about Tehran extending the repression overseas and tells the story of an engineering student receiving a threatening email telling him to stop criticising the Iranian government on Facebook, again to give meat to the thread that his father was captured by security guards at his home in Tehran. The blog dated 16 July 2010 rejoices in women becoming more assertive and independent. An essay written on 13 February 2011 for iran-free.org includes the sentence “the failure of the reformation government which leaded [sic] to suppressing the youth generation is the biggest evidence”.

380. Clearly this is overtly critical of the present regime. The website under the name of [name redacted] has a number of critical postings against the government. Her complaints about the number of people being executed, for example a posting dated 1 June 2011, which can hardly be a comforting thought for the Iranian leaders is entitled “the success of the Syrian movement and the disease called reformism in Iran”. Another on 25 March 2011 is entitled “farewell to religion is the start to living freely”. There is an article under the [name redacted] website under the pseudonym [name redacted] dated 27 February 2012. The article comments on criticisms of an Iranian actress who allowed herself to be photographed naked. Mahtab suggested they should mind their own business and expressed the view that it was Islam that had lost its dignity. She suggested that those concerned should be more concerned by women in Iran using the internet to try and find customers.
381. She then wrote about the attack on the British Embassy in Iran which she described as:
- “the peak of madness and craziness of the government but it seems that it is purposely done; the aim to stop the pandemonium flames of fire is to continue its survival whereas at the time of losing control the sponsors would be the first to be sacrificed.”
382. Mr Hodson suggested that the same liberal feminist outlook is demonstrated in the Facebook pages. Other entries referred to “a moving documentary about the SKSM and the role of the clergy in promoting religious prostitution” and then a reference to someone being tortured to death in Islamic regime prisons.
383. On 5 November 2012 there was a rather emotional reference enjoining the reader to think about a woman imprisoned unjustly and the effect that that had on her family.
384. We were then referred to background material which we have considered but titles such as “Freedom House ‘Iran not living up to promise of greater freedoms’” or “International Campaign for Human Rights in Iran ‘repression intensifies

despite Rouhani's promises' October 2013" sufficiently identify the thrust of the evidence.

385. Our attention was particularly drawn to the Amnesty International Report "We Are Ordered To Crush You" dated 28 February 2012. The opening paragraph, which is wholly justified by detailed examples given later in the report, says how the "net of repression is widening in Iran" and the authorities arresting a range of people who might in the broadest sense be thought opinion formers simply for speaking out against the government or even just expressing views with which the authorities do not agree.
386. At paragraph 4.6 the report says how "bloggers" have been held for long periods without charge or trial before being sentenced to long periods of imprisonment.
387. We know particularly the case of Hossein Derakhsahn who, according to the report, is sometimes called the Iranian "blog father". It is understood that he had started the surge of blogging in Iran by posting in Persian simple instructions about how to set up a website. He was sentenced to a total of nineteen and a half years' imprisonment comprised of a variety of sentences to be served consecutively for such imprecise offences as "cooperating with hostile states" or "insults to the holy sanctities". Most of his blogging had been conducted outside Iran but he returned for a family visit and was arrested at his family home soon afterwards.
388. The report lists a total of 21 people who had attracted the attention of Amnesty International and are considered in the report. The synopses are understandably short but it is impossible to regard the list as composed entirely of people who might be thought to be particularly prominent and therefore particularly objectionable to the Iranian state. There is, for example, reference to one Javid Houtan Kayan described as a legal representative who was imprisoned because he defended a woman sentenced to death by stoning. Similarly Mahboubeh Karami is serving a three year sentence because of her peaceful campaigning for greater rights for women. We note also the case of Peyman Aref, a student activist who was flogged with 74 lashes after being convicted of "insulting the president".
389. We note too the quotation from the Organization Suisse d'Aide aux Réfugiés report of 18 August 2011. This deals particularly with returned asylum seekers and quotes an unnamed judge as saying:

"Asylum seekers are interrogated on return, whether or not they have been political activists in Iran or abroad. If they have tried to conduct propaganda against Iran, they are culpable and are detained until the judge decides the sentence. In recent years many people have tried to destroy the reputation of Iran and this must be stopped. Such people help the opposition groups and their culpability is plain. Returnees will therefore be held for a few days until it is clear to the police, that they have not been involved in political activity. If the police can prove that the person was not active and has not done or said anything that can damage the reputation of the Islamic Republic, they are released. If the person was either politically active in Iran before leaving, or had been active abroad, they must be tried and receive the punishment appropriate to their activities."

390. There are many references in the skeleton argument and reports of bloggers being arrested and detained. We have particularly looked at the Country of Origin Research and Information Report dated 20 June 2010 produced by the Refugee Review Tribunal of the Government of Australia. This report was particularly concerned with protesters who returned from London after the June 2009 presidential elections. This quotes the Wall Street Journal reporting that:
- “dozens of individuals in the US and Europe who criticised Iran on Facebook or Twitter said their relatives back in Iran were questioned or temporarily detained because of their postings. About three dozen individuals interviewed said that, when travelling this summer back to Iran, they were questioned about whether they hold a foreign passport, whether they possessed Facebook accounts and why they were visiting Iran. The questioning, they said, took place at passport control upon their arrival at Tehran’s Imam Khomeini International Airport.”
391. The same report said that five of those interviewed said they were forced by the airport police to log onto their Facebook accounts on arrival. The Wall Street Journal again contrasted information from the Iranian Diplomatic Mission in New York claiming that its officials encouraged and facilitated the return of Iranian citizens to Iran with contrary evidence. He gave the account of an Iranian engineer who attended protests in a European country. When he travelled to Iran his passport, mobile phone and laptop were confiscated and he was called in for questioning on several occasions and blindfolded, kicked and abused and required to hand over his Facebook passwords. The authorities had images of him taking part in demonstrations in Europe. He said that he had only been to a few demonstrations and did not live in Iran. The Wall Street Journal speculated that this conduct was done with the intention of sowing panic in the Diaspora.
392. The Landinfo report for February 2013 deals particularly with Christian converts and Kurdish people and post-2009 election protesters. It quotes the International Organisation for Migration saying that Iranians who return with their passports will not face any problem at the airport and a long stay abroad is not an issue provided the person left lawfully. However, Iranians who left with passports but are returned on a laissez-passer will be questioned. According to IOM nobody had been arrested while travelling back on a laissez-passer. However, its information related solely to those who had returned voluntarily. Nevertheless it had no experience of people being arrested by the authorities at the airports. All Iranian citizens leaving Iran had an exit stamp placed in their passport showing the date of departure.
393. Our attention was drawn particularly to the Australian Government Refugee Review Tribunal country advice on Iran published in April 2010. This concluded that it was “likely that the Iranian authorities would be aware of protests against the Iranian regime by overseas Iranian communities”. A number of sources claim that the Iranian authorities monitor the activities of overseas Iranians via social network sites such as Facebook and YouTube and by directly filming overseas protests. The same article made it plain that “a number of media sources confirm that through its monitoring of sites such as Facebook, YouTube and Twitter, the Iranian authorities were able to track the political activities of overseas Iranians.”

394. The question “is there any evidence that people involved in such protests outside Iran have had problems on return to Iran?” is answered unequivocally in the affirmative. It developed the answer by referring to “a small number of western media sources” claiming that returnees on arrival at the airport were asked to log into their Facebook accounts and people thus questioned were detained or threatened or had their passports confiscated and even disappeared. The report referred to the Wall Street Journal article mentioned above, December 2009, which said how the author had conducted interviews with 90 Iranians in various western countries and noted that “it could not independently verify the claims but the interviewees provided consistently similar descriptions of harassment”.
395. There was a report from someone posting on the American “Foreign Policy” magazine website saying how the writer had overheard an Immigration Officer at Tehran ask someone if she had a Facebook account. When she replied untruthfully that she had not the officer found her name on Facebook and noted the names of her friends. In the Times in July 2009 it was reported that the Persian community in the United Kingdom had been investigating claims that a number of British Iranians had “disappeared” from the airport and returned to Iran. The section concludes as follows:
- “Given the above information and the current political climate in Iran, Iranians who participated in overseas protests against the Iranian government, or who have criticised the government on their Facebook pages, may be at risk of harassment, detention and even disappearance on return to Iran.”
396. The skeleton argument then directed us to Mr KG’s report. This emphasised the use of devices to slow the operation of the internet to facilitate the use of intercepting devices to learn about traffic that is sent. There are reasons to believe that the authorities can track down any computer user if they are sufficiently determined. This appellant operates an insecure system. For example, the [name redacted] website was easily hacked, with permission, by an expert. The report reminded us that even a person who is normally exceptionally careful can still be let down by a careless mistake.
397. Given that the authorities are targeting bloggers and users of social networks and the appellant has expressed views in her online writings that are critical of the government, she is in the category of people who would risk persecution if detected. Opposition by the Iranian authorities is savage and whilst oppression may have peaked in the lead-up to the 2013 presidential election there is no reason to think that it has waned to the point of a person no longer being at risk. A person can be identified because of internet activity outside Iran and, it was contended, real risks exist for the appellant and people in her circumstances without more. On return a person with other than a valid passport properly stamped to show lawful exit can expect to be interrogated and questioned about internet activity and made to give out details such as Facebook passwords which would create a risk.
398. This appellant is at risk for a variety of reasons. Her profile and history have raised question marks about her behaviour. Indeed she has been unable to secure a full-time appointment as a result and is a known political analyst. She was telling the truth when she said she had been under investigation by Herasat.

She supported reformist candidates in past presidential elections and this too would be known. The profile built up as a result of the Herasat investigations would of itself attract a real risk of interrogation and persecution at the airport. Her circumstances are made very much worse by her blogging and similar activities which would create difficulties in the event of her return. Without the need for further interrogation her scissoring activities might well be known to the authorities anyway. It is her case, consistent with her activities in Iran, that her *sur place* activities have been for genuine reasons but even if they are opportunistic and insincere they have created a risk and she is entitled to protection. She could not give a proper account of herself in the United Kingdom without attracting opprobrium and the risk of persecution. In short, the appeal should be allowed.

399. Notwithstanding the very thorough skeleton argument (which we have found helpful) Mr Hodson addressed us at some length. He outlined the argument that the Iranian authorities were the leading surveillance monitors of the world. Filtering, monitoring and checking were standard activities in Iran and Virtual Private Networks not entirely reliable alternatives. The appellant CD is “a classic blogger” and is engaged in many different kinds of internet activity and has the education and aptitude to make political or quasi-political comment. It is not surprising that much of the evidence about risk is conjecture but it should not be dismissed for that reason alone. Conjecture can be informed by established facts and expert opinion and that is the kind of evidence we received, he said. It was possible rather than fanciful to suggest that her activities had been intercepted and records of them added to her profile in Iran.
400. However, without in any way diminishing this point the fact is that she would be returned in a way that would attract attention. She would be a failed asylum seeker who had been in the United Kingdom for some time. That would be obvious and quickly established by questions and would of itself suggest she had been badmouthing the Iranian state.
401. The suggestion in the report “after the Green Movement” of Opennet Initiative in February 2013 that blogfa is no longer filtered is no indication that it will not be filtered on some future occasion. It was quite clear that it was possible that her activities in the United Kingdom had been intercepted.
402. It was trite law but worth remembering that people cannot be expected to lie their way through the airport in the event of return. She had been doing things that put her in the category of risk and she could expect to be interrogated. It was only a short step from there to say that she is in fact at risk.
403. He emphasised points made in the skeleton argument which we have outlined above. The Country of Origin Information Report dated September 2013 is helpful to the appellant. It summarises points already made, namely that the Iranian authorities are expanding their oppression of dissent and saw the World Wide Web as something from which people had to be protected. Surveillance, harassment and threats to internet users were described as “routine”. Much activity is forbidden and there is a low threshold of tolerance for criticism.

404. The report “Freedom on the Net Report 2012” referred to a crackdown on online activity and prison sentences against bloggers and examples given of sentences of fifteen years and nineteen years. He referred again to the ongoing battle between the state and the blogger as they each tried to outdo each other’s security devices. The report from Freedom House Freedom on the Net 2013 said how the internet service providers are required to record all the data exchange by their users for a period of up to six months. The report says that “it is not clear whether the security services have the technical ability to process all this data”. That, Mr Hodson submitted, meant what it said. It was not clear. It is possible that they do. Bloggers were frightened.
405. He then talked specifically about CD’s case. He submitted that she was a substantially truthful witness. There was internal consistency in her story and her writing and political views, particularly those supportive of women, were the kind of thing that would not be appreciated in Iran.
406. She had written things at a time when there was much optimism. The optimism was not being fulfilled. Now the situation is getting worse. The report “Radio Free Europe/Radio Liberty, ‘in Iran, beware of your Facebook friends’” dated 8 June 2011 explains how activities thought to be private on Facebook had come to the attention of authorities in various ways and circumstances. Put simply, there is a risk and he has proved his case.
407. We now turn to the submissions made by Mr Rawat for the Secretary of State. He too relied on a skeleton argument.
408. We have outlined the skeleton argument above and have considered it. There were agreed issues. These are set out very neatly in the skeleton argument and we have mentioned them above.
409. Mr Rawat then considered the list of issues that we have set out above.
410. He addressed the first two points (essentially, would the Iranian authorities know or care about his internet activities) together.
411. He made the point that Iran has the highest proportion of internet users in the Middle East. Its predominantly young population is educated and internet-literate. Somewhere between 26% and 47% of the population have access to the internet. If the latter figure is right there are 42,000,000 people in Iran who can use the internet.
412. The authorities have sought to control internet access by slowing the speed and raising prices and blocking and filtering websites. The official national system is easily bypassed and the state has not succeeded in diminishing internet use. People in Iran use circumvention tools, particularly Virtual Private Networks, to view websites and online material. They are relatively easy to obtain and set up on the black market and their use does not lead to serious punishment.
413. The Iranian authorities target users. The organisation Reporters Without Borders recorded 26 journalists and twenty “netizens” in prison in March 2013 and in October 2013 the United Nations Special Rapporteur reported 29 “bloggers” being currently in prison. Whilst this tends to confirm that some people are persecuted in Iran for expressing opinions that are offensive to the

state, the number detained is clearly a very small percentage of internet users and many of those targeted had a raised profile. For example, they are identified as working journalists or associated with reformist movements.

414. Although the authorities had closed websites their attitude is inconsistent. For example, although Facebook and Twitter are both blocked the supreme leader Khamenei is a member of Facebook and has a Twitter account. All six presidential elections for the 2013 election maintain a presence on both chat rooms. President Rouhani has a Facebook and a Twitter account as do other cabinet members. It really did not seem plausible that people would still be in trouble just for having Twitter or Facebook accounts.
415. Although the Iranian authorities have been determined to close things down the abundance of circumvention tools and internet users indicates it has not been successful and there is an open internet in Iran.
416. The evidence did not support the suggestion that all internet activity is monitored. Reporters Without Borders said in March 2012 (?) that “the regime does not yet have the resources for keeping millions of internet users under surveillance”. The authorities could use against people outside Iran the techniques for infiltrating and impersonating activities that they used against people inside Iran. To make sense of this it must be assumed that the amount of risk is related to the degree of interest that a party’s presence creates and none of the appellants here had done enough to attract attention.
417. In concerning issue 3 (additional factors) the Secretary of State accepted that many things might create a risk on return. The respondent contended that each case had to be looked at carefully on its own facts and that sur place activity *per se* would not raise the level of risk. This followed the lead given in BA (Demonstrators in Britain - risk on return) Iran CG [2011] UKUT 36 (IAC).
418. Understandably the skeleton argument particularly drew attention to the matters referred to above from IOM (International Organisation for Migration) Tehran and summarised in the joint report from the Danish Immigration Service, the Norwegian Landinfo and the Danish Refugee Council of 2013 showing that there was no evidence of anyone being arrested because they had been returned on a *laissez-passer*.
419. We look again at these reports now. We set out below in its entirety paragraph 6.1.2 of the joint report headed “entry for returnees” relied upon by the Secretary of State. The paragraph says:

“IOM, Tehran informed the delegation that the organisation is operating an assisted voluntary return (AVR) programme worldwide. Asked about the number of persons who have benefited from this programme, IOM informed that it is less than 100 per year. The majority of people who have returned to Iran under this programme from various countries including Switzerland, Norway, Belgium, Australia, Indonesia (people who were on the way to Australia) and the Netherlands are according to IOM, people who have been looking for a better life, studying opportunities and people who have family abroad.

Regarding returnees, IOM, Tehran, stated that Iranians who return with their passports will not face any problem at the airport when they return after a long

stay abroad. It was added that a long stay abroad in itself, is not an issue as long as a person has left the country legally. IOM added that Iranians who have left the country on their passports and are returned on a Laissez-passer will be questioned by the Immigration Police at the airport. This questioning may take a few hours, but according to IOM, nobody has been arrested when travelling back on a Laissez-passer.

When asked specifically as to the situation of deportation, IOM stressed that they are only dealing with voluntary return and had no knowledge of the situation of deportees if any. It was added that they would assume that such persons would be welcomed upon return, as these persons are nationals of Iran.

IOM stated that so far, they have not had any experience with people being arrested by the authorities at the airport. IOM added that if persons have been involved in criminal activities abroad and are on the Interpol list, it is another issue.

Mr Hossein Abdy, head of passport and visa department, stressed that the Iranian Constitution allows for Iranians to live where they wish. It is not a criminal offence in Iran for any Iranian to ask for asylum in another country. He further stated that approximately 60% of Iranians who have asylum in other countries, travel back and forth between Iran and other countries.”

420. We cannot understand how Mr Abdy can possibly know how many Iranians have asylum in other countries and therefore how that statistic can possibly be right.
421. The skeleton argument continued that following SB (risk on return-illegal exit) Iran CG [2009] UKAIT 00053 it was established that there is no general risk of persecution consequent on leaving Iran illegally.
422. There was no evidence that possessing a laptop or other equipment that could be used to access the internet did anything to increase any risk there might be.
423. Use of internet activity before leaving Iran could be a consideration but a great deal depended on exactly what had been done and whether it had been noted and how long had passed since it had been done and what attention it had attracted.
424. Whether a person who had been active on the internet would be identified and linked to his internet activities was very fact-dependent and something about which general pronouncements could not be made. There was no evidence to show that there was a general capacity or desire to link a returnee with social media.
425. Dealing with issue 6 (opportunistic activity) the skeleton argument recognised that opportunistic activity is not a bar to international protection.
426. Mr Rawat made oral submissions.
427. He particularly took us to the Freedom House report entitled Freedom on the Net 2013 Iran. This is set out in the respondent’s bundle and Mr Rawat made it clear that the Secretary of State accepted that the Iranian authorities are intent on controlling internet access. A similar point was made in the report from Reporters Without Borders.
428. We were looking at Freedom on the Net 2013 and Enemies of the Internet 2013. The Freedom on the Net report 2013, however, expresses doubt about the ability

of the Iranian state to process the vast quantity of information that it gathers. Although the Freedom on the Net 2013 report supports much of the appellants' evidence about the determination of the Iranian state to spy on the internet it raises clear doubts about the ability of the authorities to process the information they gather. Page 17 of the report (page 62 in the bundle) says expressly "it is not clear whether the security services have the technical ability to process all this data."

429. We are instinctively inclined to the view that this doubt must be very widespread or how else can it be understood that so many people in Iran use the internet. The report from Reporters Without Borders on freedom of information entitled "Enemies of the Internet 2013 Report Special Edition: Surveillance" again supports much of the other evidence we have received about the means and mechanisms available to control or spy on the internet. Its summary under the heading "Iran" is significant. It puts the number of internet users lower than the figures before us of 25,200,000. Nevertheless this represents an internet penetration rate of 32.8%. It records that there were 26 journalists in prison and twenty netizens and one netizen killed in the past year.
430. The report recognises that the internet "plays a key role in circulating news and information thanks to dissidents and independent news providers". It also observes that the "authorities often accuse social networks of being tools in the pay of western powers that are plotting against the government". The article also confirms other evidence about the unpredictable nature of the Iranian authorities. It notes examples of "pro-regime websites" being blocked and the outcry from government officials that followed the blocking of Google in Iran. We particularly note the phrase: "They subject the Iranian internet to an illogical and uncoordinated rollercoaster on the basis of often divergent political interests."
431. The report confirmed that in January 2013 the government announced new technology particularly targeted at Twitter and Facebook. There was doubt about the government's ability to achieve this target but this was not seen as an example of loosening control but of developing new ways of increasing it. The report confirmed that the government of Iran has deep packet inspection tools and the legislation was increasingly oppressive. The report gave detailed account of one Saeid Pourheydar who was described as a journalist arrested and ill-treated in 2010. The intelligence officers had transcripts of the telephone conversations and printouts of his emails and SMS messages. Nevertheless, the report concluded that Virtual Private Network technology which although unlawful was readily available in Iran and could be used to circumvent content blocking and censorship. The paragraph headed "Tips" advises:
- "The regime does not yet have the resources for keeping millions of internet users under surveillance. You should be able to fend off most threats if you adopt basic precautions such as regularly updating your operating system and software applications, using antivirus and VPN software, and systematically using the HTTPS Protocol whenever possible."
432. The report warned against the continuing use of websites such as Facebook, YouTube or Twitter which were blocked but suddenly became available. It was

suggested this will “often be because the authorities are trying to use the man in the middle to capture users’ names and passwords”. Nevertheless the report indicated that using VPNs eliminated that risk.

433. A very similar picture emerges from the document “after the Green Movement internet controls in Iran, 2009 – 2012” published by Opennet Initiative, February 2013. This recognises the tension between the desire of the Iranian authorities to control any desire of the citizens to express themselves freely. The writers were satisfied that dissidents and anti-regime activists outside Iran had been tracked and eventually persecuted by following the footprint of their social media activities. However, circumvention of filters by using proxies and Virtual Private Networks is commonplace.
434. We have found it instructive to consider the article “Iran’s ‘Cable Guys’ Provide Service Four Contraband Satellites – Al-Monitor: the Pulse”. This is concerned with the supply of satellite television receivers and is dated October 2013. It illustrates the extraordinary tension between the wishes of the Iranian authorities and the wishes of the Iranian people and shows how the people adapt to changes in the law. Satellite dishes are illegal items in Iran, yet somewhere between 50% and 70% of households in Tehran own one. Satellites have developed to make them easier to hide and they can be repositioned quickly to pick up signals from the best available satellite. The article explains how the “moral police” have abandoned the tactic of bursting into someone’s home because they are no longer let in. They have developed an alternative tactic of climbing of walls and entering by that means. The government clamps down from time to time and an example was given of hundreds of satellite dishes being confiscated and crushed but they are quickly replaced. The article explained that they were smuggled into Iran either by corruption at the land borders or underneath ships.
435. Mr Rawat particularly drew our attention to the report of the Special Rapporteur on the situation on human rights in the Islamic Republic of Iran dated 28 February 2013. There seemed little reason to doubt that people are persecuted in Iran. The article included at Appendix II a “list of currently imprisoned journalists in Iran”. We have counted 44 people in that list. Their plight sounded grim. There were people facing, for example, fourteen years’ imprisonment in Evin Prison for “insulting the supreme leader”. A prisoner was also to be lashed and faced ten years’ exile. Whilst an extreme example, there are many others on the list sentenced to terms of imprisonment measured probably in years rather than months and some of them to be lashed. The offences are of the rather vague kind that were identified and criticised in Ms Enayat’s report. No-one was suggesting that their plight should be trivialised or excused but it was suggested that 44 imprisoned journalists does not really support the implicit suggestion that anyone of Iran’s many millions of bloggers or low level occasional net activists really faces a real risk of persecution.
436. Mr Rawat submitted that the fact was plain that Iran did operate an internet system where many of its subscribers were able to contact the world news sources. The government was not able to exercise the control it wanted to exercise and a very large number of people were not frightened of the

government, at least in this regard. He further submitted that the fact that the Iranian authorities seek to infiltrate websites by impersonation or pretending to be a supportive subscriber is of itself proof that the monitoring facilities are not totally effective. If they were then there would be no need for such intrusion. He submitted that there was clear evidence of the extent of internet activity that could not be controlled by the government. He submitted it clearly could not be the case that all bloggers were at risk. It was difficult therefore to say how we could assess whether there was a risk for any particular blogger for activities in or outside Iran. He submitted it was relevant to decide if the blogger was original or passing on material.

437. Although recognising Ms Enayat disagreed on this point he submitted it was a way of deciding the degree of threat a particular blogger produced. He suggested that the persons identified as imprisoned in the report "Reporters Without Borders" of April 2012 looked like people with some prominence. Thus one person who was in prison was described as the author of the blog "Iran's land report". Another report as an example was of a lawyer who defended journalists and cyber dissidents. Another who was constantly harassed before being detained was described as a founder of the Centre for Human Rights. A blogger who was released on bail it was reported was described as a "satirical poet openly critical of the government".
438. There are many other examples given. Those who attracted attention, it was submitted, tended to look like leaders of movements albeit perhaps in some cases relatively modest ones. Persons who occasionally expressed critical views or passed on the critical views of others were not really at risk of imprisonment.
439. He then dealt with the suggestion that the person would be questioned on return. No doubt aware of the potential damage that Ms Enayat's evidence could do to his case, Mr Rawat submitted that Ms Enayat's examples of people who had had trouble on return was somewhat dated and did not necessarily indicate the present position. The L'OSAR report was dated 2011 and the Danish report was dated 2009. At paragraph 97 of Ms Enayat's report she referred to Appendix III where she claimed to have logged 29 known cases of returnee treatment since the year 2000. Appendix III is in fact headed "redocumentation procedures for Iranian nationals resident abroad".
440. Mr Rawat then made submissions concerning each appellant's case.
441. In the case of CD he said it was accepted that she had been employed by the broadcasting organisation but not that she had acquired a profile for being disloyal. It really made no sense that she would be perceived as disloyal but then employed in what might be thought a sensitive position. Her disloyalty did not go much beyond not observing Islamic prayers. The local Herasat were security guards with a mandate to snoop. Attracting their disapproval did not amount to very much. Her documentation did not really support her. When interviewed the appellant found it difficult to explain why she might be thought disloyal. Her political activities in Khatami's time were very limited but she assumed they were enough. She indicated in answers to questions around 28 of her interview that there may have been economic advantages to her employer in keeping her on a more casual basis.

442. Her blog had attracted seven entries. It had been shut down for a variety of reasons that had not been specified. Elsewhere she had 119 friends. She really did not have very much exposure. There was not much interest in her.
443. Dealing with the case of EF Mr Rawat said that his account of leaving Iran lacked credibility. He was in the same position as other people who did not apparently wish to leave Iran. He had about 137 followers or people may have seen his video. The interest in his blog is minimal. The Iranian National Council's website had attracted 16,000 individual supporters (Ms Khashefi at paragraph 121). Against this background EF's 137 was not impressive. The background material shows how Anonymous Iran had drawn over 22,000 supporters worldwide. This, he submitted, is the kind of activity that attracts the interest of the authorities.
444. In the case of AB adverse findings had already been made about him and upheld in the Court of Appeal. He has done little in the United Kingdom. He is not a prominent figure. He does not make original criticisms. He passes things on. His Facebook and YouTube identities have changed. He would not be at risk now.
445. Mr Haywood exercised his right to reply. He particularly challenged the suggestion that a person had to have a high profile before facing any risk on return. Although some people who had been in trouble clearly had a high profile there was no reason to assume that was true of everyone. By way of example, there is a report from the national campaign for human rights in Iran referring to the arrest in September 2012 of Kaveh Taheri who was charged with "acting against national security" and "creating public anxiety in the virtual space". He was said to have had no political activities whatsoever outside his blog where he expressed personal opinions. At page 1034 in the respondent's bundle there is a table entitled "removals and voluntary departures by the country of destination and type". There are figures given for Iran from 2004 until 2013 and the figures are given at quarterly intervals. In the last two quarters of 2012 and the first two quarters of 2013 there were 26 enforced removals. A further fifteen who were refused entry at port subsequently departed. There were (we think, the print is very small) 141 voluntary departures in the same period. Mr Haywood submitted these were small numbers and were not a sound basis for predicting exactly what would happen. We remind ourselves that the appellants only have to show a "real risk".
446. Ms Harrison chose not to address us.
447. Mr Hodson redirected us to the "Enemies of the Internet" and emphasised that although that report encouraged the use of Virtual Private Networks it also emphasised the suspicious and determined nature of the Iranian state and described as emphatic that people should not use the state-controlled VPNs. He repeated Mr Haywood's theme that there was no evidence that only high profile people were at risk. The appellant CD had her leave to remain cancelled and that would attract attention. The website was not secure and the aliases would have been rumbled.

Conclusions

448. We have considered carefully the material before us. Unusually for a case such as this there has been little challenge to the evidence. The experts gave honestly held opinions that were substantiated with reference to appropriate sources. Where they were challenged the challenge was nuanced rather than aggressive. Questions by the Secretary of State were intended to make us ask searchingly if the matters complained of established a real risk in this particular or any case rather than to suggest that the experts were inept or partisan. We do not think that they were either of these.
449. Certain things are quite clear and uncontroversial. Iran is a country that does persecute some people who oppose it. Persecution takes many forms. We have been given detailed examples of a small number of people sent to prison for a long period of time in conditions that must be very challenging.
450. However, persecution is not limited to imprisonment. We have been given more examples of people who are beaten up or lashed or harassed. The fact that there are only a relatively small number of journalists known to be in prison is not the particularly illuminating point that the Secretary of State tried to make it.
451. It is very difficult to establish any kind of clear picture about the risks consequent on blogging activities in Iran. It cannot be the case that a real risk or persecution is generated simply by making some unsavoury remark or mild criticism of the government of Iran. We make it clear that this is not because the government of Iran is tolerant of mild criticisms. There is evidence that it is not. However, we cannot argue with the numbers. People who are active on the internet run into millions in Iran and on the most conservative estimates represent a very substantial part of the population. Many of them, no doubt, are involved in activity that is entirely benign or even supportive of the government. Given the low levels of tolerance illustrated above we are quite satisfied that many of the people active on the web in Iran are critical. This is not necessarily overt. Mild concerns can be enough as can association with western music or western ideas or western fashions. All of these things attract disapproval and, we are satisfied, might attract persecution.
452. It is quite clear that the Cyber Army, however big it may be, is capable of perusing the internet and intercepting messages and closing down accounts. There is no reason to assume it goes on from there to persecute those involved. Given the scale of operations there would surely be evidence if those whose accounts were closed down were routinely caught, interrogated and ill-treated. That does not seem to happen routinely although there are no doubt occasions when it does. All of the witnesses who expressed a view described this tension between the Iranian authorities trying to supervise everything and the Iranian people, or parts of them, seeking to avoid being supervised. It is indeed a “cat and mouse” battle in which one side or the other at any particular time might gain the ascendancy.
453. We accept the evidence of people blogging outside Iran reporting that members of their families had, consequentially, been detained. This is a significant finding supported by skimpy evidence but we note that several examples were given to the reporters. We find it unlikely that they were all made up when the claim is intrinsically believable. We accept that some monitoring of activities outside Iran

is possible and that it occurs. We are not able to say what circumstances, if any, enhance or dilute that risk.

454. We were impressed by the evidence of Mr Esfaniari who was detained and then persecuted because of a careless remark made on his blog. By identifying a shop that had ill-treated him he set up a chain of circumstances that allowed him to be identified. This really can only have come about in one of two ways. The first is that he was just very unlucky, the second is that he was being monitored closely and the authorities had the time and inclination to study his reports and look for something that might reveal his identity. The fact that that happened in his case is not evidence that it happens in every case or that there is any real risk of it happening in every case. He was someone who had been annoying the authorities persistently and we can understand why they may have devoted resources to supervising him.
455. We do reject Mr Rawat's submission that a high degree of activity is necessary to attract persecution. It is probably the case that the more active persons are the more likely they are to be persecuted but the reverse just does not apply. We find that the authorities do not chase everyone who just might be an opponent but if that opponent comes to their attention for some reason then that person might be in quite serious trouble for conduct which to the ideas of western liberal society seems of little consequence.
456. The fact that people who do not seem to be of any interest to the authorities have no trouble on return is not really significant. Although Iran might be described as exceedingly touchy there is no reason to assume that the state persecutes everyone and the mere fact of being in the United Kingdom for a prolonged period does not lead to persecution. It may lead to scrutiny and this is what concerns us most. The fact is that although there may be quite a large number of people who choose to go to Iran their fate is of little value in determining what risk, if any, might be faced by a person who is not willing to return. Clearly an Iranian citizen is more likely than someone not familiar with the country to appreciate the risks that he or she really faces in the event of return. A person with no profile, with nothing to hide and whose biggest fault is to have overstayed in another country may well feel that he has done nothing to attract attention and will therefore go home. Such a person may well be right and will not produce statistics showing a risk of persecution.
457. We accept the evidence that some people who have expected no trouble have found trouble and that does concern us. We also accept the evidence that very few people seem to be returned unwillingly and this makes it very difficult to predict with any degree of confidence what fate, if any, awaits them. There is clear evidence that some people are asked about their internet activity and particularly for their Facebook password. We can think of no reason whatsoever to doubt this evidence. It is absolutely clear that blogging and activities on Facebook are very common amongst Iranian citizens and it is very clear that the Iranian authorities are exceedingly twitchy about them. We cannot see why a person who would attract the authorities sufficiently to be interrogated and asked to give account of his conduct outside of Iran would not be asked what he had done on the internet. Such a person could not be expected to lie, partly

because that is how the law is developed and partly because, as is illustrated in one of the examples given above, it is often quite easy to check up and expose such a person. We find that the act of returning someone creates a “pinch point” so that returnees are brought into direct contact with the authorities in Iran who have both the time and inclination to interrogate them. We think it likely that they will be asked about their internet activity and likely if they have any internet activity for that to be exposed and if it is less than flattering of the government to lead to a real risk of persecution.

458. We now direct ourselves particularly to the questions asked as the list of issues. Under (1) we say that social and other internet-based media is used widely through Iran by a very high percentage of the population and many of the people who use it are involved in blogging, uploading photographs and videos, using Facebook and some of them do things that are at least perceived as criticisms of the Iranian state. The Iranian state is very aware of the power of the internet and is very determined but not particularly successful in restraining it. We are quite satisfied that the Iranian authorities in their various guises both regulate and police the internet. There is no other explanation for the large number of reported examples of internet sites being closed down or marked by the Cyber Police or similar organisations. We do not see any direct link between such activity by the state or quasi-state officials and persecution.
459. It is not clear to us how the state officials are able to intercept blogs. Partly it must be the result of being a false friend, which must be some response to intelligence-led activity or guessing, partly maybe the result of filtering, which we accept can be extremely sophisticated. We were, however, impressed by the suggestion that the most revealing method is just carelessness or response to questioning.
460. The capability to monitor outside Iran is not very different from the capability to monitor inside Iran. Essentially the internet as the name implies is associated with the World Wide Web. We accept that there is some evidence, which we find persuasive rather than compelling, that some websites operating outside the United Kingdom have been intercepted and this again is most likely to be the result of the Iranian authorities being concerned. There is clearly some level of interest within Iran in the comments of people living outside Iran. We do not find this particularly revealing. We accept the evidence that a party of ten is sufficient to create an offence. There is no particular reason why a person outside or inside Iran involved in blog activity doing things such as that done by AB should attract a great deal of attention but search engines and browsing could find them and start to build a profile. The Iranian authorities clearly have the capacity to restrict access to social internet-based media. They do it in a variety of ways but all of them can be overcome, and this is where we get the “cat and mouse struggle” indicated above. Overall it is very difficult to make any sensible findings about anything that converts a technical possibility of something being discovered into a real risk of it being discovered. Under (3) we find that our main concern is the pinch point of return. A person who is returning to Iran after a reasonably short period of time on an ordinary passport having left Iran illegally would almost certainly not attract any particular attention at all. However, very few people who come before the Tribunal are in

such a category. At the very least people who would be before the Tribunal can expect to have had their ordinary leave to be in the United Kingdom to have lapsed and may well be travelling on a special passport. Nevertheless for the small number of people who would be returning on an ordinary passport having left lawfully we do not think that there would be any risk to them at all.

461. We do accept that a person who is interrogated would have enquiries made and the more active they had been the more likely the authorities would become interested and pursue their investigations. We have no hesitation in saying CD is in such a category. She is a woman who has in the minds of the authorities been a nuisance for a long time and this would come to light in enquiries on her return.

462. As to question (4) we are again in an area of uncertainty. A person who has been extremely discreet and careful may well not be linked. The difficulty is that it is easy to be indiscreet and very difficult to stand up to the interrogation of the kind that we think is very likely to happen in the event of return. The mere fact that a person blogged in the United Kingdom would not mean they would necessarily come to the attention of the authorities in Iran. They may well have been discreet and successful in being discreet but only if everything had worked for them.

463. In answer to question (5) we are again to some extent speculating but it is clear to us that the more active a person had been on the internet the more enquiries that were we to make the more likely of that person getting into trouble.

464. We do not find it at all relevant if a person had used the internet in an opportunistic way. We are aware of examples in some countries where there is clear evidence that the authorities are scornful of people who try to create a claim by being rude overseas. There is no evidence remotely similar to that in this case. The touchiness of the Iranian authorities does not seem to be in the least concerned with the motives of the person making a claim but if it is interested it makes the situation worse, not better because seeking asylum is being rude about the government of Iran and whilst that may not of itself be sufficient to lead to persecution it is a point in that direction.

465. It follows therefore that we allow all of these appeals.

In summary

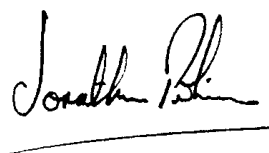
466. It is very difficult to establish any kind of clear picture about the risks consequent on blogging activities in Iran. Very few people seem to be returned unwillingly and this makes it very difficult to predict with any degree of confidence what fate, if any, awaits them. Some monitoring of activities outside Iran is possible and it occurs. It is not possible to determine what circumstances, if any, enhance or dilute the risk although a high degree of activity is not necessary to attract persecution.

467. The mere fact of being in the United Kingdom for a prolonged period does not lead to persecution. However it may lead to scrutiny and there is clear evidence that some people are asked about their internet activity and particularly for their Facebook password. The act of returning someone creates a “pinch point” so that

a person is brought into direct contact with the authorities in Iran who have both the time and inclination to interrogate them. We think it likely that they will be asked about their internet activity and likely if they have any internet activity for that to be exposed and if it is less than flattering of the government to lead to at the very least a real risk of persecution.

468. Social and other internet-based media is used widely through Iran by a very high percentage of the population and activities such as blogging may be perceived as criticisms of the state which is very aware of the power of the internet. The Iranian authorities in their various guises both regulate and police the internet, closing down or marking internet sites although this does not appear to be linked directly to persecution.
469. The capability to monitor outside Iran is not very different from the capability to monitor inside Iran. The Iranian authorities clearly have the capacity to restrict access to social internet-based media. Overall it is very difficult to make any sensible findings about anything that converts a technical possibility of something being discovered into a real risk of it being discovered.
470. The main concern is the pinch point of return. A person who was returning to Iran after a reasonably short period of time on an ordinary passport having left Iran illegally would almost certainly not attract any particular attention at all and for the small number of people who would be returning on an ordinary passport having left lawfully we do not think that there would be any risk to them at all.
471. However, as might more frequently be the case, where a person's leave to remain had lapsed and who might be travelling on a special passport, there would be enhanced interest. The more active they had been the more likely the authorities' interest could lead to persecution.
472. The mere fact that a person, if extremely discrete, blogged in the United Kingdom would not mean they would necessarily come to the attention of the authorities in Iran. However, if there was a lapse of discretion they could face hostile interrogation on return which might expose them to risk. The more active a person had been on the internet the greater the risk. It is not relevant if a person had used the internet in an opportunistic way. The authorities are not concerned with a person's motivation. However in cases in which they have taken an interest claiming asylum is viewed negatively. This may not of itself be sufficient to lead to persecution but it may enhance the risk.

Signed
Jonathan Perkins
Judge of the Upper Tribunal



Dated 19 March 2015
Re-Dated 29 April 2015

APPENDIX 1

EVIDENCE OF CD

1. The appellant CD gave evidence before us. She made statements dated 15 March 2011, 3 May 2011, 16 June 2011, 29 March 2012 and 7 January 2014. Subject to unremarkable but necessary corrections which we have noted the appellant adopted these statements as part of her evidence. We consider them now.
2. In her first statement she outlined her personal circumstances. These are not contentious and not everything she raised is relevant but we refer to some of the peripheral points because they set the appeal in its context.
3. The appellant CD was born in small town in the Isfahan area of Iran and was one of five children. She has brothers and sisters and nephews and nieces in Iran. She was successful at school and was commended in High School for having the best grades in her term. She studied political science at Isfahan University and like many students of her generation was politically aware and she was active in the May 1997 presidential elections that brought Mahammad Khatami to power.
4. She graduated with a first class degree in political science and got work at the Ministry of Education teaching history but the Ministry of Education expelled her for two reasons. She started questioning and objecting to the content of books because they were unreal and untruthful and she was not engaged in promoting and encouraging students to practise the Islam.
5. In 2000 she started to work as a political researcher on Iranian Television which she explained “operates directly under the government authorities”.
6. She said she gained a reputation as a “very good” political analyst.
7. She began to publish articles in political journals including the [journal redacted] published by the Iranian Revolutionary Guards. Then she became a member of a research committee for the Middle East in the Foreign Ministry.
8. She was trying to make her employment at the State Television as permanent rather than temporary arrangement but Herasat blocked her appointment because she was not regarded as being sufficiently loyal.
9. Eventually she was recruited as a translator for news in 2007 but was warned to mind her behaviour.
10. In the presidential elections in 2009 she campaigned in favour of the Green movement. She hoped that Mir Hussein Mousavi would bring about fundamental change in Iran and she planned to continue her studies hoping to obtain a doctorate in a United Kingdom university.
11. She sought to improve her command of the English language and obtained a visa to enter the United Kingdom as a student to attend language college.
12. The terms of her employment permitted her paid study leave and she was rather reluctantly given six months’ paid leave of absence.
13. On 19 September 2010 she arrived in the United Kingdom but after a few weeks her family was contacted by her employers objecting to her departure and requesting her to return to Iran to appear at a hearing.

14. In anticipation of making plans to return to work for the television station by contacted an executive by email. She then was approached by a colleague from the Information Ministry who said that her file had been opened. This contained information in writing about Iran's intention to enrol in nuclear programmes in the Middle East. Enquiries were made about her political activities and religious beliefs and reasons for leaving Iran. She understood that the people who were enquiring her were the same branch of the security services that imprisoned and tortured people. She regarded them as "highly ruthless and unethical" and she was frightened of them because of their reputation for causing people to disappear without trace. The same people then questioned her former roommate and visited her family home and encouraged her family to encourage her return.
15. After two months her former employers stopped paying her salary although payment had been approved for six months. This left her very apprehensive about returning.
16. She took part in demonstrations in front of the Iranian Embassy. She believed that the government of Iran would fall and demonstrations of the kind that she attended might help bring about that end.
17. The demonstrations were filmed and she became very anxious about her circumstances.
18. She had heard that a student whom she identified as Ehsan Abdoh who had taken part in such demonstrations returned to Iran and was soon sentenced to seven years' imprisonment.
19. Additionally she wrote some papers on Middle East revolutions and the Iranian Green movement for a Persian website. She described the regime as "very angry about this kind of online activities".
20. In her statement of 15 March 2011 she commented on the Reasons for Refusal Letter of 25 March 2011.
21. CD gave more details of how she came to secure a permanent job with the Iranian State Television notwithstanding that she had been sacked as a teacher because she refused to promote Islam. She said that the pay was low and that persons employed on a temporary contract are not subject to as much scrutiny as a person on a permanent contract. Her history stopped her getting a full-time job.
22. She obtained a permanent position as a translator of the news from English to Farsi in 2007. Sensitive material was only distributed to managers. It was not published generally.
23. She sought to support her claim with reference to various contractual or similar documents and also a copy of the [journal redacted] where she was identified as an author and her position at the IRIB (Iranian Broadcasting) noted.
24. She brought that particular publication with her because the articles she had written caused a stir in Iran and she wanted to try and publish it in a British magazine.

25. She also submitted copies of her payslips that she had obtained from the IRIB website under her personal portal and explained that although she only had continuous employment from 2003 to 2007 she had moved from successive contracts from 2000 to 2003. However, they did not give her pension or other entitlements.
26. She understood that it was suggested that if she would be monitored by Herasat as she alleged she could not have published articles as she claimed to have done. She said that the articles were published before 2007 when she was working as a political researcher and her managers were open-minded to some extent. Researchers had to show loyalty to the supreme leader but were otherwise allowed some licence to express their views, particularly in election time. Even so she showed some restraint and tact. It was only after she arrived in the United Kingdom that it was clear that Herasat were concerned about her.
27. She said that it was rather missing the point to criticise her for saying that her salary was stopped after two months although Herasat were interested in her. A better way of putting it is that Herasat became interested in her and two months later her salary stopped. That was the time it took for the interest of Herasat to crank its way through the IRIB bureaucracy.
28. She explained at paragraph 35 of that statement that her blog had been shut down because she would be identified as someone who supported Mousavi in the election.
29. She had posted on her blog after coming to the United Kingdom. She had also created a new blog under the nickname "Mahtab". She had posted a link to that blog on www.balatarin.com which is a website for Iranian activists. She had written articles that had been published on www.iranfree.org.
30. She had tried to get work at the BBC and Manoto Cable TV in the United Kingdom.
31. In her statement of 16 June 2011 she explained how on 31 May 2011 a former colleague had contacted her to tell her that IRIB had decided to dismiss her. She asked her friend to obtain a copy. When a copy was not forthcoming she contacted another colleague who explained that IRIB would only release the document to the appellant or a lawyer. Her lawyer lived 400 kilometres away.
32. On 2 June 2011 she contacted IRIB and was told that there was no right of appeal against the decision. Herasat had pushed the IRIB into making it and it was not to be changed.
33. She made a statement on 29 March 2012. There she explained that in August 2011 a former colleague had contacted her to say that she had heard that the appellant's name had been published in a newspaper as someone who had been dismissed from IRIB. It was published in the state newspaper Jam-e-Jam. It was a message to ensure she would not be employed again.
34. The appellant had tried to find an electronic copy of the edition and her friend had tried to find a paper copy but they had both failed.
35. She explained that she had borrowed money from her employer. The money was collected every month from her wages. Since she had been sacked her colleagues

who had guaranteed the loan had had money taken from her account. Her colleague had asked the appellant to provide the money which was owed. She had to find about £1,700. She had paid the loan by transferring money from her own account to a friend's account and the friend had transferred it into the guarantor's account. She still owed money and was coming to an arrangement with the bank.

36. She talked about the voluntary work she was doing in the United Kingdom and her continuing to write online and had written on topics including the attack on the United Kingdom Embassy in Iran by government loyalists, the civil war in Syria and criticism of Iranian policies of oppressing people. She had also posted links on Facebook about never forgetting the young people at the election protests of 2009 and criticising Islam for suppressing women.
37. She had written a book about her experiences as a journalist in Iran and is an asylum seeker in the United Kingdom. She said it was not an autobiography but based on her experiences and she intended to publish it in Manchester.
38. She had not been involved in any street protests against the Iranian regime since moving to Manchester. She could not afford to travel to London.
39. Her most recent statement was dated 7 January 2014.
40. She gave more details on her family circumstances.
41. As she had stated previously her parents divorced when she was young. She is now in contact with her mother and her father. Typically she spoke to her father by telephone every month and her mother every week. Sometimes she is able to use Yahoo Messenger to contact her mother. Her mother goes to a member of the family who has a computer. She speaks sometimes to her brothers and sisters and to her half-sisters, to her sister R about twice a week and her sister N about every two or three weeks.
42. The Iranian authorities had contacted her father about her.
43. She identified close friends in Iran. One she had lived with as a student and the other was a colleague at IRIB but was now a teacher in Northern Iran. She listed other friends she contacted sometimes by Facebook, Viber, Oovoo, SMS, and Messenger or ordinary email.
44. She had been prompted to claim asylum. One of the events that had led to that decision was her blog being blocked in February 2011. Blogs were posted under the name "E M" (this represents the name actually given in evidence). She had copies of the blogs on her desktop computer at her home in Tehran. She continued to post blogs after she arrived in the United Kingdom. She had written about the problems Iranians faced overseas and the Green movement and the protests against the election President Ahmadinejad and in praise of the courageous role of women in the movement. In December 2010 she posted an extract from a speech by Mir Mousavi and she has made copies of her blogs.
45. She said that the blogs she had posted when she was in Iran were not as bold as those when she was in the United Kingdom.

46. She speculated that her blogs were closed in February 2011 because she had posted three blogs in the United Kingdom and was openly critical of the regime. She accepted that it was true that a lot of blogs were closed at about that time.
47. She confirmed that after coming to the United Kingdom she had written two articles that were posted on the internet. One was a commentary on the Tunis revolution which was written at the request of a former colleague then based in Switzerland who ran a website called iranfree.org. Another one was on the power of Facebook as a means of assisting protesters. Her name was on the articles. It was a week or so after the article was posted on the internet that her blog was blocked on blogfa. She repeated that she was known as a political analyst in Iran but the criticisms she had made there were milder than those from outside the United Kingdom.
48. She said that it did not deter her from writing blogs when her blog on blogfa was blocked. Rather she went to blogdoon.com which she described as another Iranian Persian language domain for blogs. She identified her blogs. One of them translated as [redacted] and was intended as a pun on the cutting action of the censor.
49. Her first blog on that post was entitled “Farewell To Religion Is The Start Of Living Freely”. She was “generally critical of the whole idea of an Islamic state.”
50. Since then her blogs had become more critical. She had blogged under an assumed woman’s name and started using one of her own names but not her whole name. She said it was a very common name. She did not know if this would work as a security measure but it seems a sensible precaution.
51. She said she had also posted matters on her Facebook page. She had a following of 120 Facebook friends. Some she knew well, some she did not know at all outside Facebook.
52. She identified her Facebook page, which she said was in her full name.
53. She insisted she had been active in the United Kingdom in other ways, typically attending demonstrations. She had photographs. She said the First-tier Tribunal Judge had misunderstood the evidence she gave about the dates.
54. She had been asked to talk to the Seventh National Black Nation Writers Conference and Festival because it was known that she was writing a book. She felt particularly well-qualified to talk about the way the government of Iran repressed and intimidated freedom of speech.
55. She had taken “full advantage of my blog to communicate my thoughts, reactions and feelings on a whole range of topics” after coming to the United Kingdom.
56. She believed that if she returned to Iran she would be stopped at the airport and asked to provide her Facebook and email details including passwords. She believed there was a real risk of the Iranian authorities knowing about her blog, particularly because of her use of Messenger to communicate with friends and family. She did have a profile as a political analyst. She was afraid of being interrogated in Iran. She also believed she would risk being arrested, detained and charged with serious crimes.

57. The appellant said that she had a profile in Iran. This was a result of her working as a political analyst and working for the Iranian national media. Her loyalty had been questioned and she was confident that this would be noted especially as she was dismissed following investigations by Herasat. She described Herasat as a branch of the Iranian security system. The further her absence from Iran over a period of three years would attract questions. She would be questioned about what she had done in the United Kingdom and this was likely to lead to the truth emerging of her writing and blogging.
58. It was her belief that she would be arrested, detained and charged with serious crimes and she would be subject to severe ill-treatment whilst detained and could not expect a fair trial. She said at the very least she would receive a disproportionate prison sentence. She was asked about blogfa. She said this was a blogging service which was blocked or stopped by the authorities. She did not know who had blocked it.
59. She denied violating any laws and agreements or publishing any immoral content.
60. Her attention was particularly drawn to an article in the bundle at page 133 and an English translation at 132. These are short blogs written on 7 December 2010 and 10 November 2010. The November article includes praise for people who protested outside Parliament in support of women, socialists and green reporters. She expressed her respect for the “bravery of these green movement women”.
61. The December article reflected on the election that would determine Iran’s future. She expressed the view that “we” did not want a superstitious government, a charity based government, a genius who had made sole decisions for the country. She was also careful to say that “we” respected the revolutionary guard. Both of these articles bore the name CD and then a further name that could not be deciphered. She was then referred to the notice page 418 in the bundle in translation that the blog had been stopped. It was dated 14 February 2011 and she said that was when she discovered the blog had been blocked. 14 February was significant because it was the day of a demonstration in front of the embassy. She confirmed she had attended various demonstrations although could not remember all of the occasions and had attended the Embassy demonstration on 14 February. She said that she had been inspired to write by an article in the website “Iranfree.org” which had commented on the Egyptian revolution. There was a similar article about the Tunisian revolution. The English translation at pages 150 to 152 of the log beginning at page 153 began by saying how the overthrow of the Hosni Mubarak dictatorship in Egypt had “offered hope to the people in Middle East as well as Africa and Arabic countries and particularly Iranians”. The concluding passage of the blog suggested that if demonstrations were widespread the government of Iran would have less opportunity of suppressing it. The statement was supported by pictures that appear to show her demonstrating outside the Iranian Embassy in Kensington. She said there was also an entry showing her at the demonstration.
62. For completeness she also produced her Iranian broadcasting corporation identity card which identified her as a translator.

63. She was cross-examined.
64. She confirmed that it was usual in Iran to finish high school at the age of 18 and then go on to university if the necessary exams were passed.
65. She confirmed that she was sacked from her job in the year 2000. She appealed the decision and confirmed that her appeal was unsuccessful because she questioned texts and refused to promote Islam.
66. She said Herasat were at the university that she attended. Herasat were also at the Ministry of Education.
67. She said that when she was applying for work with the Iranian Television IRIB the authorities did not go to Herasat but to another division called Gozinesh. Nevertheless she accepted that she had said because she understood it to be the case that a report would be given to Herasat. She said that her reputation of a disloyalty was not so good in the way of getting a permanent contract. She did eventually get a job as a translator because she satisfied them that she was loyal. She explained the job as an interpreter was much less sensitive than the job as a political researcher.
68. She understood the suggestion that it was strange that a person was able to get work for seven years if they were suspected of being disloyal but she insisted this was because she was working in the less sensitive work as a translator rather than the more sensitive work of political researcher. She pointed out that the American attack on Iraq had created a big demand for researchers and there were “thousands of people” working because extras were needed. She pointed out that she did suppress her disloyalty at work and nothing could be proved against her. She was reminded that in interview she had said she was never given a reason why she was not recruited earlier than she was. She said that “they were just talking generally saying that you are not fully loyal to leadership and Islam”. She regarded this as a fairly customary allegation. She was asked to comment on page 155 in translation of a review paper. It was dated January 2006 under the name CD who was then described as a “researcher”. The paper was a summary of an article written in 2006 for publication by the Iranian Revolutionary Guard. She was asked why the guard would let someone who was disloyal write for them. She said that the research she did was separate from her workplace and was submitted to the authorities before being printed.
69. She accepted that she had sat on a research committee for a few years. She was asked to explain again why this was permitted if she was not safe. She pointed out that the main accusations against her came in 2005. She was asked if it is her case that she was not a figure of suspicion at all between 2000 and 2005. She said that she was not allowed to work for them for the two years between 2005 and 2007 when they made a decision. She confirmed she had not had problems between 2000 and 2005. She enjoyed her work and did not particularly want to be a full-time employee.
70. Between 2000 and 2007 she did want a permanent job with Iranian Television. She said many reasons were offered for her lack of success. For example on one occasion she was thought not to be compliant with the dress code requiring her to cover her hair and wear a Hajib. She explained at her interview that the main

problem she faced was they did not want to recruit her officially or give her a permanent contract. They wanted to use her skills but not give her all the benefits and rights of a full-time employee.

71. She accepted that generally they preferred temporary staff.
72. She insisted it took her about two years to improve her loyalty.
73. She was asked about her visit to the United Kingdom. She had said in her statement (paragraph 12, page 24) that government employees were entitled to three years' paid leave and three years unpaid leave. Once she became an assistant she was granted six months' paid leave of absence. This was supported by her managers.
74. She had no direct contact with Herasat although Herasat signed her identity documents. She said it was not usual to ask Herasat for permission.
75. She was reminded that in answer to question 45 at interview she said that the problems in Iran that prompted her to seek asylum started a few weeks after she had arrived in the United Kingdom. She said Herasat were enquiring about her. Her managers knew she might want to be away for more than six months. She said that the emails at page 277 in the bundle dated 17 December 2010 and 20 December 2010 came from a private email address of a colleague who worked for Iranian Television. She did not know why the person had used Yahoo.
76. She was reminded she had said earlier that IRIB did not have the facility for sending emails and she confirmed that that was right. However it was pointed out to her that there was a contact page for Iranian Television website printed in January 2014 that did show an email address for Iranian Television. She said every channel had an official email contact but there were not email facilities for all 50,000 members of staff.
77. She was asked to comment on the criticism at page 277 in the email that she had not obtained the necessary permission from Herasat before leaving. She said she was not aware of the rule at the time. She believed the rule was enforced after she had left the office. She confirmed that when her friend Mrs Khodabandeh had contacted her she had intended to return to Iran. She said that Mrs Khodabandeh would solve the problem and she did not talk to anyone else. She did not ask Mrs Khodabandeh to speak to the manager. She said things did not work like that in Iran.
78. She was then asked about leaving her PhD proposal in a private cabinet. She was asked why she had left an incriminating document in a cabinet, albeit a private one, when she believed that her superior blocked her and made it hard for her to get a permanent contract. She was asked why if that was the case she left an incriminating PhD proposal where it could be found when she was away from work for six months. She said that it was in a locked private cabinet.
79. She confirmed that she had not got into trouble because she had expressed approved for the Green Movement at work. She also confirmed that many people had demonstrated against the Iranian Government. She also confirmed that it was her case that thousands of people blogged in Iran. She also confirmed she had attended demonstrations after coming to the United Kingdom. College

students had told her about the demonstrations. She was particularly interested in blogdome.com. She believed it was popular in Iran but there was no particular reason for using that site. She also confirmed that she had used the name [redacted] on her blog for a time. She was asked more questions about the selection of her Facebook entries. She confirmed she had had a “beautiful poster of [redacted] under beloved child” work of graphic designer in Holland. That person was a lawyer who had been put in prison. Her blog of 27 September 2013 reflected that although more than 50 people had been executed in the last month [redacted] had been unconditionally released.

80. The appellant said she had started using Facebook after she came to the United Kingdom. She had used it to communicate with friends and more distant family members in Iran.
81. She confirmed that she had never been arrested and was not aware of there being a warrant for her arrest, that she had been sacked from her employment. Her employer made no attempt to try and contact her although they had contacted her father. That was on one occasion in 2010. It was suggested to her that in March 2011 she wanted to stay in the United Kingdom to complete her education. She had contacted Leeds University and they had offered her a partial scholarship but that was not enough to support her. She replied that she did not have any choice.
82. She was not re-examined.

APPENDIX 2

EVIDENCE OF EF

1. The appellant EF gave evidence before us. He had made a statement dated 15 December 2011.
2. There he said that he was born in Iran in Firoozabad in the province of Fars in 1972 and had lived there all his life.
3. He said that he followed the “Zarodastian” religion that he described as the ancient Persian religion. Many Iranian nationals had left Iran for India to follow their religion peacefully.
4. He said his mother and father were both Muslims and followed Islam but he did not believe in Islam. Islam was a disunited religion and did not respect human rights. He was particularly unattracted by Iranian “Islamic” punishments.
5. He was an unmarried man who lived mainly on his own but sometimes with his parents in or around Firoozabad.
6. He said he was educated in Iran to university level where he studied agricultural engineering. He had worked on his father’s land and sold crops to make his living.
7. He had helped establish a group called [name redacted] with the help of four friends who he named. They intended to gather all the people who were “fed up of the current Iranian Islamic regime”. One of their objections to the Islamic regime was that it brooked no opposition.
8. They set up a group on Facebook intending to gather enough people to defy the government. He said the group was formed about two years before making the statement in December 2011 with the assistance of the friends he had identified. They encouraged other people to join the group and had small meetings. People who wanted to join they would make enquiries to satisfy themselves that they were genuine and in tune with their thinking.
9. They also went on to, for example, Yahoo chat rooms to communicate with others who wanted change. There were about 2,200 followers since the group was formed.
10. His Facebook activity consisted of posting articles and opinions for others to see.
11. Since coming to the United Kingdom he had set up a co-ordinated group with others and had about 1,500 followers. He could act more freely in the United Kingdom and expand the work of the group.
12. He said his problems began in Iran on 19 Tir 1390 when his friend BD (one of those who helped him establish the group [name redacted]) was arrested. A mutual friend not involved in [name redacted] had seen BD arrested and contacted the appellant to tell him that plainclothes officers had taken BD away and had also taken his car.
13. After that the appellant spoke with BD2, another of the founding members of the [name redacted] and decided it would be best if the appellant left Iran. BD was still in detention.

14. BD2 introduced him to one Hassan Kurd who eventually smuggled him out of Iran in a car for a fee of US\$1,500.
15. He was smuggled over the border into Turkey and eventually to a hotel in Istanbul.
16. He had a telephone conversation with one of his cousins, a medical practitioner with a surgery near to his home. His cousin told him how the authorities had been to the appellant's house and confiscated his computer and paperwork but he had no news about BD.
17. The appellant had saved banned books on his computer including two particular banned books whose possession attracted heavy punishment. He thought it would cost him his life.
18. He was scared to return to Iran.
19. He did not believe Turkey was a safe place for Iranians because of the close relationship between the governments. There are Iranian agents within the Turkish state. He did not think it safe to remain there and he found an agent to get him out of Turkey for US\$12,000.
20. He had been in Turkey for about 45 to 50 days and went out by lorry. He explained that there were several stages in the lorry journey but people in travel were not allowed to talk or ask questions. He was discovered by border agents in a lorry at Dover. He claimed asylum on arrival.
21. He believed that in the event of his return to Iran he would be taken to court and sentenced for opposing the regime and that he would be killed. His opposition was not just to the Islamic regime but was seen as being "against God" and therefore would attract severe punishment.
22. His asylum claim was unsuccessful and he made a written response to the refusal letter. The response was dated 15 December 2011.
23. He insisted that he had stated that he did not feel fit to be interviewed when the screening interview took place. He had been travelling for over 48 hours in the lorry and wanted a solicitor. He was told he was not entitled to a solicitor and discovered later that they had not acknowledged in the records his complaint that he was not fit to be interviewed.
24. He denied there was anything suspicious about his not being able to say he made his computer. He said that in Iran it was customary to buy the computer in parts from specialist manufacturers and assemble the computer by the final customer. It was possible to buy complete computers in Iran but cheaper to buy and assemble the parts which might be older products.
25. He said he could not have been visiting his uncle as suspected by the Secretary of State because his uncle had died in 1982 in Iran. He was visiting his cousin. He had been arrested for drinking alcohol. That was more than twenty years ago and he could not remember the name of the sentencing judge. He had not mentioned it at screening interview because he thought he was being asked about political activities. He could not recall the date of an arrest nineteen years ago. Again he explained that he was tired at his screening interview.

26. He speculated he had a medical condition making it hard to remember precise dates but he insisted that he had set up his opposition group about two years before making the statement.
27. He said there were 1,500 members on Facebook when he made that claim but there were now 2,190. The information was there by checking.
28. He repeated that he did not know the maker of his computer because his computer was not made by a particular supplier but assembled from parts. He did use the computer every day.
29. He explained that filter codes were available from Voice of America and Radio Farda. The American International Press encourages people to use codes to get around filters. The required information is readily available. He said he could not remember the day of the week when BD was arrested. He was told that they were dressed in plain clothes and that is how he believed the Ettela'at behaved. BD was at the water company office applying for permission for a framing project.
30. He confirmed that he was in Turkey, not Iran when his house was raided. He did not know if there was an arrest warrant. He was only trying to make sense of what he had been told.
31. He had made an updated statement which is not actually dated in our copy but according to the chronology was made on 4 December 2013.
32. There he explained that he was born a Muslim but was not a practising Muslim. He had stopped practising Islam about 25 years earlier. He was not a Zoroastrian but he followed its philosophy of "think well, speak well and do well".
33. He explained that he was from the Qashqai tribe or group. His family was well-known in the southwest of Iran and his paternal grandfather had been a famous [redacted] or tribal leader. He spoke Farsi at school but Turkish Qashqai at home.
34. The family had problems since the start of the Islamic revolution. In about June 1981 there was a skirmish between Sepah Pastaran and Qashqai leaders. The Qashqai had a military base where about 500 men were stationed. The Central Government wanted to close it. There was a three day war and his uncle, [redacted], was killed. After the war the remaining Qashqai soldiers were arrested and imprisoned. Four or five people were executed by firing squad and the others were forcibly displaced and removed to other areas of Iran. They were banned from returning to Fars province.
35. His father had been one of the 500 soldiers fighting at the Qashqai military base. He was imprisoned because he had arranged the funeral of the appellant's uncle, [redacted] who had died in a combat. He was imprisoned for nearly a year.
36. His family had been members of the "elite" and suffered in the revolution as a consequence. Most of the land they owned was confiscated leaving them only a small amount of land to farm. The family said that they were victims of constant discrimination. For example, although the appellant had a degree in agricultural engineering he could not get a decent job in Iran and he attributed that to discrimination because his family were actively involved in opposition politics.

37. He explained how Facebook was not permitted in Iran but various organisations including the BBC, Voice of America and Radio Farda would email links on how to access the internet.
38. In late 2009 or early 2010 he set up a website called [WEBSITE]. He said there were “absolutely no privacy settings on that account” so anyone who accessed it could access all on the site.
39. This gave easy access to his date of birth and mobile telephone numbers, his United Kingdom address and his screen names for use with Yahoo Messenger and Skype. An email is given as well. This information was on his “about” page where there is also a link to a website of which he was the General Secretary.
40. He established [WEBSITE] in late 2009 or early 2010 while in Iran using it to criticise the regime. He would ask for his own thoughts and others with a similar political opinion and he would also publish news or other information that he thought would his readers. He said he presently had 4,051 friends. He usually checked the Facebook account of someone who made a “friend request” to ascertain that they were consistently of the same political view.
41. His “friends” links included a link to opposition political figures and journalists and also a famous Iranian feminist “Azar Majedi”.
42. He published and shared political articles via his [WEBSITE] Facebook page.
43. On that site there was a column showing links in Farsi to an earlier Facebook page for which he was responsible. This was begun in 2010 with four friends and he knew the page had been hacked. They were Islamic agents who had attacked many other accounts. He said that when he or his colleagues uploaded articles against the Islamic regime which they had written they found them on the internet in a distorted form.
44. He said there were originally seven administrators, that they lost control. The account was hacked because there was a message in the “about” section saying “God is great” and linking to soldiers of Islam. After that page was hacked the original management lost all control and could no longer use the page.
45. The next link on the favourites page is to a group he established and which attracted 1,636 friends. It had no privacy settings and he was one of the administrators of the website. He said the site worked as a newspaper and the place for exchanging ideas. It showed him using the earlier pre-Islamic Government flag of Iran.
46. After the group [group name redacted] was hacked we established a new group with a slightly different name called [group name redacted] which is a closed group so that each member can enter information. The appellant was one of four administrators of that group which at the time of writing had 5,184 members.
47. He also ran a website known as the [website name redacted] which was established with 26 other people from different groups and organisations and the group had been hosted by another website but they had lost control of that site. The purpose was to establish a national Council and this was done at a meeting in Paris in early 2012.

48. Prior to the establishment of the national Council there was a meeting for all of the groups conducted by Skype in which the appellant participated. The establishment of the [group name redacted] was broadcast in Iran by the satellite channel, Andishe. After the Skype meeting a new website was established by the original committee and placed before the elections in Paris. The details of the appellant's group and name and personal details were on that website in Farsi and English. Notwithstanding his role in founding the group the appellant's delegate was not permitted entry to Paris (? paragraph 25 witness statement meaning a little obscure) and there was dissatisfaction with the way things had been addressed on the national committee so the appellant opted out and the story about that was broadcast in several opposition newspapers.
49. The appellant also used YouTube as a means of broadcasting his political activities. He had uploaded twelve of his own videos onto that site.
50. On 12 August 2013 a regional newspaper, the Evening Gazette, published a report about his United Kingdom activities and the names of the spokespeople for the Iranian People's Freedom Front where one of the names was misspelt.
51. The appellant was twice interviewed with [company redacted] which is accessible via his YouTube account. The first interview was in 2011, the second in 2012. He had heard about [company redacted] when he was co-operating with another organisation based in Sweden. In his first interview with [company redacted] he discussed political activities and what he did with regard to [WEBSITE]. The second interview was about bringing different opposition groups together through Facebook.
52. The appellant had a YouTube account with a video about the announcement which is discussed above. He also spoke to the presenter of the programme speaking against the Iranian regime.
53. He used Skype as a means to discuss politics. He referred to open session on Skype about the killing of the Mujahideen in Iraq. The discussion on Skype was later posted on YouTube and was critical of why people are massacred and enquired about who was responsible.
54. As well as adopting his statements the appellant drew attention to printouts in the bundle showing his Facebook page. These included screen shots with people the appellant identified as prominent critics of the Iranian regime. He identified sites that had been hacked. He explained there were some pages where he shared control with five or six other people and another page that was private to him. He then explained how a group had hacked one of the sites to which he contributed including one used to bring together the different groups. He had several sites of which he was administrator including a Facebook page and a YouTube page.
55. The witness was cross-examined.
56. He confirmed that when he was in Iran he had set up a Facebook page with four others and it was the arrest of one of those, BD, that made him leave Iran. He left within 24 hours of the arrest with the help of BM. This had all been explained in his statement. He also accepted that he did not shut down the Facebook page when he heard of the arrest and he did not put up a warning to

tell people that it was a dangerous place to have discussed politics. In fact he did nothing to deter anyone from being open.

57. He confirmed that he did have US\$13,500 available to get him out of Iran.
58. He was at the time on a family farm.
59. He said the Facebook pages had been open for two years before he had to leave Iran and were run from a computer in his bedroom.
60. He was asked about the make of computer and his inability to remember it. He repeated as explained in his statement that the computer was assembled from separately purchased components. He confirmed that he could not remember the name of the components either. He also confirmed that after he had come to the United Kingdom the page was still open. He was then asked particularly about his own site, [WEBSITE]. He said that only he could put things on his own Facebook page. He did post videos from other sites. He was asked if friends could put what he wants onto the page and he said with his permission that could be done. He confirmed that anyone accepted as a friend could read his Facebook page and that when he was running the page from Iran he would check the identity of potential friends. He was less careful now he was in the United Kingdom but he did still give some thought to requests to allow people to be a friend. He was asked about his YouTube pages. This recorded how many times exhibited being watched, the recorded numbers tended to be in the low 100s or less. For example, on page 21 in the bundle, one featuring the appellant had recorded 301 views whereas one beneath it which the appellant had liked had attracted 42,812 views. He was asked about the interviews he had given and said they were for internet channels or satellite channels. One with Beca was a satellite channel and was a live interview so he was sure that had been broadcast. He could not know if other things that had been recorded had been noted. He accepted that very few people had visited his website.
61. He was not re-examined.

APPENDIX 3 ERROR OF LAW



Upper Tribunal
(Immigration and Asylum Chamber)

THE IMMIGRATION ACTS

Heard at North Shields
On 25th April 2013

Date Sent
On 02nd May 2013

.....

Before

UPPER TRIBUNAL JUDGE DAWSON
UPPER TRIBUNAL JUDGE COKER

Between

EF

Appellant

and

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Respondent

Representation:

For the Appellant: Ms S Harrison of Halliday Reeves Law Firm
For the Respondent: Mr C Dewison Home Office Presenting Officer

DECISION

1. The appellant, a national of Iran, date of birth [redacted], appeals a decision promulgated 14 May 2012 of First-tier Tribunal Judge Balloch who dismissed an appeal against a decision to remove him pursuant to s.10 of the Immigration and Asylum Act 1999. Permission to appeal was granted on 20th June 2012.

Background

2. The appellant arrived in the UK on his own passport and claimed asylum. His application was refused for reasons set out in a letter dated 27th October 2011 and he was served with a decision to remove him as an illegal entrant dated the same date.
3. The basis of his claim for asylum was, in essence, that he had been a founder member in Iran of a facebook group called [WEBSITE], the aims of which were to provide a background for a secular government in Iran. Comments, articles and links were placed on an “open” *facebook* page. He claims that one of the other founding members was arrested and, after having been informed of this a decision was taken by him and others in the group that he should leave Iran for his own safety. He also claims that the *facebook* “friends” have continued to expand since his arrival in the UK and he therefore bases a *sur place* claim on this activity.
4. During the course of his hearing before the First-tier Tribunal the appellant produced print outs of *facebook* pages which were not translated. The judge, also watched on a mobile (because of difficulties with the technical equipment in the Tribunal hearing room) an interview asserted to be with the appellant in Farsi whilst the appellant was in the UK with Mr Sorbi on [company redacted], a public broadcast internet communications company. Included in the documents produced was a transcript of that interview which was not certified by the translator (see paragraph 52 of the Consolidated Asylum and Immigration (Procedure) Rules 2005).
5. Judge Cope found:
 - a. He was unable to place any evidential weight upon the transcript of the television interview because it had no identification, no certificate of authenticity and no acknowledgement that the translator was aware of his/her responsibilities to provide an accurate translation.
 - b. The evidence was insufficient to establish that the appellant had been interviewed by Mr Sorbi on any publicly broadcast television station.
 - c. The pages of *facebook* produced during the course of the hearing were in Farsi, with no translation provided, and thus he was unable to establish the substantive content and refused to look at them.
 - d. He had not been provided with any evidential material to substantiate the appellant’s claim that the *facebook* social website had about 1,500 members which had increased to over 2000 members whilst he was in the UK.
 - e. The appellant had given contradictory evidence as to whether he had been arrested and how he had left Iran.
 - f. There are 30 million internet users in Iran; the appellant was unable to put forward any explanation why his “website” had been singled out or how it had actually come to the attention of the authorities.

Error of law

6. The grounds of appeal submit
 1. that the evidence produced by the appellant – *facebook*, *YouTube*, and [company redacted] distinguished the appellant both as an anti government activist in Iran and because of *sur place* activities in the UK.
 2. that the judge had failed to consider the ‘on-line’ evidence in the context of the background country evidence relating to Iran and the use by the Iranian Government of ‘cyberpolice’.
 3. the *facebook* page and other on-line material is open and available; a matter the judge failed to take account of.

7. The judge refused to consider the material produced because it was not translated. He appears to place great weight on the appellant’s account that he had produced these materials to his solicitors prior to the date of hearing and yet they were not produced until the hearing. Although there is no obligation upon a judge to consider un-translated document (see rules 51 and 52 of the Asylum and Immigration Tribunal (Procedure) Rules 2005) the judge is not prohibited from such consideration. The documents produced were, on the face of them from the few words that were not in Farsi, appear to relate to the appellant whose photograph appears. We note that an adjournment was not requested to enable translation but given the clear relevance to the case we do consider that the judge should have considered them on the basis of the information that was available and taken them into account in reaching his decision; at the very least he should have explained in rather more detail why the lack of translation was sufficient to ignore them when there were elements that would have been apparent and relevant.

8. The judge refers to 30 million internet users in Iran but does not appear to have recognised that an open *facebook* account does not require such scrutiny as the judge appeared to consider necessary, by the Iranian authorities to identify subversive or anti government activity.

9. The judge in his determination did not address the appellant’s *sur place* activity despite this being a significant element of the appeal; he referred and made findings upon the appellant’s activity in Iran only. However we are satisfied that those findings made by the judge have been infected by the lack of consideration of the facebook material and the refusal to consider the TV interview transcript.

10. In these circumstances we are satisfied there are errors of law such that the decision be set aside to be remade. None of the findings as regards the appellant’s activity in Iran or his claimed *sur place* activity are to stand.

11. Further directions are to follow.

Conclusions:

The making of the decision of the First-tier Tribunal did involve the making of an error on a point of law.

We set aside the decision to be re-made.

Date 30th April 2013 re-dated 13th May 2013

Judge of the Upper Tribunal Coker