Background papers for the [proposed] Guidelines on Analysing Social Media Evidence for the IARMJ

From the IARMJ's Country of Origin Information, Expert Evidence and Social Media Working Group

The rise of social media has been one of the most significant phenomena of the 21st century. It is regularly encountered in every area of life in developed societies where information technology is available. We hope it will be useful to take time in reflecting how judges adjudicating in Refugee Convention claims to consider how such material should be weighed in the balance alongside other evidence.

By social media we refer to interactive technologies that facilitate the creation and sharing of information, ideas, interests, and other forms of expression through virtual communities and networks. Here is one definition propounded by a judge (speaking extra-judicially):[1]

> "Social media refers to a variety of online platforms which are centred on social interaction. These platforms defy the traditional one-way model of distribution and consumption in other forms of media. In traditional models, such as print, TV and radio, content is created at a central source and distributed to consumers in a one-way, usually dead-end direction. Letters to the editor and talk back radio are limited exceptions within this traditional model. With social media, content is not merely consumed by users, it is also created, organised and distributed by them. Social media platforms thereby create a dialogue between different people, allowing them to communicate and share information."

Social media applications (commonly termed "Apps") typically feature user-generated content (such as text posts by the author and comments by other users on the author's posts, though also digital photos and videos) and data generated through online interactions. Users create profiles specific to the service in question that are then maintained by the application. Active use of a particular application helps the development of online social networks by connecting a user's profile with those of other individuals or groups. One form of social media is the blog (from "web-log") which is an informational website published on the World Wide Web consisting of discrete, often informal diary-style text entries ("posts", a term also given to any written contribution by a user via their account).[2] Typically posts are the subject of "likes" where approved by other users who may well distribute them onwards by sharing them with their own online circle of acquaintance.

There are numerous forms of social media, some so well known as to be ubiquitous in modern life: Facebook, Twitter and Instagram are commonly encountered. Around the

[1] The Hon T F Bathurst (Chief Justice of New South Wales) Tweeters, Posters and Grammers Beware: Discovery and social media evidence (10th Information Governance & Ediscovery Summit, 21 June 2016)

[2] Wikipedia definition – we cite Wikipedia as the leading online public encyclopaedia is particularly apposite for social media, itself an online phenomena.

world there are many others and different countries may restrict access to platforms seen as Western in ownership or outlook: for example in China only LinkedIn is available amongst the more common internationally popular applications,[3] whereas in Iran, Instagram and Pinterest amounted to over 55% of all social media usage and Facebook only 15%.[4]

Not everyone engages in social media, of course, and the judicial community is doubtless much more reticent than some other professions. Nevertheless as noted by the Global Judicial Integrity Network:[5]

> "Irrespective of whether they use social media or not, judges should have a general knowledge of social media, including how it may generate evidence in cases that judges may decide. Judges should also have an understanding of existing online communication tools and technology, including artificial-intelligence-powered technology."

National status determination authorities take an increasing interest in social media. In 2019 the USA's Department of Homeland Security proposed collecting usernames from nineteen social networking sites.[6] In Norway asylum seekers are asked to hand over their mobile phones and Facebook login details at their first point of contact with the authorities, noting that this may permit access to photos, friends, likes, interests, activities, travel routes and more – the law requires that their consent be informed and freely given.[7] Then government agents may access social media data (on the asylum seeker and their connections) not only by looking at publicly available data online but also by logging into social media platforms using constructed personas which cannot be traced back to the individual civil servant or to the institution, in accordance with internal guidelines: a practice intended to protect both civil servants and claimants. In Germany the analysis of digital devices to determine the nationality and identity of an asylum seeker or potential deportee is permitted without their consent[8] where necessary if no less intrusive measure is available; potentially this would authorise analysis of social media accounts.[9]

Blanket policies to confiscate the mobile phones of asylum seekers need to be critically assessed as to whether they are in accordance with the law and the underlying statutory

[3] Statista records the *Share of internet users of the leading social media in China as of 3rd quarter 2022* as 81.6% for Wechat.
[4] Social Media Stats Islamic Republic Of Iran (Feb 2022 - Feb 2023) published by Statcounter GlobalStats.
[5] Non-binding Guidelines on the Use of Social Media by Judges (UN Office of Drugs and Crime pursuant to the Global Programme for the Implementation of the Doha Declaration, Guideline 3).
[6] Federal Register Vol. 84, No.171 Federal Register, Volume 84 Issue 171 (Wednesday, September 4, 2019) (govinfo.gov).
[7] *Social media screening: Norway's asylum system* (Forced Migration Review, June 2019; Jan-Paul Brekke and Anne Balke Staver of the Institute for Social Research and Oslo Metropolitan University).
[8] Under Article 7 of the EU GDPR consent must be freely given, specific, informed and unambiguous.
[9] Article 15a of the Asylum Act (§ 15a AsylG), section 48(3a) of the Residence Act (§ 48 Abs. 3a AufenthG); the Federal Administrative Court is set to examine the issue in BVerwG 1 C 19.21 - Urteil vom 16 February 2023.

powers permitting such actions.[10] There may be national or regional norms which control the processing of data, such as the European Union's General Data Protection Regulation, which requires lawful, fair, transparent and secure accurate data collection procedures which retain only the minimum data which is essential to achieve a specific purpose.[11]
UNHCR
have warned of the need for safeguards against unwarranted seizure of devices: such measures should never become routine but should take place only where strictly necessary, regard should be had to lawyer/client privilege in reviewing the material thereby obtained, and it should be borne in mind that asylum seekers may well use false names to avoid endangering their families in the country of origin. UNHCR stress that regard should be had to the rights to human dignity, to private and family life, to protection of personal data, and to own, use, and dispose of one's lawfully acquired possessions.[12]

Social media evidence may be relevant in asylum determination in various ways, most obviously:

(a) In corroborating the truth of an account, because events asserted to have taken place are verifiably documented online.
(b) In controverting the truth of an account, because information comes to light which is inconsistent with the asylum seeker's story.[13]
(c) In determining the level of exposure a person's profile or views may have had, via the extent of their social network and via any express threats received.
(d) In assessing whether the foreseeable reaction of the authorities in the country of origin would be because of an actual, or attributed, Convention reason, such as political opinion or religion.[14]
(e) An individual who was a previously active blogger in their home country may cease posting in the country of refuge out of fear for their family members, or they may start posting under an anonymous name.

[10] See eg *HM, R (On the Application Of) v Secretary of State for the Home Department [2022] EWHC 695 (Admin).*
[11] The EU GDPR (General Data Protection Regulation) Reg 2016/679.
[12] UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers (4 August 2017): citing the Universal Declaration of Human Rights Art 1 and International Covenant on Civil and Political Rights Article 10, the EU Charter of Fundamental Rights), Article 1 for human dignity, Article 17 ICCPR and the ECHR for private and family life, and Article 12 UDHR, Article 17 ICCPR and Article 8 EU Charter of Fundamental Rights for the data protection and property rights.
[13] Or the events allegedly portrayed may be deemed incredible because they appear tangibly staged, as in *ML (India)* [2022] NZIPT 802024 where the attack appeared unduly gentle and was inconsistent with the narrative in witness statements. It should be recalled that events posted on Facebook may be backdated and edited: see *BF (Turkey)* [2018] NZIPT 801264.
[14] The Asylum Research Unit (ARU) at the Higher Administrative Court of Baden-Württemberg has regard to the Twitter accounts of Taliban Ministries as these are more informative than official websites.

However, just because we live in the age of social media does not necessarily mean that every asserted event will find some form of confirmation online, and courts have found an assumption to the contrary unwarranted.[15] The deletion of an asylum seeker's social media account in the course of status determination may raise an inference that their credibility is suspect.[16]

Social media evidence may arise in the context of any kind of asylum claim, though for the purpose of example we will concentrate on asylum claims arising from political opinion. The evidence may relate to a continuum of scenarios:

(a) A genuine political activist with a historic profile abroad may continue their blogging and posting, wholly consistently with their past conduct.

(b) An individual with a modest profile abroad historically (below the level that might have otherwise attracted persecution) might begin posting their views in the country of asylum, because that is the only way of conducting any political activity once they are no longer in their country of origin.
(c) A previously non-demonstrative individual might respond to an environment of free speech by posting views that they had not previously expressed. This would be a response to what is often called the chilling effect of repressive laws in the country of origin.
(d) An asylum seeker whose claims as to their personal history may be rejected as wholly dishonest such that the conclusion must be that their current social media activities are not underlain by any genuine beliefs.

Social media may be new, but the underlying themes it raises are not. Most of them are addressed in UNHCR's long-standing *Handbook on Determining Refugee Status*.[17] The Handbook states:

> "83. An applicant claiming fear of persecution because of political opinion need not show that the authorities of his country of origin knew of his opinions before he left the country. He may have concealed his political opinion and never have suffered any discrimination or persecution. However, the mere fact of refusing to avail himself of the protection of his Government, or a refusal to return, may disclose the applicant's true state of mind and give rise to fear of persecution. In such circumstances the test of well-founded fear would be based on an assessment of the consequences that an applicant having certain political dispositions would have to face if he returned. This applies particularly to the so-called refugee "sur place".
> …

[15] The Federal Court of Australia in *BZD17 v Minister for Immigration and Border Protection* [2018] FCAFC 94.
[16] *Pestova v. Canada (Citizenship and Immigration)*, 2016 FC 1024 (CanLII).
[17] Handbook on Procedures and Criteria for Determining Refugee Status under the 1951 Convention and the 1967 Protocol relating to the Status of Refugees (UNHCR, 1979, reissued 1992 and 2019.

> 95. A person becomes a refugee "sur place" due to circumstances arising in his country of origin during his absence. ..
>
> 96. A person may become a refugee "sur place" as a result of his own actions, such as associating with refugees already recognized, or expressing his political views in his country of residence. Whether such actions are sufficient to justify a well-founded fear of persecution must be determined by a careful examination of the circumstances. Regard should be had in particular to whether such actions may have come to the notice of the authorities of the person's country of origin and how they are likely to be viewed by those authorities."

We can see in this foundational UNHCR guidance a number of the issues that have reverberated through refugee status determination subsequently.

(a) Opinions may become apparent after leaving the country of origin
(b) Assumptions may be made by the authorities abroad simply based on claiming asylum
(c) Relevant considerations are likely to be whether there has been verifiable association with dissidents or acts of political expression, and the reaction of the authorities abroad

Even acts undertaken in bad faith may create risk. National courts have found that there is no exclusion clause for acting in bad faith, and so an asylum seeker may have a viable refugee claim based on expressions of political views that they do not truly hold.[18] However such cases should receive especially close examination: UNHCR have suggested that "*a more stringent evaluation*"[19] would be appropriate in those cases.

The European Union's Qualification Directive also addresses the possibility that *sur place* activities have been conducted with a view to manufacturing an asylum claim:[20]

[18] The Court of Appeal of England and Wales in *Danian v Secretary of State for the Home Department* [1999] EWCA Civ 3000. Similar thinking is shown by the Federal Court of Australia in *Mohammed v Minister for Immigration and Multicultural Affairs* [1999] FCA 868 §§24-28 stating that "fraudulent activity by an applicant for refugee status may, in itself, attract malevolent attention from authorities in the country of nationality" and that "close scrutiny" is appropriate in such cases. See also the New Zealand case of *re HB* (Refugee Appeal No 2254/94); the United States Court of Appeals, Seventh Circuit, in *Bastanipour v INS* 980 F 2d (1992); *Ghasemian v. Canada (Minister of Citizenship and Immigration)*, 2003 FC 1266 (CanLII). The Australian legislature has intervened with a contrary approach: s5J(6) of the Migration Act 1958 provides "(6) In determining whether the person has a well-founded fear of persecution … any conduct engaged in by the person in Australia is to be disregarded unless the person satisfies the Minister that the person engaged in the conduct otherwise than for the purpose of strengthening the person's claim to be a refugee."

[19] Letter from Peter van der Vaart of UNHCR cited in *Danian* (fn 4 above).

[20] Art 4(3)(d), Art 5(2) of Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted.

"The assessment of an application for international protection is to be carried out on an individual basis and includes taking into account: …

> whether the applicant's activities since leaving the country of origin were engaged in for the sole or main purpose of creating the necessary conditions for applying for international protection, so as to assess whether these activities will expose the applicant to persecution or serious harm if returned to that country;

A well-founded fear of being persecuted or a real risk of suffering serious harm may be based on activities which have been engaged in by the applicant since he left the country of origin, in particular where it is established that the activities relied upon constitute the expression and continuation of convictions or orientations held in the country of origin."

One national Tribunal[21] itemised the following relevant factors to be considered when

assessing risk on return having regard to sur place activities, here in the context of public participation in demonstrations within sight of an asylum seeker's country of origin's Embassy or Consulate. It emphasised

(a) The nature of the activities in question (a demonstration's political objectives, the role of the asylum seeker as a leader, mobiliser, organiser, crowd member or banner carrier, the regularity of these activities, the publicity attracted, and how matters will be seen by the regime abroad);
(b) Identification risk via evidence (if it can be reasonably expected) of surveillance of demonstrators via filming or crowd infiltration by agents, and the foreign regime's capacity to identify individuals via advanced technology such as facial recognition or allocating human resources to fit names to faces in the crowd;
(c) Factors triggering inquiry/action on return such as political profile and category of activities, immigration history as to mode of departing the country of origin which may lead to the necessity of the country of asylum negotiating directly with the country of origin over emergency travel documents;
(d) The consequences of identification, ie whether there is differentiation between demonstrators depending on the level of their political profile adverse to the regime
(e) Identification risk on return: is positive identification systematically stored and used and accessible to border posts.

Any legal process will focus on the available evidence. But national courts have warned that expectations should not be set too high:[22] intelligence services worthy of the name are likely to mask their surveillance activities. Accordingly it may be appropriate to assume, regarding

[21] The UK's Upper Tribunal in *BA Iran CG* [2011] UKUT 36 (IAC).
[22] *YB (Eritrea) v Secretary of State for the Home Department* [2008] EWCA Civ 360.

asylum claims brought in relation to States known to suppress dissent and to take an interest in their reputation abroad, that public

demonstrations in host countries will be filmed or photographed, and that they may well have informers amongst expatriate communities.

When considering the likely meaning to be attributed to social media postings, it may be appropriate to bear in mind the nature of the medium. Judges have identified the format as a conversational medium for which an impressionistic approach is fitting, bearing in mind that very often the intention of the "App" and of the post is that the message be passed on to other users.[23]

Asylum claims involving expression of genuine political opinions will require consideration of whether the asylum seeker can reasonably be expected to conceal their true beliefs on a return to their country of origin. As one judge put it in the related context of concealment in gender preference claims:[24]

"The way he conducts himself may vary from one situation to another, with varying degrees of risk. But he cannot and must not be expected to conceal aspects of his sexual orientation which he is unwilling to conceal, even from those whom he knows may disapprove of it. If he fears persecution as a result and that fear is well-founded, he will be entitled to asylum however unreasonable his refusal to resort to concealment may be. The question what is reasonably tolerable has no part in this inquiry."

The UK's Upper Tribunal has reviewed some issues arising from the use of social media evidence.[25] It had the benefit of receiving answers to written questions from Facebook Ireland and the input of two expert witnesses, a research assistant at the computer laboratory of the University of Cambridge, and the director of research of a campaigning and advocacy organisation for the rights of those wishing to publish social media material, without hindrance, in Iran and the wider Middle East. The Upper Tribunal accepted that both witnesses had relevant expertise and noted their evidence that:

(a) Permanent deletion of an individual user's Facebook account was possible and would remove everything added to Facebook, from that user's perspective.
(b) However that deletion might well take up to 90 days to take full effect albeit that it would not be accessible to individual users over that period.
(c) Deletion however was partial: for example messages between users would not be deleted, because they were was stored separately in user inboxes; nor would

[23] Lord Kerr in *Stocker v Stocker* [2019] UKSC 17; an English judge in *Monroe v Hopkins* [2017] EWHC 433 (QB) §35.
[24] *HJ (Iran) v Secretary of State for the Home Department* [2010] UKSC 3 §35(b); see also the CJEU in *Bundesrepublik Deutschland v Y & Z* [2012] EUECJ C-71/11 (05 September 2012) at §78-80; the Federal Court of Canada in *Antoine, Belinda v. M.C.I.* (F.C., no. IMM-4967-14), Fothergill, June 26, 2015; 2015 FC 795; the High Court of Australia in *Appellant S395/2002 v MIMA* (2003) 216 CLR 473 at [40].
[25] *XX (PJAK - sur place activities - Facebook) Iran CG* [2022] UKUT 23 (IAC).

photographs that had been shared with other users as those would remain extant within the latters' accounts.

(d) Facebook would disclose information from users' accounts to governments in certain circumstances (Facebook reports on this via regular Transparency Reports):[26] it would

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

(e) If Facebook considers content is illegal under local law, then it is made unavailable in the relevant country or authority.

(f) In general, internet search engines may search online and cache information (there is a privacy setting that can prevent this, but most users opt for the defaults: ie fully public, or shared with friends only).

(g) The modern approach of intelligence services to social media would probably not be to conduct enquiries at the border at the point of return, but rather to "scoop" vast quantities of data periodically and search within that downloaded resource. Web crawler software can "scrape" data from many websites though well known Apps such as Facebook are alive to this possibility and aim to prevent it. It appears that web crawlers can only obtain limited information from Facebook at present. There was no evidence that Facebook had itself been "hacked".

(h) There are various ways to access a person's Facebook records – simply by engaging with an account which is public in the first place, or seeking to obtain access to non-public material via false friend requests (ie requests from user accounts asserting sympathy with the asylum seeker's cause but in truth emanating from their country of origin's security forces), or tricking them into revealing their log-in details (eg by phishing and spear-phishing, by which personal information is sought on false pretences with a view to obtaining or securing the means to access a password).

[26] Eg *Transparency Report, First Half 2022* including the *Government Requests for User Data* report – eg in the first half of 2022 Facebook received from the Bangladesh authorities 659 requests into 1,171 user accounts of which 610 were legal process requests; Facebook produced some data in response in 66% of those cases.

Having regard to that evidence, the Upper Tribunal in *XX Iran* concluded that

(a) Intelligence services are likely to place significant weight on a person's "social graph": ie their position within a broader network of related people and their relative importance within that network. This will likely determine the level of surveillance they subsequently receive.
(b) It was possible for intelligence services to extract information about users even if they kept their accounts private: because their "Friends" with public settings on their own accounts might have republished the material.
(c) An asylum seeker's prominence via social media could usually be assessed by the level of interaction with their account: eg via "likes" and "comments".
(d) Oppressive regimes were likely to research the profile of a returnee at the moment an emergency travel document was sought on their behalf, rather than at the border on return.
(e) Social media evidence from Facebook should, for transparency, be presented via the "Download your information" function which would give a full overview of the account and avoid only partial disclosure.
(f) One aspect of status determination should be to consider whether a returnee would, if faced with imminent return to their country of origin, close their Facebook account, and not reveal its prior existence if questioned by their national authorities on return. This could reasonably be expected of individuals who lacked any genuine political beliefs and where the social media usage in question was not linked to the exercise of any fundamental right.[27]

Sometimes it may be considered desirable to access an asylum seeker's social media accounts with a view to seeing if the material therein corroborates (or undermines) the case being put. For example, when a young person's age is disputed, their postings and their communications with friends and family might cast light on their maturity. Where the national legal regime includes a duty of candour by which the parties must place all their cards on the table it may be appropriate or necessary for the lawyers representing children to analyse and disclose relevant social media messages to the court.

In so doing legal representatives would need to ascertain what social media Apps are used, identify the content therein, and consider whether anything adverse to their client needs to be disclosed. A disclosure statement explaining the steps taken might be appropriate explaining the scope of the research and that the work undertaken was reasonable and proportionate.[28] Disclosure of social media accounts is likely to represent an interference with a young person's private life and so excessively broad disclosure would not necessarily

[27] *XX (PJAK - sur place activities - Facebook) Iran CG* [2022] UKUT 23 (IAC). *Rizwan v. Canada (Citizenship and Immigration)*, 2017 FC 456 (CanLII), holding that it would be reasonable to expect an asylum seeker to avoid disclosing their location via social media in the context of seeking employment opportunities.
[28] *BG, R. (on the application of) v London Borough of Hackney (social media, candour, disclosure)* [2022] UKUT 338 (IAC).

be appropriate (eg a demand to hand over one's one's passwords to a government legal team would be likely to be disproportionate). In those jurisdictions where the legal principle of proportionality applies, it will be appropriate to consider the necessity of making a disclosure order against an asylum seeker and whether a less intrusive measure is appropriate.[29]

The appropriate means of presenting social media evidence needs to be considered. National procedure rules may address the issue directly or by implication. Judges may wish to check the online version at the internet domain address. But it will usually be desirable for a hardcopy (or its equivalent in the modern era of electronic filing) to be available so that the legal representatives for the government and the asylum seeker as well as the judge can ensure they are literally "on the same page" when reviewing the evidence. It may be thought desirable for the asylum seeker's legal representatives to comply with a form of standard directions as to how best to present social media evidence: for example confirming that the critical pages are public and have been so at key moments throughout the period during which their representation of the case, including the period that the asylum application and subsequent appeals/reviews have been extant, and giving a concise summary of the associated metadata such as the account's following and the numbers of likes, shares and other forms of engagement. This would avoid matters which are in truth objectively ascertainable with appropriate case management being left to conjecture. Case management directions may be appropriate to allow for social media evidence to be accessed and viewed in the course of a hearing.

The review above of salient legal issues arising from the social media evidence in international protection appeals highlights several recurring legal themes:

(a) Is the asylum seeker relying on social media evidence as part of the material supporting their asylum claim?
(b) If so, how can this information be accessed safely and lawfully?
(c) If not, should steps be taken to encourage the disclosure of any such material? What are the privacy and private life implications of so doing?
(d) Will their activities have come to the attention of the authorities of the country of origin and, if so, what is their likely response?
(e) Should the asylum seeker reasonably be expected to desist from their social media activities?
(f) How can any social media evidence relied upon in an appeal be preserved?

[29] The legislative powers in Germany permitting analysis of asylum seekers' electronic devices include measures to protect private life: see fn 8 above.

Proposed Judicial Guidelines for the analysis of social media evidence in refugee, protection and migration appeals:

Judges will wish to consider taking the following factors into account.

1. **Malleability**
   - **How easily could the account have been altered such that what is now provided does not reflect the real account**
2. **Reliability**
   - **How do we know that what we are shown truly comes from the Appellant's established social media profile?**
3. **Durability**
   - **How long will it last/how long was it live?**
4. **Visibility**
   - **Public/private settings, friends, "shares", "likes", links from other platforms**
5. **Deletability**
   - **Could it be deleted and what would the fundamental rights consequences of that be?**
6. **State enquiries**
   - **Country of origin's authorities' interest in social media: monitoring expatriate activities, "false friends", enquiries on return**
7. **Accessibility**
   - **How can a relevant social media account be accessed safely and lawfully**
8. **Preservation of evidence**
   - **How can relevant social media evidence be preserved and archived**

Contributors:

- Mark Symes (Deputy Judge of UK Upper Tribunal Immigration and Asylum Chamber)
- Louise Moor (Member - Immigration and Protection Tribunal of New Zealand)
- Christine Cody (Member - Administrative Appeals Tribunal of Australia)
- Dr Sophie Roche (Head of Asylum Research Unit) and
- Dr. Philipp Wittmann (Judge) – both at the Higher Administrative Court of Baden-Württemberg
- Hugo Storey (Judge of UK Upper Tribunal Immigration and Asylum Chamber, retired)
- Julian Phillips (Resident Judge of UK First-tier Tribunal Immigration and Asylum Chamber)

This background paper and draft Guidelines are the views of individual judges and do not represent the view of the courts and tribunals for whom they work.

May 2023