UNHCR
United Nations High Commissioner for Refugees
Haut Commissariat des Nations Unies pour les réfugiés

UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers

1. Introduction

A number of European States have recently adopted or are currently considering the adoption of legislation allowing authorities to seize and search personal electronic devices, such as mobile phones and tablets, for the purpose of verifying an asylum-seeker' identity, but also to assess the substance of an asylum application, including for potential security risks, as well as possible exclusion grounds.

UNHCR recognizes the legitimate interests of States in seeking to identify persons on its territory, including in relation to individuals who may potentially have committed excludable acts or pose a threat to national security, as well as their interest in seeking to ensure that asylum decisions are based on the most comprehensive and accurate information available.

In accordance with established and widely-applied legal principles and practice, applicants for asylum and decision-makers also have a shared duty to ascertain and evaluate all relevant facts and to clarify incomplete or contradictory statements relating to the material elements of a claim.[1]

UNHCR therefore acknowledges that there may be situations in which the seizure and search of asylum-seekers' personal electronic devices may be justified to achieve these legitimate purposes. However, for this to be the case, certain conditions must be met. Given the potential consequences of such intrusive measures, the legal safeguards protecting individuals against unwarranted seizure and search of personal electronic devices should not be reduced or denied to asylum-seekers in individual instances, nor should they become a routine part of asylum procedures, but should apply only where necessary for the examination of the application.

This notes sets out UNHCR's preliminary legal observations and key principles that should apply to the formulation, adoption and application of legislation and practices on the seizure and search of electronic devices of asylum-seekers.

2. Relevance and Use of Data Retrieved from Electronic Devices

Electronic data saved on mobile devices will frequently include a wide range of information of a personal and sensitive nature (e.g. private communications, financial records, browsing history, GPS location; social media etc.). While some of this data may bear direct relevance in the consideration of an asylum application, much will not, or will even be subject to specific protection under the law in most jurisdictions, such as information covered by lawyer-client

[1] UNHCR, *Handbook on Procedures and Criteria for Determining Refugee Status under the 1951 Convention and the 1967 Protocol Relating to the Status of Refugees*, December 2011, HCR/1P/4/ENG/REV. 3, para. 196, http://www.refworld.org/docid/4f33c8d92.html.

privileges and medical information. The ease of access of electronic data does, in UNHCR's view, not justify an unfocused, indiscriminate or speculative search for information.

UNHCR also wishes to underline that the evidentiary value of electronic data should be considered with great care. Asylum-seekers will often avoid using their correct names on social media platforms, including to evade surveillance and possible persecution, or potential harm to their families in their country of origin. Further, digital and electronic evidence may in certain instances have limited reliability or accuracy or may be easily altered. Finally, it is relatively common for mobile devices to have been handed over or used by other individuals, including smugglers or traffickers.

Due consideration should be given to these factors when verifying information or otherwise assessing the credibility of an asylum-seeker's application, based on information retrieved from electronic devices. Moreover, due care should also be taken to ensure that the asylum-seeker or his/her legal representative has access to any evidence that will be used to determine the asylum application.

3. Seizing and Searching Electronic Devices

Relevant for the seizure and search of electronic devices are the asylum-seeker's right to human dignity;[2] the right to private and family life;[3] the right to protection of personal data;[4] and the right to own, use, and dispose of his or her lawfully acquired possessions.[5]

In accordance with these legal standards and practices, any seizure or search must be conducted for a *legitimate purpose,* provided for by law, and be *necessary* and *proportionate* to achieve that specific purpose, while ensuring that appropriate procedural safeguards are in place and respected in practice.

The following considerations and safeguards should, in UNHCR's view, apply for any seizure and search of electronic devices to be legitimate:

a. Any seizure and search should be undertaken based on the free and informed consent of the individual concerned. For consent to be informed, the individual must receive adequate information regarding the procedure and its purpose, in a timely manner, and have access to counselling in order to properly understand her or his rights, and the potential implications of consenting or not.

b. Seizure and search without the consent of the individual may be justified only if it serves a legitimate purpose provided for by law and is based on a decision reached in an individual - case-by-case – assessment, in accordance with applicable legal safeguards, and made by a competent authority. Of particular importance is an assessment of the necessity of the seizure and search and its impact on the individual concerned.

---

[2] See e.g. *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III) (UDHR), Article 1, http://www.refworld.org/docid/3ae6b3712c.html, *International Covenant on Civil and Political Rights* (16 December 1966) 999 UNTS 171 (ICCPR), Article 10, http://www.refworld.org/docid/3ae6b3aa0.html and *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02 (EU Charter of Fundamental Rights), Article 1, http://www.refworld.org/docid/3ae6b3b70.html.

[3] See e.g. Article 17 ICCPR and *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, Article 8, http://www.refworld.org/docid/3ae6b3b04.html.

[4] See e.g. Article 12 UDHR, Article 17 ICCPR and Article 8 EU Charter of Fundamental Rights.

[5] *Ibid*.

c. Any seizure and search can only be carried out by a competent authority in accordance with legally-defined powers and safeguards.

d. If less intrusive measures or techniques are available to fulfill the purpose (for example, to verify a person's identity), these should be applied instead.

e. Authorities should only retain and store data that is *relevant and material to* the purposes of seizure, and only for so long as necessary to fulfill this purpose (for example to assess the asylum claim, or a potential exclusion ground or threat to national security). Excess data should not be retained, but rather returned in a timely manner or destroyed, provided this does not infringe other rights of the person concerned.

f. Data which is retained should be stored in a safe manner, and its further use limited to the specified purpose which is relevant to that individual case, and accessed by authorized personnel only.

g. The seizure of property should be limited in time and the seized property returned to its owner when the purpose has been fulfilled. If the purpose of the seizure can be fulfilled by taking a copy of the relevant data, rather than seizing the device itself, this should be done instead.

h. No action taken by relevant authorities and persons employed representing these authorities should change, alter or delete data which may subsequently be relied upon in asylum proceedings.

i. In circumstances where a representative of the relevant authorities find it necessary to access original data, that person must be competent to do so, equipped with the relevant specialised knowledge, and able to give evidence explaining the relevance and the implications of their actions.

j. An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and reach the same conclusion.

k. Asylum-seekers whose devices have been seized and searched must have access to an effective remedy, to challenge the legality of the seizure or search; and to ensure the return of any seized devices.

UNHCR

04 August 2017