European Court of Human Rights

***Maciej NABRDALIK v. Poland*, Application No. 30614/22**
***Maciej MOSKWA v. Poland*, Application No. 30848/22**

WRITTEN SUBMISSIONS OF PRIVACY INTERNATIONAL AND ARTICLE 19

Introduction and summary of intervention

1. This intervention is submitted by Privacy International (PI) and ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19, henceforth jointly referred to as the "Interveners"), pursuant to leave granted by the President of the Section of 31 July 2023 in accordance with Rule 44(3) of the Rules of the Court. PI is a non-profit, non-governmental organisation (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. ARTICLE 19 is an international human rights organisation which defends and promotes freedom of expression and freedom of information all over the world.

2. The present case concerns the apprehension of journalists and searches of their phones and cameras in relation to them documenting events close to the Polish-Belarusian border, in November 2021. As such, it presents the Court with a unique opportunity to assess the seriousness of interferences with privacy and freedom of expression that searches of digital devices constitute, and what safeguards are therefore necessary.

3. In order to assist the Court in its assessment of the compatibility of digital device searches with Articles 8 and 10 of the European Convention on Human Rights (the "**Convention**"), the Interveners will address:

   (i) the impact on fundamental rights of known forms of digital device extraction methods used by authorities around the world and the types of data obtained;

   (ii) comparative case law from other Contracting and non-Contracting States with regard to extraction of data from digital devices in immigration enforcement and border control contexts; and

(iii) the necessary and appropriate safeguards pursuant to Articles 8 and 10 of the Convention for the protection of journalists and media organisations against the search and seizure of their digital devices.

(i) The impact on fundamental rights of known forms of digital device extraction methods used by authorities around the world and the types of data obtained

4. The Interveners note at the outset that the search of individuals by authorities amounts to an interference with the right to respect for private life, under Article 8 of the Convention (see e.g. *Gillan and Quinton v. UK,* no. 4158/05, 12 January 2010, §63). As for the specific search of digital devices, the practice that the Applicants were subjected to by Polish military officers during their apprehension can be broadly referred to as "mobile phone extraction" ("MPE").[1] It involves the extraction, retention and analysis of data stored on a phone or other digital device, and of cloud-stored data.[2] The Interveners do not know whether the Polish military officers used forensic extraction tools in order to search the applicants' devices, or if they obtained access through other "soft" methods (such as demanding and obtaining the applicants' PIN codes) and copied contents to another device. Whatever method was used, the potential level of intrusion into the applicants' private lives is similar.

5. MPE is intrusive in at least three interrelated ways. **First**, it involves the collection, review, and analysis of much greater amounts of information than would a search of a home, which has for decades been subject to stringent safeguards around the world. The US Supreme Court in the case of *Riley v California* 573 US 373 (2014), one of the first cases worldwide to explore the use of MPE evidence in law enforcement, observed:

> *"Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. […] The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows just even one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labelled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier … a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."*

6. While the Interveners do not know whether and what software was used to extract and analyse the data in this case, they are aware of recent reports that the Polish Police has purchased MPE software from Israeli provider Cellebrite.[3] In 2019, Privacy International

[1] The applicants claim that *"the contents of their phones and cameras [were] checked and partly copied"*.
[2] Privacy International, Mobile phone extraction, https://privacyinternational.org/learn/mobile-phone-extraction.
[3] Claudia Ciobanu, New Powers and Software for Polish Police Alarm Experts (Balkan Insight, 19 January 2023), https://balkaninsight.com/2023/01/19/new-powers-and-software-for-polish-police-alarm-experts/.

performed technical research into Cellebrite's UFED software.[4] The images in Annex 1 are screenshots of the software's data visualisation platform, showing the vast number of files and types of data that were extracted, and the very granular categorisation of data. The numbers in red show deleted items, which can also be extracted depending on the type and level of extraction used.[5] Privacy International's research has also shown that Cellebrite's MPE software allows for the reconstruction and automatic ordering of vast amounts of data from various sources and of various kinds into categories, timelines and chronologies.[6] A full list of the types of data that the Interveners are aware the most common MPE software are able to extract is available in Annex 2.

7. The Interveners note that recent technology now enables the extraction of data from cloud-based services, hence providing access to data that is not stored on the device. This opens the door to considerably larger amounts of data than simple device extraction. Of even greater concern, it also enables authorities to continue tracking the online behaviour of the device's user even once they are no longer in possession of the device, by using online storage, social media or other login credentials acquired through the initial device extraction process.[7]

8. **Second**, the data collected by MPE is highly sensitive. MPE extracts *communications data*, or metadata, whose collection has been recognised by the Court of Justice of the European Union ("CJEU") as a *"particularly serious"* interference with privacy (*Privacy International v Secretary of State for Foreign and Commonwealth Affairs ao*, C-623/17, Judgment, 6 October 2020, §81), but also *content data*. This includes the content of messages and emails, as well as photos, videos or documents on the device, location data and social media data.

9. Further, unlike a notebook, where the owner has full control and knowledge of its contents, users of digital devices may not initiate or even know about all the data created and stored on their devices.[8] Apps can record data without the user's awareness, such as app usage, location data, browsing data, cookies, etc. Their media library may contain items they have not stored there themselves – apps such as WhatsApp, on their default settings, will push media sent by someone else onto the device (such as in the Photos folder), unless the user explicitly disables this feature.[9]

10. All this data can reveal information about the most sensitive parts of a person's life: their health conditions, personal relationships, family life, sex life or sexual orientation, everyday movements and activities, most intimate thoughts, political and religious beliefs,

---

[4] Privacy International, What types of data can law enforcement extract from my phone? (30 April 2019), https://privacyinternational.org/news-analysis/2840/what-types-data-can-law-enforcement-extract-my-phone.
[5] For more information on the different types and levels of extraction, see Witness Statement of Privacy International in *R (on the application of HM and MA and KH) v Secretary of State for the Home Department* [2022] EWHC 2729 (Admin), https://privacyinternational.org/sites/default/files/2022-01/06.01.21%20Graham%20Wood%20WS%20Privacy%20Int%20Redacted_0.PDF, §§ 24-41.
[6] Witness Statement of Privacy International, §42-55.
[7] Privacy International, Cloud extraction technology: the secret tech that lets government agencies collect masses of data from apps (7 January 2020), https://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data.
[8] Information Commissioner's Office (ICO), Investigation report: Mobile phone data extraction by police forces in England and Wales (June 2020), https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.
[9] Witness Statement of Privacy International, §47.

finances, etc. If the device is also used as a work medium, it can reveal sensitive and confidential information, in particular when the phone owner is a journalist, as in the present case.

11. Where the information acquired concerns *"a most intimate part of an individual's private life"*, *"particularly serious reasons"* are required to justify the interference (*Lustig-Prean and Beckett v UK*, nos. 31417/96 and 32377/96, 25 July 2000 §82). This is especially so in respect of health data, or that which might reveal ethnic origin (*S and Marper*, nos. 30562/04 and 30566/04, ECHR 2008, §§72 and 76).

12. MPE also permits the reconstruction, minute-by-minute, of a person's life.[10] The reconstruction of where a person goes and what they do has been recognised by this Court as a serious interference with Article 8 (*National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*, nos. 48151/11 and 77769/13, 18 January 2018, §191).

13. **Third**, much of the extracted data will be irrelevant to the purpose of the operation in question. The MPE software that Privacy International has researched has very limited options for selective data extraction, only allowing the selection of very broad categories of data.[11]

14. Further, smartphones and other digital devices are likely to contain significant amounts of information about third parties such as family, friends, and other contacts, accessible through files stored on the phone and through social media applications. MPE therefore does not only interfere with the privacy rights of the individual whose phone is subject to extraction.

15. **Last but not least**, MPE or other forms of electronic device searches are highly invasive for journalists. The contents of mobile phones and other electronic devices can reveal the stories a journalist is developing, with whom they are communicating, including confidential sources, and their specific travel plans. The devices are integral to work of journalists who cannot simply not use or carry these devices when on assignments. MPE therefore threatens freedom of expression and freedom of the media, protected under Article 10 of the Convention.

16. MPE is therefore a highly invasive technique that raises serious potential for interference with the right to privacy and freedom of expression, and therefore requires a particularly compelling justification to be lawful, necessary and proportionate.

(ii) Comparative case law from other Contracting and non-Contracting States recognises the serious interference of digital device extraction with the right to privacy

17. In 2020, the UK's immigration authorities started seizing, in a blanket fashion, the phones of migrants who arrived in the country by small boats and using MPE software to extract and analyse data from the phones. This was performed by relying on immigration search and seizure powers and required phone owners to provide their PIN to immigration officers under threat of criminal sanction.

[10] ICO report, pp. 2-13.
[11] Witness Statement of Privacy International, §§ 81-84.

18. The blanket policy was challenged in the UK High Court, and judgment handed down on 25 March 2022, *R (on the application of HM and MA and KH) v Secretary of State for the Home Department* [2022] EWHC 695 (Admin). During the proceedings, the Secretary of State for the Home Department conceded that the policy was unlawful (for it was blanket and unpublished) and therefore not "in accordance with law" for the purposes of the Convention, lacked a lawful basis under data protection laws, and that the complete extraction of every mobile phone seized did not comply with the Convention or with data protection laws. It further conceded that the practice pursuant to which immigration officers required migrants to provide the PIN for their phones, under threat of prosecution, was unlawful.

19. Following these concessions, the High Court further found that the Secretary of State had breached the Claimants' Article 8 rights as it did not have the requisite powers of seizure.

20. This case, originating from the national courts of a Convention Contracting State, made strong precedent, which established phone seizures and MPE as a significant intrusion in the private lives of those subjected to it. Recognising the widespread illegality that the UK immigration authorities had perpetrated, the High Court ordered in a remedial judgment that the Secretary of State for the Home Department write to the hundreds of individuals who may have been affected by the unlawful policy and inform them of their potential right to redress.[12]

21. A similar action was brought in Germany against the Federal Office for Migration and Refugees ("BAMF"), to challenge the extraction and analysis of asylum seekers' phones in order to verify their identity.[13] Such extraction became authorised in July 2017 under §15 of the Asylum Act (Asylgesetz, AsylG), requiring asylum seekers to surrender all data carriers if they are unable to produce a valid passport.[14] The Berlin Administrative Court, affirmed on appeal by the Federal Administrative Court, found that the blanket analysis of mobile phones at the start of an asylum procedure is illegal, and that authorities must first examine whether less intrusive means of establishing identity are available.[15]

22. Despite the existence of a clear, purpose-made legal framework in Germany to authorise the search and analysis of asylum seekers' phones, the national courts of the Convention Contracting State found that searching asylum seekers' phones required a "good reason to do so", and that it had been in this case neither necessary nor proportionate.[16]

---

[12] *R (on the application of HM and MA and KH) v Secretary of State for the Home Department* [2022] EWHC 2729 (Admin).
[13] Gesellschaft Für Freiheitsrechte (GFF), Refugee Phone Search, https://freiheitsrechte.org/en/themen/digitale-grundrechte/refugee-daten.
[14] Gesellschaft Für Freiheitsrechte (GFF), Race, Borders, and Digital Technology: Submission to the Office of the United Nations High Commissioner for Human Rights on the Reinforcing, Reproductive and Compounding Effects of the Deployment of Digital Technologies in the context of Border Enforcement and Administration (May 2020), https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Gesellschaft_fur_Freiheitsrechte.pdf.
[15] InfoMigrants, German court rejects phone searches of asylum seekers (16 February 2023), https://www.infomigrants.net/en/post/46897/german-court-rejects-phone-searches-of-asylum-seekers.
[16] https://www.infomigrants.net/en/post/46897/german-court-rejects-phone-searches-of-asylum-seekers.

23. These two cases, read together, established the serious interference with the right to privacy that digital device searches constitute, the need for a clear legal framework governing their use in specific contexts (differentiating between a law enforcement and an immigration control context), and the fact that a clear legal framework does not guarantee the necessity and proportionality of the measure. It is therefore crucial to now examine the safeguards required for search and seizure of digital devices to be lawful and compliant with the Convention.

24. The Interveners note that non-Convention states have also recognised the intrusiveness of MPE and found that it violated the right to privacy. For example, in *R v Canfield* (2020) ABCA 383, the Alberta Court of Appeal held that the use of legislation permitting border officials unfettered discretion to search goods as a legal basis for MPE violated the Canadian Charter of Rights and Freedoms ("the Charter"). The Court ruled that phone seizures and MPE breached the Charter rights of privacy and dignity: a conclusion that was reached on the basis of "the massive amounts of highly personal information" stored on mobile phones and the consequent need to protect the "biographical core of personal information" they hold.[17] These findings were endorsed by the Canadian Supreme Court, which refused the government leave to appeal.

(iii) The search and seizure of journalists' digital devices must be subject to significant safeguards to prevent violation of Article 8 and Article 10

25. The Interveners highlight that international and European law recognises that information collected or created for journalistic purposes enjoys a special degree of protection from search and seizure by the authorities. For example, this Court noted the particular significance of journalistic material in the context of the seizure of a journalist's laptop and the subsequent data extraction from it by custom agents (*Ivashchenko v Russia* no. 61064/10, §92). There are various justifications for according journalists' stronger immunity against search and seizure than others. In the first place, there is an obvious risk that the search and seizure can be used as a means to circumvent the protection of sources. A second reason is the 'chilling effect' exerted by such search and extraction operations. Such clearly alarming and intimidating action can have the effect of discouraging the person concerned, or others in the same profession, from continuing their activities, even if those activities are in fact legal. This is highly problematic, especially if the activity in question – practice of journalism - is one guaranteed by international law.

26. The Interveners submit that the above considerations particular to journalists apply in relation to the use of MPE on their devices. The Interveners note that this Court has previously underlined that *"the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests."* (*S and Marper*, §112)

27. Hence, the Interveners submit that a stronger justification for, and stricter judicial oversight over, the search and seizure affecting journalists is needed to prevent unnecessary

[17] Privacy at the border: routine searches of electronic devices breach the *Charter*, https://www.nortonrosefulbright.com/en/knowledge/publications/7ec0dac4/privacy-at-the-border-routine-searches-of-electronic-devices-breach-the-charter.

intimidation of journalists. That particular caution is necessary when targeted journalists – as in the present case - have been investigating alleged wrongdoing by the authorities.

Phone seizures and data extraction must be in accordance with the law

28. Seizing and searching the digital devices of any individual must be subject to strict safeguards to be considered "in accordance with the law" under Article 8(2) of the Convention. In *Malone v. The United Kingdom* (no. 8691/79, §70, 2 August 1984), the Court held that the provisions need to be laid down *"with reasonable precision in accessible legal rules that sufficiently indicated the scope and manner of exercise of the discretion conferred on the relevant authorities"*. Further, in *Weber and Saravia v. Germany* (no. 54934/00, §93, 29 June 2006), the Court stated that *"the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures"*.

29. It is unclear what law the Polish authorities considered applied to the military officers' operations. The Court's communication indicates that it considered that the Code of Criminal Proceedings and Police Act did not apply. Article 217 §1 of the Code of Criminal Proceedings provides that *"[o]bjects which may serve as evidence […] should be surrendered when so required by the court, the state prosecutor, and in cases not amenable to delay, by the Police or other authorised agency."* It is unclear what counts as an "authorised agency". The Police, according to the Police Act 1990, explicitly consists of the *"criminal service, prevention service and the service providing support for the Police activities in the field of organisation, logistics and technology"* (Article 4.1), as well as the *"(1) Higher Police Training School, training centres and Police schools, (2) separate prevention units and anti-terrorist subunits, (3) research and development units"* (Article 4.3). Article 4.4 also provides that other services may be designated as performing functions that fall under scope of the Police Act, by the Police Commander in Chief.

30. Whether the actions of military officers fall under these provisions or not, the Interveners submit that this legal framework is grossly insufficient to govern the searches of digital devices. A law mandating the surrender of "objects" cannot foresee the significant intrusion that a search of digital devices constitutes. Further, any law authorising the search of digital devices must also contain *"a specific procedure or safeguards"* when protected materials, such as journalistic sources, are concerned. None such procedures or safeguards seem to exist in Polish law.[18]

31. Digital devices represent such vast and powerful repositories of information about an individual's activities and relationships that law enforcement authorities have in recent years sought further abilities to exploit this information in their investigations. Digital forensics, including MPE, have therefore exponentially grown in popularity.

32. As technology enabling digital data extraction developed, in some countries police forces started using it outside of a clear legal framework and without relevant safeguards. In the UK for example, Privacy International's research revealed in 2018 that police forces were using this highly intrusive technology in the absence of a legal basis, national guidance or

[18] *Sorokin v. Russia,* no. 40226/02, §49, 30 November 2022.

local policy.[19] Following a complaint by Privacy International, the Information Commissioner's Office issued a critical report on these practices, highlighting the serious risks they pose to data protection and privacy rights, and the need for a stricter legal framework and safeguards.[20]

33. In *HM and MA and KH* (see above, §18), the UK's High Court similarly noted the complete absence of a legal basis underpinning the policy of seizing the mobile devices of asylum seekers. Whilst the reasoning in the Canadian case referred to at §24 of these submissions was premised on a different legal framework, the case also exposes the inadequacy of a legal framework that permitted searches of mobile devices at borders on the basis that they are no different to other goods.

Any interference with the rights to privacy and freedom of expression should be subject to prior authorisation by an independent judicial authority

34. Measures intrusive of privacy and threatening journalists' freedom of expression must be subject to the prior authorisation of an independent judicial authority. This is particularly the case when searches of digital devices are involved.

35. This was confirmed recently in the opinion of the Advocate General at the CJEU in *C.G. v Bezirkshauptmannschaft Landeck* (Case C-548/21), a case that concerned the seizure of a suspect's phone in a criminal investigation involving the seizure of 85kg of cannabis. While the Advocate General concluded that access to information on a phone should not be limited to the investigation of serious crime (provided that access is justified in each case and limited to what is strictly necessary and proportionate), he also found that prior authorisation from a court is required before law enforcement can get *"full and uncontrolled access to all the data stored on a mobile phone in the course of a criminal investigation where those data make it possible to obtain a detailed picture of a person's private life"* (§105).

36. Prior authorisation is even more important in respect of intrusions with both Article 8 and 10 of the Convention, and its standard must be higher, when journalistic material is concerned. In the case of *Sorokin v. Russia* (no. 40226/02, 30 November 2022), concerned with search and seizure warrants relating to the premises used by journalists, the Court concluded that:

> *"[T]he requisite review should be carried out by a body separate from the executive and other interested parties, invested with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not".*

37. As the search of digital devices can be much more intrusive than the search of a home or premises, as set out above, safeguards that apply to the latter must necessarily apply to the former and more. In *Cacuci v. Romania* (no. 27153/07, §91, 17 January 2017), the Court had to determine whether the search of premises (authorised by a warrant) was necessary

[19] Privacy International, Digital Stop and Search (March 2018), https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.
[20] ICO report, *op.cit.*

in a democratic society, and established that the question for it was *"whether the relationship between the aim sought to be achieved and the means employed can be considered proportionate"*, taking into consideration whether a warrant had been issued and what was the quality of this warrant. A similar question must be asked in this case, and the answer should take into consideration the significantly higher degree of interference with privacy and freedom of expression that digital device searches involve.

Any interference with the rights to privacy and freedom of expression should be based on a reasonable suspicion that an offence has been committed

38. Authorisation of the search of electronic devices from an independent judicial authority must be based on a reasonable suspicion that an offence has been committed, not merely the fact that the person is crossing the border. Particularly strong justification for a search and seizure must will be required where persons affected are not themselves suspected of the offence in respect of which the investigation is being undertaken (see e.g. *Ernst and Others v. Belgium*, no. 33400/96, 15 July 2003, *Buck v. Germany*, no. 41604/98, 28 April 2005, *André and Another v. France*, no. 18603/03, 24 July 2008, *Zubal v. Slovakia*, no. 44065/06, 9 November 2010 or *Misan v. Russia*, no. 4261/04, 2 October 2014).

39. The authorisation should contain information about the ongoing investigation, the purpose of conducting it or why it was believed that it would enable evidence of any offence to be obtained, as well as adequate record-keeping of the authorisation given.

40. The absence of these requirement will necessarily entail a violation of Articles 8 and 10 of the Convention.

Necessity and proportionality

41. Finally, a wide range of considerations should be taken to account when determining, whether the conduct of a search was actually proportionate to the aim being pursued and whether the reasons adduced to justify such a measure were "relevant" and "sufficient.

42. The Interveners submit that the volume and the particularly private nature of the data extracted from digital devices require a particularly stringent necessity and proportionality assessment.

43. Extracting all, or even half, of data from a phone will rarely ever be justifiable, as access to the volume and variety of information this entails is unlikely to be necessary to investigate a specific offence. This is supported by the ICO report (see above at §32), which noted that the UK police were regularly extracting disproportionate amounts of data in criminal investigations resulting in the acquisition and retention of excessive amounts of data[21].

44. The Interveners reiterate that in addition to private and sensitive information, in cases of journalists, electronic devices store and transmit large quantity of journalistic material. These might include potentially confidential sources, hence access to them and their exposure threatens the ability of journalists to gather and report the news. It must be considered whether accessing such voluminous information is proportionate to the

[21] ICO report, page 57.

seriousness of the offence under investigation or to the public interest pursued and whether all reasonable alternative measures to protect that interest have been demonstrably exhausted.

Conclusion

45. For the above reasons, the Interveners submit that the search of journalists' digital devices represents a serious interference with privacy and freedom of expression, requiring cogent justification before such an interference can be justified. Further, such search is only in accordance with law where a clear, specific legal framework authorises digital device extractions, and where it is subject to prior independent authorisation based on a reasonable suspicion that an offence was committed. A stringent necessity and proportionality assessment is required for accessing and reviewing such voluminous, private and sensitive information.

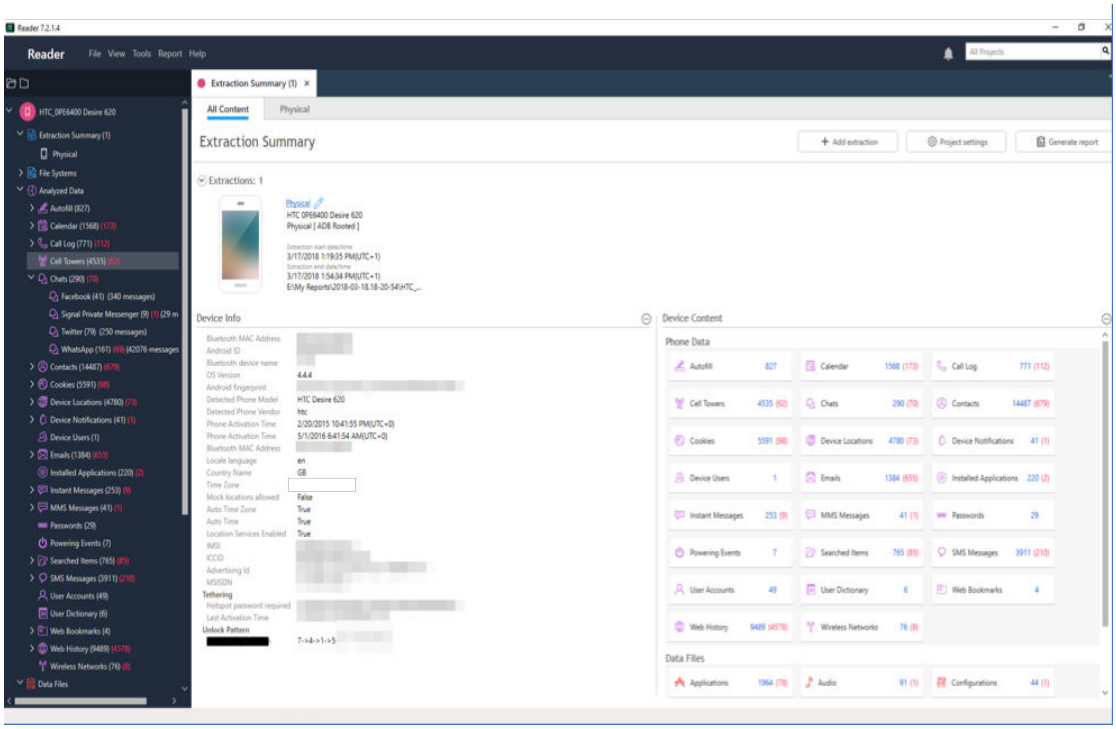
31 August 2023
On behalf of the Interveners

Lucie Audibert
Lawyer & Legal Officer
Privacy International

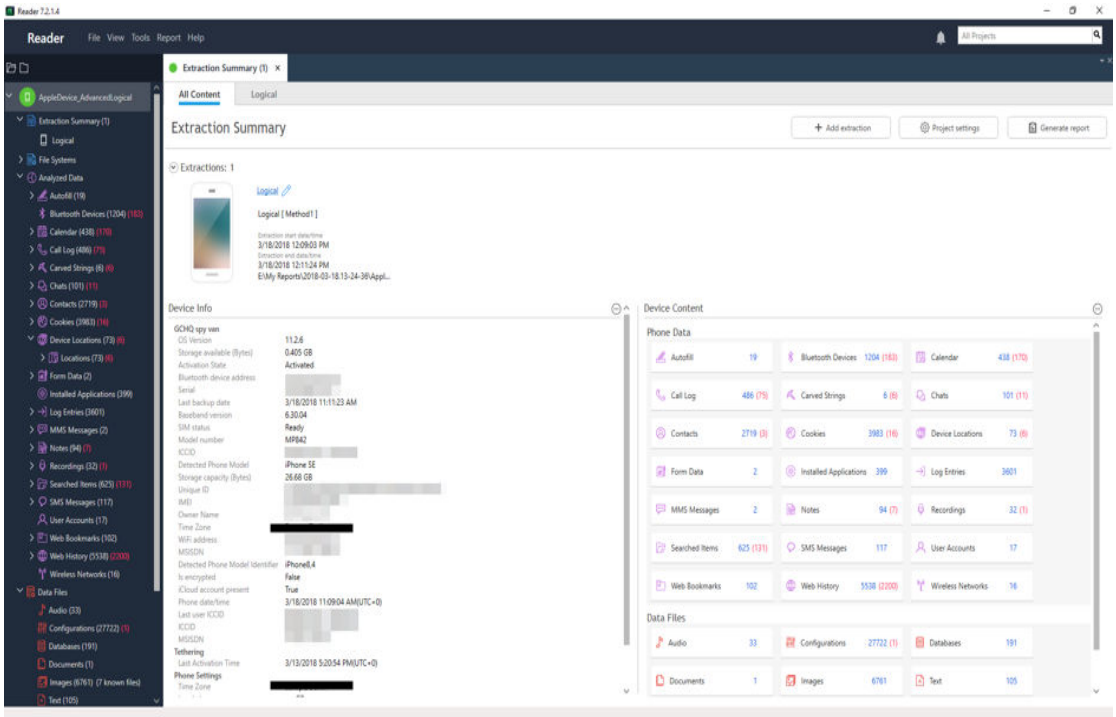
Barbora Bukovska
Senior Director for Law and Policy
ARTICLE 19

Jonah Mendelsohn
Lawyer and Legal Officer
Privacy International

Annex 1 – Cellebrite UFED Data Extraction Visualisation Platform



Summary of extraction of an Android phone (HTC Desire) using a Physical [ADB Rooted] extraction



Summary of extraction of an iPhone SE using a Logical extraction

Annex 2 – List of Data Types Available for MPE

Data Type
Address book (contact names, numbers, email & postal addresses etc)
Call history (dialled, received, missed, duration, date/time)
SMS/MMS messages (contents)
Emails
Web browser history, bookmarks, cache, cookies
Media (photos, videos, audio recordings – often with date/time stamp and geolocation i.e. metadata)
Applications data (which can include social networking data, health & activity data, financial data, bio data, friends and family's movements etc, potentially other sensitive data)
GPS Location data (including historical)
Social Media (as discussed below)
Calendar
User dictionary
Documents (stored locally and on the cloud)
Swipe Patterns
Autofill and keyboard cache
Bluetooth connections
Cell Tower connections
Wi-Fi networks
Deleted data
Metadata and logs