Webinar on extracting data from mobile phones (and the cloud)

FORMOBILE

PRIVACY RULES

Moderators

Denitsa Kozhuharova

Head of Human Rights Department at Law and Internet Foundation (Bulgaria), Member of the Formobile Project

LAW AND INTERNET FOUNDATION
RESEARCH CENTER FOR LAW AND INFORMATION TECHNOLOGIES

Pieter Gryffroy

Attorney at law at Timelex (Belgium), Member of the Formobile Project

TIMELEX

Speakers

Krešimir Kamber

Lawyer at the European Court of Human Rights

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Martijn Egberts

Senior Public Prosecutor for Cybercrime, The Netherlands

NETHERLANDS
PUBLIC PROSECUTION SERVICE

Mike Dickinson

Chief Business Development Officer at MSAB, Member of the Formobile Project

MSAB

Webinar on extracting data from mobile phones (and the cloud)

Table of Contents

Executive summary

PrivacyRules together with the **Formobile Project** had the pleasure to organise an online event which unveiled the intricacies of extracting data from mobile phones and cloud storage.

Denitsa Kozhuharova, Head of Human Rights Department at the **Law and Internet Foundation** (Bulgaria) and **Pieter Gryffroy**, Attorney at law at the law firm **Timelex** (Belgium), both members of the Formobile Project, were co-moderators of the webinar. Denitsa Kozhuharova opened the event by introducing the Formobile Project, an initiative focused on fighting crime and terrorism by supporting the mobile forensics investigation chain. In her introduction, Denitsa touched upon the highlights of the 3-year research and the legal mechanisms that are currently framing mobile forensics across Europe.

Pieter Gryffroy introduced the jurisdictional conundrums of requesting, collecting and processing e-evidence in international investigations, and the right to an effective defence.

Further, **Krešimir Kamber**, Lawyer at **the European Court of Human Rights** (ECtHR), focused on the collection and use of electronic evidence in criminal proceedings from the perspective of the ECtHR.

Then, **Martijn Egberts**, Senior Public Prosecutor for Cybercrime in The Netherlands, presented the legal grounds to access e-evidence and tools for prosecutors and law enforcement to obtain information available on mobile phones and the cloud from a Dutch perspective.

Michael Dickinson, Chief Business Development Officer at **MSAB** which is a member of the Formobile Project, explored the lawful powers and technical competency in the recovery of digital evidence from mobile devices and cloud storage.

Concluding observations have been delivered by **Andrea Chmieliński Bigazzi**, Chief Executive Officer of PrivacyRules.

Denitsa Kozhuharova

Head of Human Rights Department at Law and Internet Foundation (Bulgaria), Member of the Formobile Project

Preliminary findings of the Formobile Project

The Formobile Project consists of 19 partners from 16 countries, including one partner from Asia representing the country of Kyrgyzstan.

The Project is divided in three parts, consisting of tools, mobile forensics standardization and training. Within the legal domaain of the Project, various tasks have been pursued such as: defining the applicable legal and ethical frameworks; and, issuing a comparative report on 30 jurisdictions with respect to criminal procedure.

This comparative report has been conducted by taking into account the fundamental rights at stake in each stage of the criminal proceedings, based on European and national systems approaches.

Although the legal research on mobile forensics is still ongoing, the consortium is already able to map out several findings on the EU perspective on extracting and sharing electronic evidence:

(1) there is little cognizance on mobile forensics, especially on the issue of internal and external storage of data and related jurisdictional conundrums; **(2)** while there are several legal mechanisms applicable to mobile and cloud stored evidence, this rather niche field is yet to be codified in national systems; and, **(3)** due to the above there is little clarity on these legal issues. Therefore, it's not surprising that many practitioners encounter challenges working on the topic of mobile forensics.

The entire research has been built on the premise that the devices at stake, namely mobile phones, were lawfully seized by law enforcement.

Legislation applicable to mobile forensics

An introductory remark is that magistrates, legal practitioners and enforcement authorities are currently applying various interpretations of the already limited international and regional legal instruments in cross-border cases involving electronic evidence. As the law on mobile forensics is rather scarce, States are left with no other option than to recourse to conventional mechanisms and EU directives that are only tangentially regulating the field of mobile forensics. Amongst these are the **Convention on Cybercrime** of the Council of Europe (CETS No.185), known as the Budapest Convention, and the European Investigation Order and other similar ad-hoc mutual agreements between States.

1) The Convention on Cybercrime, also known as the Budapest Convention, which has been effective since 1 July 2004 with 66 ratifications, is the first international treaty that targets cybercrime. While the issue of mobile forensics is not directly tackled by this treaty, it contains several provisions on search, seizure, exchange and preservation of electronic evidence. However, while the treaty is mainly aimed at supporting interstate cooperation and improving investigations in the cybercrime sector, it does not establish minimum standards when it comes to the protection of fundamental rights, simply because these standards are not amongst the main objects of the instrument. Due to this, Signatory States are individually regulating issues linked with mobile forensics. Further, as different States adopt different decisions on a topic which is still unregulated at intranational level, disparate interpretations usually arise. This burdens the assessment of applicable rules in each jurisdiction.

The good news is that the Budapest Convention has been significantly updated by the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence which has been approved on 28 May 2021 by the Cybercrime Convention Committee.

This Protocol is particularly important for the rule of law as it provides, amongst others, legal tools specifically designed to enhance the disclosure, request and provision of electronic evidence, protection of personal information, direct cooperation with service providers, instant cooperation during emergencies and joint investigations between Parties.

(2) Another legal mechanism that could be used in cases involving electronic evidence is the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

While the scope of the legislative act is to enable the application of investigative measures in executing States in order to gather evidence, it could also be applied in cases involving electronic evidence. However, the Directive has only regional outreach, being applied within the European Union. Even so, it has rarely been employed by Member States.

(**3)** Finally, mutual legal assistant treaties are usually concluded on an ad-hoc basis in those cases where the law does not set provisions applicable to mobile forensics or when States decide to complement any legal mechanisms with a set of rules specifically drafted for the case at hand.

Pieter Gryffroy

**Attorney at law at Timelex (Belgium),
Member of the Formobile Project**

Jurisdictional conundrums on mobile forensics

As we have previously mentioned, Denitsa Kozhuharova and Pieter Gryffroy analysed the approach of 30 states on criminal procedural law and issued a comparative report on how they responded and dealt with cases involving mobile forensics. The 30 jurisdictions analysed include all Member States of the European Union, United Kingdom, Norway and Kyrgyzstan . The research for the report commenced from the hypothesis that law enforcement agencies (LEA) are in lawful possession of a mobile device that can be technically examined in its entirety, including the examination of installed apps, such as cloud storage, social media, messages and others.

Starting from this assumption, the national correspondents were asked to what extent LEAs are legally allowed to access data stored on, or accessible through a mobile phone. This is in particular relevant for cloud services which store data externally, but can still be accessed on the phone through an app (with or without having to provide credentials). The Project considered both cases where the location of the data was known and unknown to law enforcement officers. The importance of the research question lies in the fact that by accessing data on the phone that is likely to be stored outside the jurisdiction of the LEA, such agencies could infringe the sovereignty of other States and be in breach of the Budapest Convention.

The most straightforward answer was given to the situation where the data location is available, and based on this, it can be ascertained that the location is within the jurisdiction of the LEA. In this case, while some of the correspondents in the report underlined that service providers ought to be asked for permission, most of them declared that it is typically allowed to access such data.

The answers to the research question is more complicated and divergent when the location of data is unknown or is known to reside in another jurisdiction ,. In such cases, the rule would be to resort to international cooperation, as prescribed by the Budapest Convention.

According to art. 31 (1) of the Convention:

'A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29'.

This means that, in principle,where law enforcement ascertains that the location of data is outside their jurisdiction, the Budapest convention seems to require that they refrain from directly extracting and analysing such data. Instead, LEAs should then use international cooperation or European instruments like the European Investigation Order (and in the future the European Preservation and Production order).. There are two exceptions to art. 31(1): data which is publicly available, and the express consent of the authorised individual enable law enforcement to access, analyse and secure the required data. However, in most cases these exceptions will not apply.

National perspectives on how to approach this issue were divergent.

Countries like Croatia, Latvia, The Netherlands, Slovenia and Sweden reported to be in line with the strict interpretation of art. 31 of the Budapest Convention, in principle refusing to take access to data in the Cloud when it is stored abroad. Other countries declared that direct access to data stored in the Cloud outside the own jurisdiction would be possible, either because of express legal provisions (e.g. Belgium), because of an absence of rules forbidding this (e.g. Cyprus, Finland, Hungary, Luxembourg, Poland) or because of a legal fiction which considers data to be stored locally if this data is connected to a crime for which there is jurisdiction (e.g. Greece, Italy, Norway, Estonia), thereby taking back sovereignty.
Many States declared that in the circumstances when the location is unknown, LEAs will typically access it.

In addition, many countries make a distinction between data accessible/reachable through the phone (e.g. an open app) and data that is on a Cloud service for which credentials are needed or which would require technical circumvention of security. Think of an open whatsapp vs. a dropbox account that is logged out. Even countries which indicate to "always use international cooperation" in a strict application of the Budapest Convention often admitted to acquiring Cloud data because of this distinction (open apps or legally obtained credentials).

Importantly, most of the surveyed countries indicated that if law enforcement would take direct access to data stored in the Cloud in breach of procedural rules or jurisdictional rules, the bar for inadmissibility of that evidence would be rather high, typically requiring that the fairness of the trial is affected.

This challenge will remain relevant even under the new e-evidence rules.
All of this highlights that the territoriality principle of the location of the data may not be useful any longer for determining jurisdiction and for protecting sovereignty, as data location is not always known, can be volatile and moved quickly, or can be inconclusive as data sets can be split over different locations or duplicated in different locations.

Krešimir Kamber

Lawyer at the European Court of Human Rights

The European perspective on mobile forensics

When it comes to mobile forensics, the case law of the European Court of Human Rights is rather scarce, as this area of procedural law is currently under development. Nevertheless, general principles, such as the right to a fair trial and the right to privacy, are certainly applied in any case including those on obtaining evidence from a mobile phone or from the cloud. The rule of law is equally important in these circumstances, as mobile forensics are inherently linked with, inter alia, the right to a private life, respect for correspondence, etc. Consequently, clear and precise provisions are needed in order to respect standard legal order across Europe and to avoid excessive control or intrusive tools from investigative authorities. In this regard, there are several key requirements posed by the ECtHR when it comes to search and seizure of electronic data carriers. The debate mainly evolves around privacy and its potential to shape investigation and prosecution.

The starting point, which is also reflected in the case law of the Court, is that law enforcement officers must have a judicial order which explicitly includes the mobile phone on the list of items to be seized (Bagiyeva v. Ukraine, § 54). Further, the specific act of seizure and search must be documented, enabling a higher authority to follow on the chain of custody of the data which is sought (Wieser and Bicos Beteiligungen GmbH v. Austria). A critical issue posed by analysing data on a mobile phone is represented by the challenge of protecting private information of the defendant while searching for potential evidence in the same storage space.

The case Libert v. France, a case based on internal investigations on a computer of a railway company employee, is an example of this. As the employee was suspected of storing pornographic material on a work computer, the distinction between private information and work-related information arose. In these circumstances, the Court underlined that a defendant must have previously identified private data on his or her computer system in order for it to be protected by additional safeguards, such as exclusion from the search related to infringement of work regulations.

Since the defendant did not go further in identifying the pornographic material as private within the work computer, the internal investigation did not breach any right to privacy of the individual. In another case, Saber v. Norway, concerning mobile forensics, it has been shown that submitting a mirror copy of all the data on a mobile phone to law enforcement authority by the City Court significantly breaches the right to privacy and the right to a private life. The case was particularly sensitive, as the mirror copy contained correspondence between the victim and his lawyer, which was subsequently protected by legal professional privilege (LLP).

To summarise, according to the ECtHR, there are specific requirements that must be met in cases involving mobile forensics. Judicial and law enforcement authorities must have an explicit order containing the right to seize data on a mobile phone. The seizure and search of mobile devices must be properly documented. An individual may be requested to identify the private and personal information before a seizure is conducted, to avoid the compromise of private information. Finally, mobile forensics regulations are especially needed, in order to conduct a smooth investigation and prosecution in such cases.

Collection and analysis of evidence does not typically raise concerns amongst practitioners, being clear-cut most of the times. However, these steps are substantially sensitive in cases of mobile forensics due to the rapid evolution of technology. The right to a fair trial is very much at stake during mobile forensics cases, as it is linked to the admissibility of (mobile) evidence, chain of custody and privilege against self-incrimination. In this regard, there are several safeguards and means that must be considered during pre-trial and trial phases in order to protect the right to a fair trial.

To start with the admissibility of evidence, one must first acknowledge that States usually have different standards when it comes to admissibility of evidence. Therefore, from the perspective of the ECtHR, reconciling the legal systems of the 47 Member States of the Council of Europe poses a real burden. Therefore, the Court came up with a test in its case-law to overcome a potential clash between jurisdictional interpretations. The test has its roots in the Bykov v. Russia; hence it is called the Bykov test. According to this test, the admissibility of evidence should be conducted whilst analysing the quality of the evidence, the circumstances in which it was obtained and whether such circumstances could negatively affect the reliability or accuracy of the evidence. Moreover, the accused must have the opportunity to raise doubts connected with the authenticity of the evidence.

In the same line, domestic courts are expected to sufficiently support their decisions. Another aspect to be borne in mind is the chain of custody, since the Court raised the issue of admitting evidence which could not be verified as originals went missing (Horvatić v. Croatia; Khodorkovskiy and Lebedev v. Russia, § 702; Beraru v. Romania, §§ 76-81).

Access to vast amounts of electronic data is an additional issue pertaining to mobile forensics. A couple of ECtHR cases have demonstrated that the defence must be involved in determining what data could be relevant for disclosure (Sigurður Einarsson and Others v. Iceland, § 90; Rook v. Germany, §§ 67 and 72). On top of that, it is also imperative that the defence team is allowed to consult the evidence to be able to prepare their defence (Sigurður Einarsson and Others v. Iceland, § 91).

Violating the privilege against self-incrimination also interferes with the right to a fair trial. To regulate this, the Court introduced the Saunders formula, according to which the privilege against self-incrimination does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing (Saunders v. United Kingdom [GC], § 69)

Martijn Egberts

Senior Public Prosecutor for Cybercrime, The Netherlands

Solving mobile forensics cases in The Netherlands

Going back to the importance of data location and its power to determine which jurisdiction is applicable, National Prosecutor Martijn Egberts emphasised that the general approach of the Public Prosecutor's Office is to attribute jurisdiction to The Netherlands in a Dutch criminal procedure against an inhabitant of The Netherlands in those cases in which location is either unknown or the data is stored on multiple servers, rendering it impossible to determine the principal location. This is, of course, on the basis of principle of territoriality and/or principle of active personality. Therefore, investigative judges and police officers are advised to extract data stored on cloud services, based on an explicit order which includes the device, but only in cases in which there are legal grounds to extend the search for E-evidence to other computer devices, such as servers. These are cases in which judicial authorities or police officers realise that they have to search additional devices. In these cases, provided that they are authorised, they extend the search to such devices/servers. This is only possible if the accused is an individual authorised to use all the devices included in the seizure warrant. This means that one can only extract and secure evidence from cloud storage accounts to which the accused has access.

While this is one of the interpretations advanced by other States too, it has been acknowledged that the mobile forensics field requires proper codification.

The biggest issue in the field is that laws on computer-based crimes, electronic evidence and computer systems were drafted in a period where external storage was absent. Cloud services were not yet on the market, but when they appeared, judicial authorities were left with no other option than to apply general rules of mobile forensics cases. Fast-forward to contemporaneity and we might be surprised to find out that a vast majority of cybercrimes are, in fact, committed using data stored entirely on the cloud. Taking into account the unfolding area of mobile forensics together with cloud services, we must ask ourselves a further question: is the practice of search and seizure of cloud-stored data foreseeable for individuals? In other words, could defendants reasonably foresee that even if they store their data on a cloud service, police officers could still legally obtain it based on application of general rules?

As prosecution service we indeed think that this is foreseeable for individuals because the rules and conditions that apply before we can violate the right of privacy or correspondence are clearly stated in our criminal procedure. The exact way we obtain that E-evidence depends – unfortunately- for a big part on technological developments. Additionally, states across Europe often do employ quite disparate interpretations on extraction of evidence from the cloud.

The issue of sovereignty is further complicating the area of cloud and mobile forensics, an area which is already quite complex on its own. The best way to illustrate how sovereignty is further challenging national authorities is to take a look at how they could obtain data stored on the cloud services offered by tech giants, without knowing the location of the data. Sending a production order to the headquarters of a big tech company that will extract the evidence from a server they host in a third country, will technically also produce a breach of sovereignty of that third country. However, what is important to underline is that issues of sovereignty should not aid criminals, as the purpose of sovereignty is to protect the internal autonomy of a State, as opposed to playing the role of shield for culprits.

Furthermore, as lawyer Krešimir Kamber previously conveyed, a balance between privacy and the right to a fair trial is particularly important in cases involving the extraction of evidence from mobile devices. Often, in the investigation process, LEA and practitioners are put in a situation where they must ensure that they gather all possible evidence, without violating individuals' privacy. Striking this balance when one seizes a mobile phone is quite sensitive and prosecutors must plan in order to make sure that they do not access more data than the scope of investigation requires.

What is important to underline is that at times prosecutors and police officers simply do not know what they are looking for at the beginning of an investigation. This situation often leads to a decision to analyse and secure everything from a seized phone. However, by analysing the type of crime committed, law enforcement is usually able to redirect the search to certain types of data. They might decide to search all the data produced within a certain timeframe, or they could only focus the analysis to a certain type of data, either photos, messages, emails, etc. Employing this method, agents could limit their intrusion in the personal life of individuals.

Another good advice is to decide prior to the search what types of information you are looking for and how are you going to search it. Another useful practice could be to put the device on flight mode in order to ensure that you are only accessing information stored on the internal storage of the device. In cases where authorities do not know yet what they are looking for, it is advisable to make a forensic copy of the content on the phone, select the data you need and get rid of the data you don't need. As we have seen, judicial and law enforcement authorities do need further clarification in many of the issues posed by mobile forensics.

Mike Dickinson

Chief Business Development Officer at MSAB, Member of the Formobile Project

Mobile Forensics Technology

Mike Dickinson offered the perspective of mobile forensics technology, pointing at the rapid change in the technology business and how the legal world has a hard time in keeping up with it. Fortunately, there are certain tools that could help prosecutors and police officers to comply with the right to privacy and the right to a fair trial, while still enabling them to conduct a complete and effective investigation involving mobile phones. A related effective tool has been developed by **MSAB,** a company which studies and develops mobile forensics technology used for mobile device examination. This kind of tool is forensic in nature and multipurpose, meaning that they can be employed either by prosecution, defence and witnesses in criminal investigations, but they can also be used in non-criminal circumstances. The way in which it works is that it provides a digital scientific truth on the type of data at hand, which often contributes to proving people innocent. Additionally, such tools are built with required data security protections, and forensic audit logs according to standards set up by the European Union. The technology deployed is powerful and this is why, outside the EU, MSAB is particularly vigilant to who it supplies this technology to, as certain stakeholders could employ it for unethical purposes. Such control is important to make sure that technology developers are fully supporting and comply with fundamental human rights.

Mobile forensics technology could offer great help to national authorities and law enforcement agencies, especially in cases where one must balance the need to gather all the evidence on a device and the need to respect the right to privacy. At the beginning it can be incredibly difficult to determine what data one will need throughout the whole investigation. Experience shows that authorities often keep certain amounts or types of data, even if it is unclear whether they are going to be needed at the outset. However, these practices are not always welcomed in the European sphere. On this account, the selection process poses a technical, operational and legal challenge. Simply because the act of deleting data is attached to a great risk which could harm the parties in a criminal case. One could end up missing or deleting data that could prove the defendant innocent.

MSAB has developed a good practice technical implementation which could help national authorities in their search: they usually gather all the data on a mobile device, however, they are only delivering to the requesting authority a subset of the relevant data collected. Employing this method, specialists in mobile forensics are able to decide which data is private or sensitive, forwarding only a package of relevant information to the investigators for analysis and decoding. There are different extraction techniques available to recover data from a mobile device. One benefit of a logical extraction which interacts with the operating system of a device, is that it can be directed to search only for specific types of data, or specific timestamps. This method is very commonly used, as it complies with data privacy and proportionality standards; nevertheless, there is always a degree of technical risk, as one cannot fully rely on logical extraction to recover all possible data. Often other methods need to be deployed such as physical extraction, where it's not possible to restrict data acquisition in advance and often entails additional manual search and analysis by authorities.

Conclusion

This PrivacyRules webinar explains how crucial it is that mobile forensics become thoroughly regulated and that such regulation will be opened to rapid adaptation to fast-paced evolution of technology. At this moment in time, virtually all crimes present at least one element which is committed through or documented via computer systems and, especially, mobile devices. Judicial authorities, law enforcement agencies and practitioners agree that extracting data from mobile devices is, on many levels, a sensitive step in criminal investigations. In addition, cloud storage is further complicating the balance that needs to be stroked between the right to a fair trial and the right to privacy. Considering the growing use of cloud storage in criminal activities, one could even argue that cloud forensics may become a brand-new field that needs to be analysed and possibly regulated. In depth analysis and practice related to the Second Additional Protocol to the Council of Europe Convention of Cybercrime, will determine a sure amelioration of the various interests and rights at stake.

By Cătălina Gemănari, Legal Intern
PrivacyRules Cybercrime and Fundamental Privacy Right Committee

Cleared by Andrea Chmieliński Bigazzi, CEO, PrivacyRules Ltd.