communication@formobile-project.eu
Linkedin – Formobile-project
Twitter – @Formobile2019
www.formobile-project.eu

Criminals' smartphone – friend or foe?

Contents

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

communication@formobile-project.eu
Linkedin – Formobile-project
Twitter – @Formobile2019
www.formobile-project.eu

Introduction

IDC Research shows that 80 % of the respondents reach for their mobile phones within the first 15 minutes after they wake up. Similarly, 74% check their phones about 15 minutes before going to sleep. The functionalities that smartphones offer have made their popularity even greater than laptops (86% of respondents answered that they owned smartphones while 71% have laptops). As phones have become an inseparable part of people's lives, we are constantly collecting and receiving information - taking pictures, sending and receiving text messages and emails, finding driving directions, accessing the Internet, playing games, watching videos and listening to music.

Many of these activities track users' actions, and the actions of the people around them. This is equally valid for the regular citizen as it is for the criminal. Supported by research, this theory is closely connected with the decline in crime rates. Even as early as 1990 - 2000, when mobile phones were not so commonly used, they were claimed to be one of the factors for the decline in homicides. Nevertheless, the development of new technologies has undoubtedly supported police authorities but also criminals.

Despite the fact that phones know all about the person using them —where they go and when, who they talk to, when they are using it, there are a number of apps coming out that use encryption to provide anonymity to their users. This makes the data accessible only through digital forensics software. Therefore, the digital world has become a field of battle between extracting information from criminal minds through their phones on the one side, and concealing it with new tools and applications on the other.

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

The relationship between mobile forensic evidence and the law

The law has always had to keep up with how technology develops and evolves, but never more than now. As the guardian of people's rights and freedoms, it must constantly ensure that new and emerging technologies do not violate them in any way. After all, the use of mobile forensics by law enforcement in practice, while undoubtedly contributing to the fight against crime, involves a plethora of issues - from what data is being accessed to who has the right to access it, and what the required steps to follow are to ensure that the extracted evidence is actually going to be admissible in court. This means that the required procedure, depending on the national context, must be followed, including seizing mobile phones by the book and establishing a chain of custody for the evidence being obtained from it – for this reason indicating who has authorised use to the data and establishing a clear audit trail are a must.

Of course, Law Enforcement Agencies (LEAs) also need to follow the applicable human rights legislation to be certain that the rights of all involved in the criminal proceedings are respected – this includes the victim and any witnesses, but also the accused suspect.

The most relevant human rights to be protected in the mobile evidence context are the right to a fair trial (including the principle of equality of arms), the right to presumption of innocence, the right to privacy and the right to non-discrimination. On an EU level, each of these rights is enshrined under the Charter of Fundamental Rights of the European Union.

Also, when we talk about mobile forensics, it is inevitable that personal data - **including sensitive personal data** - is involved. While the General Data Protection Regulation (GDPR) made quite a splash in the EU legislative pool in terms of strengthening personal data protection measures, especially with the hefty fines imposed under its remit for non-compliance, the focus is on another piece of EU legislation that is relevant in the context of personal data processing by competent authorities during criminal investigations – namely, the **Law Enforcement Directive**.

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

communication@formobile-project.eu
Linkedin – Formobile-project
Twitter – @Formobile2019
www.formobile-project.eu

Similar to its 'cousin', the GDPR, the Directive complements its provisions and also bases itself on the key principles of processing, which include the need for a legal basis; making sure that only the data needed for the processing and for the required purpose is actually processed; that the data is appropriately deleted after a certain period of time; that it is securely stored so that it is not lost or stolen etc. The Directive also requires a clear distinction to be made between the different categories of data subjects for the purposes of data processing, i.e. suspects, convicted, victims and witnesses, respectively.

Following this, it becomes clear that in practice, the law allows LEAs to use forensic software to acquire data for the purposes of an ongoing criminal investigation, however the above-mentioned safeguards must be duly observed and followed at all times. However, this is easier said than done as witnessed, for example, in the two Apple vs. FBI disputes which were effectively described as walking the line between privacy and security and - as technology continues to develop- such debates are invariably going to continue in the future.

Mobile phones – the best detectives in criminal matters

The application of mobile evidence has proven to be profoundly valuable on a number of occasions, from simple thefts to terrorist attacks and organised crime. What is more, with the constant upgrade of mobile devices, which makes them more and more sophisticated, LEAs can nowadays use them to extract a greater amount of information pertinent for their investigations than they were able to at the turn of the century.

Despite the fact that their approaches may differ, a noticeable number of crimes have been resolved thanks to the developed forensic tools.

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

For example, the acquisition of data from mobile phones belonging to low-level smugglers in illegal wildlife trade in Thailand, and the subsequent extraction of relevant information, allowed the law enforcement authorities to connect them to the notorious kingpin of the wildlife trafficking ring 'Hydra', Bach Van Hoa, and led to his eventual detention and conviction after more than 10 years of evading authorities.

Mobile forensics were crucial in finding Bulos 'Paul' Zumot guilty of killing his girlfriend at the time, Jennifer Schipsi, and setting their home on fire with her body inside in the Palo Alto murder case.

This was made possible as both the victim and the accused were frequent iPhone users. The police authorities were able to track their respective locations prior to the incident, and recover their deleted messages, which proved their turbulent relationship and Zumot's unsuccessful attempt to establish an alibi.

Cell phones Take the Witness Stand - Dramatic Palo Alto murder case hinges on iPhone evidence

During the Coachella festival in California, Reinaldo De Jesus Henao, 36, stole more than 100 smartphones. The reason the police was able to detect the devices and him was the Find My iPhone app available for every iPhone around the world. The lack of knowledge of some criminals can easily lead to their unproblematic and prompt arrest. A similar result, although by a different approach, was achieved in the case of Joshua Kaufman, whose laptop was stolen in 2011. Mr. Kaufman had installed software known as Hidden, which provides the computer's location, photos taken on the Mac's internal camera and shots of the screen display. Once the thief started the laptop, the program immediately began sending the owner photographs with the criminal's face as well as a screenshot with logging details for an e-mail account. Based on this information investigators later lured him into an arrest.

There are many examples of such cases where the criminals knew too little about technologies' abilities, which led to their imprisonment. However, mobile forensic evidence has also proven to be effective in organised crime environments. An example of this is Operation Greenlight/Trojan Shield,

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

created by Australian police and the FBI in 2018, which was one of the biggest penetrations and takeovers of a specialised encrypted network. It is claimed by the authorities that during this operation there were 12,000 infiltrated devices – providing insights into 300 criminal groups in more than 100 countries. That was achieved by paying a sentenced drug trafficker to provide them access to a phone that he had customised, on which he was installing ANOM, (also styled An0m), a secure encrypted messaging app. The next step was selling the phones to organised crime networks through underworld distributors. The tracking of messages from the encrypted app resulted in arresting over 800 suspects around the world, and confiscation of millions in cash, 30 tonnes of drugs, and arms caches.

Gaps and problematic areas that come with the benefits of mobile forensic evidence

Despite the undeniable benefits that mobile forensic evidence offers to criminal investigations, there is one huge aspect that practice shows to be sometimes neglected – the privacy of society and innocent people. The fragile balance between the fundamental right to a private life, and the power of the rule of law seem to be changing on a case-to-case basis. An example for this is the project of Google – Sensorvault. In 2009, the company launched the Location History option, a feature for users who wanted to track all the locations where they had been. Sensorvault stores information on anyone who has agreed to use this option, allowing regular collection of data from GPS signals, cell phone towers, nearby Wi-Fi devices and Bluetooth beacons. The data in the database is held indefinitely, unless the user decides to delete it. In the USA, warrants can be issued that allow police authorities to require information from these databases. Technology companies have for years reacted on such court orders for specific users' information. The new warrants go further, indicating possible suspects and witnesses in the absence of other traces. Frequently, Google employees said, the company answers to a particular warrant with location information on dozens or hundreds of devices. In addition, they said that the company received approximately 180 requests in one week, however, Google declined to confirm precise numbers. It is vague how frequently these requests have resulted in arrests or convictions, due to the fact that many of the investigations are still active and it is not uncommon for judges to seal the warrants.

Yet, one more large-scale example are the EncroChat arrests, which was a year's long joint investigation carried out by France, the UK, the Netherlands, Sweden, Norway, Europol and Eurojust,

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

resulting in hundreds of arrests across Europe after the French police was able to intercept the network's messages in 2020.

EncroChat: European authorities compromise phone network to arrest 'untouchable' criminals in sting – Euronews.

The law enforcement authorities in the UK, where more than 700 individuals were arrested and £54 million seized, together with 77 firearms and two tonnes of drugs, have since called this the biggest UK crackdown on organised crime in history. The EncroChat mobile service was a Europe-based encrypted communications network, modified to exclude features such as cameras, microphones, GPS and USB ports in order to provide robust security and anonymity to its 60,000 users, which was also naturally perceived by criminals as a safe heaven. Nevertheless, while the garnered media attention was commendable and mostly siding with the police authorities, legal concerns were also raised on whether evidence was lawfully obtained, on its admissibility and integrity. Also, privacy and human rights concerns were voiced, especially since not only criminals were users, but also businessmen, politicians, journalists, lawyers, celebrities and ordinary individuals seeking enhanced privacy and security of their communication.

Another problematic area is the validity and truthfulness of the mobile evidence. For example, call detail records are generated by cellular network providers, providing details about the calls, text messages, and data usage of a cellular network subscriber. An approach used by many police authorities is conducting analysis of this data. Therefore, there is an expanding market for software tools that support and speed up the process. Many commercial software tools allow modification or import of the data, which is consequently presented in court. The users of this software are only required to know how to use it and not in fact know how to conduct an analysis. When an automated software analysis of call detail records is conducted, the best practice is for an expert to critically evaluate the results. If an employee does not have the necessary knowledge to do so, inaccuracies are not impossible to occur. Another probable mistake is cell phone location evidence. An article in the New York Times says that more than 10,000 court verdicts are under review in Denmark due to the incorrect analysis of cellular call detail records by Danish authorities. Similarly, the Guardian states,

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

"The system has also linked phones to the wrong masts, connected them to several towers at once, sometimes hundreds of kilometres apart, recorded the origins of text messages incorrectly and got the location of specific towers wrong". This issue is also interrelated with the fact that a ''digital gap" persists between IT forensic experts on one hand and the legal practitioners (judges, prosecutors and defence lawyers) on the other, which in practice means that lawyers are often over reliant on the forensic experts' reports without themselves fully understanding the nature of the data extracted. In this regard, the work that the EU-funded **FORMOBILE project** is currently aiming to achieve must be noted, namely a complete forensic investigation chain targeting mobile devices. For this purpose, it has set up the development of a CEN Workshop on Requirements and Guidelines for establishing such a chain, as well as on a Digital Evidence Checklist to be included within it for lawyers to use in order to ensure the reliability, admissibility and validity of digital evidence, thus finally bridging this 'digital gap'.

FORMOBILE: From Mobile Phones to Court – An EU Project Helping To Keep Citizens Safe

The above-mentioned risks further shake the reliability of mobile forensic evidence, however, they do not undermine their general contribution to criminal investigations. It is arguable whether all the aspects and hazards that come up with such evidence are openly disseminated to the general public, enabling them to be fully informed when providing their personal information to their mobile phones. However, the benefits that mobile forensic evidence offer to the criminal investigation process are unquestionable, despite the risks that come up with them.

Conclusion

Taking into account all the aspects mentioned above, one question arises – is the number of arrested criminals thanks to mobile phones greater than the number of crimes that they facilitate?

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

There are 6.4 billion smartphone users worldwide who trust their phones to carry information regarding all aspects of their everyday lives. This results in a vast amount of data, available to different types of parties with the right knowledge and tools.

Mobile phones provide equal opportunities to law enforcement authorities and criminals. The only aspects that offer one of the sides an advantage over the other are the technological abilities, and knowledge one has. Therefore, this *'game of phones'* is the constant battle between the law enforcement agencies and the criminal, which has transferred partially into the digital world.

Both parties use different tools to be ahead of each other, relying on the information provided by the general public. Although voluntarily given, this data is used beyond its initially planned purpose to which the people have agreed when it is being accessed during lawful investigations or cybercrimes. Such actions interfere with the people's rights as data subjects laid down in the Law Enforcement Directive. However, it could not be argued that the usage of data collected from mobile phones is not useful in criminal investigations and that it has not decreased crime rates in some instances. The benefits that come with the availability of such amount of data have been decreased profoundly by the intervention in the privacy of people. Nevertheless, in many instances, data extracted from mobile phones has led not only to arrests but also prevention of robberies, murders and even terrorist attacks.

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800