Your smartphone is one of the most important threats to your privacy. Do you agree with this statement? Why? Is there anything that the GDPR can do to help you mitigate that threat?

Being able to transform mobile computing into the ability to perform everything a desktop computer can, smartphones are one of the most important devices in our lives. They have become our best assistants in accomplishing everyday tasks that would otherwise be much more time-consuming, even impossible. Counted our steps? Kept our notes? Navigated us wherever we wanted? Measured our heart rate? Suggested to buy something we were just talking about? And so it gets a bit scarier as we keep mentioning the variety of tasks we trust our smartphones to do. Essential as they might be, our mobile phones pose a lot of privacy risks, as they can be turned into surveillance and tracking devices without even spoiling their functions.

From the physical threats to the web-based ones, there are a variety of security risks that can affect our smartphones. Let us start with the physical threats. We carry our mobile devices everywhere with us. But are we aware of the potential danger that can be caused by a lost or stolen device? This is probably one of the most common mobile threats. Except for the fact that the hardware itself can be resold on the black market, a smartphone is precious mostly because of the sensitive personal information it may contain.

However, with the advancement of technology, nowadays it is possible to encrypt the data such that the phone and therefore our privacy remains protected in the above mentioned events of a lost or stolen device, or even when we trade for a new smartphone. Therefore, one might argue that the physical threat is recently no more a potential risk. Here it is worth mentioning that even though the encryption of our data is absolutely a necessity, the privacy threat will always remain considering the existence of what is called ‘broken cryptography’. The phenomenon of weak or unfamiliar encryption algorithms is not to be neglected here. Any committed attacker can take advantage of the vulnerabilities to crack passwords and gain access. Even for highly secure encryption algorithms other ‘back doors’ are left open that limit the algorithms’ effectiveness.

Here we come to another potential risk caused by what we referred to as ‘back door’, or all of our data to be accessed whenever it is wanted to. This issue became specifically significant in Apple's encryption battle with the government. Specifically, the concern arose in 2016, when FBI demanded that Apple help it break an iPhone's security concerning a terrorist attack. After this event, it was deduced that the government wouldn't even need Apple to build a back door into the iPhone. In this case, if such skill is used to prevent attacks and save lives, it could be acceptable, even necessary. But it will always be a concern that an ability to be able to access all data from a smartphone could at some point fall into the wrong hands and cause potential damage.

Another category that will be discussed is the threats that come from different applications we install on our phones. It is enough to remember here all the times we were asked from an app to allow access to our camera, microphone, location, photos, or contacts. While there are applications that allow you to give access to specific data and at a specific time, there are others that don’t even have these features. For instance, while there are many photo editing apps that allow you to choose only a specific photo or video you want to edit, there are many others for which you need to allow access to all your photos in order to be able to edit one. Same idea even for the apps that want to use our location. While there are apps that ask to use location only once, or while your are using the app, there are many others that force us to totally enable location in the settings in order to perform the needed task. In some cases, we don’t pay enough attention to these programs as there is some part of our personal data that we don’t consider it dangerous even in case of security leaks. We even ask sometimes what benefits would our location or profile photo can give to another person. What if it can send

unwanted messages to our contact list? What if instead of the location, this app can access our banking accounts? There are many types of applications that can even give an attacker complete control over someone's device. Many others collect or use private information without our knowledge or consent. We may not think that our birthday or photo can cause any harm to us, but there are cases that the stolen information is used to steal one's identity or for financial fraud. Such an example would be an app developed in 2016 that used smartphone sensors to guess PINs and therefore access a bank account. By analyzing the device's movement, this app could accurately determine 99.5 percent key combinations when tested for relatively small samples. In such cases, managing app permissions and trying to not download applications that are not approved by an app store is absolutely crucial.

Something that is also a concern nowadays is the ability to have internet access everywhere. This leads to the threats that come from the network our device is connected to. The happiness when finding a free Wi-Fi network should always be followed by the fear of what could happen to our privacy if we connect to it. Wi-Fi tracking for instance is something many businesses use to determine what the users like the most in order to alter their offers and business direction accordingly. There are other networks that once connected, they can install malware or spyware on our devices without our knowledge. The same can also happen with web-based services. There is potential damage that even the downloading of a simple picture or song can do. Many web-pages open pop-ups and automatically download an application on a smartphone. Simply by visiting an unsafe web page, one can provoke a browser action that can install malicious programs on the device.

Something that is also worth mentioning here is the fact that different from our desktop computers, smartphones don't have such a variety of antivirus software applications that could protect them from unknown networks or apps. VPN connection is something we should consider here. Since the information going to a VPN server is encrypted, using it when we connect to a public Wi-Fi or when we try to download something from a rather suspicious web-page, helps in protecting our privacy and keeping a secure connection.

After this outline of some of the most potential dangers coming from our smartphones, and some ways we can rely on to help us prevent them, we must not forget a crucial point. We are not alone in this struggle to protect our personal data. We can always rely on the law to interfere when our privacy is threatened.

Specifically, the General Data Protection Regulation can help us regain control over our personal data. Let us list some of the articles that protect our privacy in the battle against smartphone security threats. Firstly, we can mention a point in article 5, stating that "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures." A number of mobile risks can directly violate this principle. We have mentioned some typical examples above: malicious apps that could be integrated so deeply that they cannot be removed from the device even with a factory reset, and provide unauthorized remote access, cause catastrophic data loss, or transfer data to other devices or servers. We mentioned before that it is safer to download applications that are approved by an app store. But there have been many cases when a malicious app has passed the security tests of Google or Apple and found its way to a smartphone. In these cases, it is the device provider's responsibility to ensure security for the user's personal data.

Another part that should be discussed is article 6, concerning the lawfulness of processing, protecting personal data from being processed without our consent, followed by article 7, mentioning the conditions for consent. I would like to focus on the fact that the consent should be easy to withdraw, the data subject shall be informed thereof, and that the consent should be presented in a manner which is clearly distinguishable from the other matters and should

be freely given. This regulation is also very important, especially in the terms and conditions we need to accept in order to have an account, or allow an application to make changes on our device or to have access to our information. Therefore, we can rely on GDPR for poorly explained contracts, use of many technical terms, and especially the need to accept a condition that requires our data even when this information doesn't concern the application or is not necessary for the performance of the contract. Moreover, concerning the right to withdraw consent, since in many applications it is very difficult, in some even impossible, to undo some actions, like giving permissions to access our location for example, GDPR helps us to acquire such feature and protects us from the apps that don't have the option to withdraw our approval.

The right to rectification, mentioned in article 16 of GDPR is also needed to defend our data in case of possible attacks that might have altered it. Since the data subject has the right to obtain from the controller the rectification of inaccurate personal data, this means that we can regain control of our data if our device has been tampered with and our personal data is changed. The right of access by the data subject in article 15, stating that "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed" is also crucial when a third party, whether legal or not, wants to collect our data. Additionally, as explained in article 21, GDPR also ensures that the data subject has the right to object at any time to processing of personal data concerning him or her for the mentioned purposes. This right helps us as smartphone users to not allow our devices or different programs or networks to process our data, and therefore penalizes the controllers that either don't give us a choice or neglect our objection.

Information to be provided where personal data are collected from the data subject (art. 13) is also significant. It is crucial to know what happens to our data and why a device, or a program, or an application needs to collect that specific information. That is the question we need to ask ourselves whenever we encounter a controller requiring part of our personal data we would rather not give, or that might not be appropriate or necessary for its function. An example would be an application that requires our bank information, even though, providing a free version, it does not seem to be mandatory to subscribe for the pro (paid) edition. According to GDPR, the data subject has the right to acquire more information concerning "the purposes of the processing for which the personal data are intended as well as the legal basis for the processing".

There are many other articles that can help against the smartphone privacy risks, but we need to keep in mind that the law helps us to the extent that we allow it to. This means that the GDPR ensures to protect our data in cases of injustice or attacks, but it cannot protect us from a contract we sign without reading, or a term we agree to before thinking what it might cause. In the vast area of the threats coming from the usage of mobile devices, it needs to be discussed also the fact that there are threats we cannot always anticipate or prevent, for which the law can interfere, whether it might save our data or not. But there are also many other threats that come from our negligence or misunderstanding, like a saved password somewhere, an app downloaded from an unreliable source, a permission given by mistake or just because it would have been more time-consuming otherwise, and many other points for which everyone needs to be careful of. We know for sure that the security dangers presented by the usage of our smartphones will probably never be enough to stop us from using them, or from believing that their benefits are much grater than the above mentioned disadvantages. To sum up my opinion, we need to be careful with our data and try to prevent as many security threats as possible. We need to protect ourselves where the law cannot be involved, and help the law protect our data when it can.

Worked by:
Romelda Blaceri