Chapter 7
Use of Apps for Crime Reporting and the EU General Data Protection Regulation

Christina Charitou, Dimitrios G. Kogias, Spyros E. Polykalas, Charalampos Z. Patrikakis, and Ioana Cristina Cotoi

Introduction

With the number of Internet enabled devices (e.g., a smartphone, a tablet, a wearable or a laptop) highly increasing, so does their role in every person's daily life. Through the use of a call, an instant message, a post on social media or even real-time video communication, users can easily use their smartphone to report an event, ask for assistance or provide information about their status, allowing the provision of faster and more efficient safety services. To this end, community policing has come to be considered as a new and improved mode of policing by many countries in the past years.

In general, this new approach includes an increasingly active role of civilians in community policing which firstly includes to assist the police in creating improved relations with the communities they serve; and secondly, yet not unrelated, to make policing the responsibility of all members of a community which in turn should serve to decrease the level of crime in their society. In order to achieve this, the police service and communities need to have close working relationships with one another based on trust, transparency and a shared concern for safety, peace and stability. To facilitate the communication, the use of smart apps in Crime Reporting appears to be a fast and effective way of getting citizens engaged.

C. Charitou · D. G. Kogias · C. Z. Patrikakis (✉)
University of West Attica, Electronics Engineering Department, Egaleo, Greece
e-mail: charitou@puas.gr; dimikog@puas.gr; bpatr@puas.gr

S. E. Polykalas
TEI of Ionian Islands, Digital Media and Communication Department, Kefallonia, Greece

I. C. Cotoi
Engineering Ingegneria, Informatica, SPA, Lecce, Italy
e-mail: ioana.cotoi@eng.it

G. Leventakis, M. R. Haberfeld (eds.), *Societal Implications of Community-Oriented Policing and Technology*, SpringerBriefs in Criminology,
https://doi.org/10.1007/978-3-319-89297-9_7

It goes without saying that police departments routinely collect information, while police reports include intimate details about victimization and other personal events. At the same time, the use of mobile applications in crime reporting will definitely lead to an increase of personal data collection and processing. These applications demand access to the user's personal data and information (e.g., location at the time of reporting via the embedded GPS sensor in the smartphone) for their efficient performance. By providing this access to his/her personal data, the user consents on the collection, storage and process of their data, hoping that this will be done in the frame to which he/she provided his/her consent.

But the sharing of certain consenting sensitive information is not, always, a bad thing. Especially when there are specific applications that aim at helping the user to increase the feeling of security in his/her everyday actions. Such applications are developed for smartphones, wearables and the web, in TRILLION (TRILLION Project 2017), that targets to enhance the role of community policing. The citizens will use the application both to report such events (e.g., vandalism actions in a concert, scenes right after an earthquake) in order to inform and update the LEAs about the conditions at the reported place, but also to communicate with registered users asking for help in crisis situation. To prevent any misuse, the personal data that are collected should follow the new regulation from the European Parliament, taking place from 2018, regarding the collection and process of personal data from the mobile applications.

To this end, Section 2 will try to describe the efforts that aim to enhance community policing (mainly in recent Security projects), while Section 3 will focus on the European GDPR and the way it affects the mobile applications Section 4 will describe the TRILLION use-case and how the applications that are developed for its performance can meet the new requirements, without affecting the TRILLION's system performance. In the last section, a conclusion about the noticeable points of this paper will be presented.

Related Work

The new data protection framework is based on the assumption that personal data processing is lawful only if this data is processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law: legal obligation, performance of a contract, vital interest of data subject or a third person, public interest or legitimate interests of the data controller or third persons. The GDPR preserves the purpose limitation principle as central element of the legal framework stating that data should be collected for specified, explicit and legitimate purposes and - principally - should not be processed for incompatible purposes. The Regulation confirmed the principles of accuracy and purpose-related duration of storage. Of utmost importance for a proportionate processing in the context of community policing is the data minimisation principle, which must be taken into consideration by the designing of the system.

Many solutions, that enhance the role of community (or neighborhood) policing, have been developed and applied lately with increasing interest and participation from the users. Next Door (NEXTDOOR n.d.) is an upcoming application that encourages the citizens of a neighbor to subscribe in an online system where they can register their neighbor and form a social network to circulate news. Xpose (Xpose n.d.) is another recent solution that manages to combine more modern social network features in an effort to provide for efficient reporting of hazardous situation.

Recent Security Projects that are funded by the European Union under the HORIZON 2020 program aim, also, to enhance the role of community policing. To achieve this, some of them decided to develop a mobile application for two-way communication. INSPEC2T (INSPEC2T Project 2017) targets to develop a specific application for dissemination and gathering of real time information from the police to the citizens and vice versa. CITYCOP (CITYCOP Project 2017) is another project that has the similar scope and aims to create a system of combination of mobile application and on-line portal. On the other hand, UNITY (UNITY Project 2017) is a project that aims to develop and provide a community policing model in which citizens and police will have an effective and practical cooperation, based on the development of a communications technology.

GDPR and Mobile Applications

Internet connectivity in recent years is characterized by "3E" (Everywhere, Everytime, Everything). That means that people are willing to connect to the Internet from everywhere (home, work, entertainment etc.), at every-time (working days, weekends, day, night etc.), with every-thing (pc, tablets, smartphones, smart TVs, wearables etc.). The daily necessity for Internet connectivity is accompanied by an increasing demand for applications in order to cover all aspects of user's needs. Thus, millions of applications are available online, the majority of them requires access to data stored in user's devices. The data stored to user's devices usually are correlated with user information such as name, age, gender, location and several other personal information.

Millions of mobile applications are available from several online web-stores, while the relevant market is characterized by duopoly since the two main players, Google Play and Apple Store, have a large portion of the market in terms of mobile apps availability.

In Google Play store the available mobile apps are provided either free of charge or paid and are organized in several categories. In each category, mobile apps are further grouped by Google taking into account the popularity, the date of release, or user preferences. In (Polykalas et al. 2017) researchers analyzed a sample of the most popular, free of charge, mobile apps provided by Google Play store, in order to examine the type as well as the extent of personal data access required by mobile apps. It was found that the majority of the examined mobile apps (84%) require

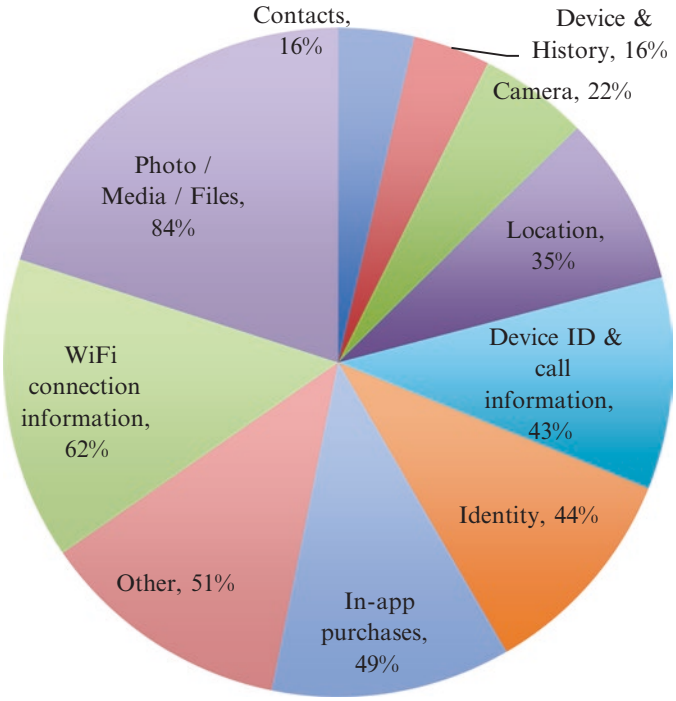

Fig. 7.1 Required access type by mobile apps

access to the data type "Photo/Media/File", while more than half of the examined mobile apps require access to "Wi-Fi connection information" (62%). "In apps purchases", "Identify" and "Device ID & call information" type of access follow with 49%, 44% and 43% percentage of the examined mobile apps, respectively Fig. 7.1.

For users who are willing to get more informed about the types of access, Google provides a short description of each type of access. For the most popular type (Photo/Media/File) is mentioned that: "*An app can use files or data stored on your device. Photos/Media/Files access may include the ability to: Read the contents of your USB storage (example: SD card), Modify or delete the contents of your USB storage, Format external storage, Mount or unmount external storage*". In practice this type of access, allows mobile apps to get access to almost all files or data stored in user's devices, while overlaps several other categories, explaining in such a way, the high popularity of this type of access among the rest types. Adopting the assumption that the sample of the examined mobile apps (10 most popular apps in each category – total 529 examined apps) is representative of all mobile apps available in Google Play store, it could be argued that there are more than 2.2 million of apps in Google Play store, which require access to almost all files stored in user's personal devices.

The rapid increase of online connected personal devices has brought new challenges to policy makers in relation to the protection of personal data. To this content

a new Regulation was approved and published by European Parliament, aiming to the protection of EU citizens' personal data from unlawful collection, storage and processing of personal data. In (Spyros 2017) the new framework laid down by the Regulation is discussed giving emphasis to the procedures that an online mobile app store or/and a mobile app developer, should follow in case that the provision of a service/application, requires personal data storage/collection/processing. The Regulation imposes as a fundamental precondition for any personal data process the existence of user consent. In addition, two basic principles are imposed in relation to personal data privacy: the data minimization and purpose limitation. Data minimization refers to the correlation between the extent of personal data collection/processing and the purpose for which are collected. Purpose limitation refers to the transparent and explicit determination of purposes in which personal data are collected/stored/processed. Last but not least, the Regulation introduces more strictly rules in cases of minor users. In particular, if users are under 16-year-old then the process of personal data is lawful only to the extent that the person who has the responsibility of the minor has given his/her consent for the processing of minor's personal data.

Coming back to the discussion in relation to the current procedures followed in Google Play store and taking into account the main principles introduced by the GDPR several inconsistences could be highlighted. First of all, it could be argued that, the current procedures are not in compliance with the two main principles of Regulation regarding data minimization and purpose limitation. In particular, as discussed earlier, the majority of mobile apps require access to almost all files stored in user devices without an appropriate justification regarding the necessity of this type of access. In addition, it is not clear the correlation between the purpose of personal data collection and the extent of personal data access. Furthermore, the current procedures are not in compliances with the new rules in relation to minor protection. More specific a user under 16 is currently able to download and install in his/her personal device a mobile app, which require access to minor personal data without the consent of the person who has the responsibility of the minor.

TRILLION Mobile Applications

With TRILLION aiming to use state of the art technology to encourage the action of community policing, the use of mobile phones and wearables will play a very significant role in this effort. Location information, device info, access to media files and time-stamp of the data are some of the information that might be shared with when a TRILLION mobile application is used by a citizen or LEA. Taking under consideration, the sensitive and personal nature of these data, TRILLION's performance will be highly affected by the new European GDPR.

In TRILLION, each user in order to enter in the application should register with his/her credentials; therefore, an account should be created. The reason is both for feedback on the status of a submitted report directly to the interested user, but also

to avoid any false alerts by identifying users that are misleading the LEAs. In addition, TRILLION will support hidden identity reporting by using a special architecture that manages to hide the user identity if he/she selects this kind of communication with the LEAs, providing also end-to-end encryption to increase the security of that communication. To achieve this, the TRILLION platform architecture will include a two-step anonymization process, which is described in (Chatzigeorgiou et al. 2017) in more detail.

On top of this, TRILLION will allow the users to send media files attached with their reports. The user will be allowed to select what should be included in their report and, apart from a short text description of the event there is no obligation as to including any attachments and/or upload a media file. As a further privacy enhancement, photos that will be taken from the application to be attached in a report (an option that will prompt the users to access the camera and take a photo will be included) will not be included in the phone's gallery and, therefore, if the phone falls in the hands of a malicious user, then he/she will not have access to them.

But for TRILLION to work efficiently and according to the regulation, detailed descriptions and/or instructions as to the reason the applications needs to access specific sensors and data should be provided to the users. Prompt messages should also be included to ask for explicit access to specific sensors and their generated data, e.g., the camera or the GPS signal of the smartphone. Those requests should be followed by details about how these data will be processed by TRILLION, in an effort to help for the efficient and smooth operation of the system, but, also, to encourage the user to permit the access. Furthermore, the user should be given the opportunity to query about and verifying that the data have been used for the described purpose and report if something is not working as it is supposed to. The above described functionality, designed for TRILLION's mobile applications, shows that they can comply with the lawfulness, fairness and transparency, data minimization and purpose limitation principles described in the GPDR and will allow them to work efficiently under the upcoming changes in the regulation.

On the other hand, as far as the protection of minors is concerned TRILLION demands the user to specify his/her age during the registration in the system, but up until now, no specific mechanisms have been adopted based on the received information.

Conclusions

In this paper, we investigated the compliance of the GDPR with the mobile applications in Google Play, in an effort to check the readiness of the today digital era and that of the IoT ecosystem with the changes that are described in GDPR. We have found that the majority of applications will not comply with the strict requirements of the GDPR, showcasing a large security gap in the existing regulation. Also, by using TRILLION as a use-case, we presented the mobile applications designed for

it and their compliance to the new regulation. The results have shown that following the security by design technique can lead to create applications that can comply, in a very large degree, with the new European data protection regulation and, at the same time, achieve the necessary operations to perform efficiently and with great results.

Acknowledgements This work is funded by the European Commission under grant number H2020-FCT-2014, REA grant agreement n° [653256]. The support is gratefully acknowledged.

References

Chatzigeorgiou, C., Toumanidis, L., Kogias, D., Patrikakis, C., & Jacksch, E. (2017). A communication gateway architecture for ensuring privacy and confidentiality in incident reporting", in the 1st International Workshop on the Internet of People and Things (IPAT 2017), June 7–9, London, 2017.

CITYCOP Project, HORIZON 2020, https://www.citycop.eu/. Last accessed at September 2017.

INSPEC2T Project, HORIZON 2020, http://inspec2t-project.eu/en/the-project-2. Last accessed at September 2017.

NEXTDOOR. (n.d.). The private social network for your neighborhood. http://nextdoor.com

Polykalas, S. E., Prezerakos, G. N., Chrysidou, F. D., & Pylarinou, E. D. (2017). Mobile apps and data privacy: when the service is free, the product is your data, In proceedings of IEEE/IISA 2017, August 2017, Larnaca Cyprus.

Spyros, E. (2017). Polykalas, assessing EU framework for personal data privacy: Is the end of "take it or leave it" approach for downloading apps?, in proceedings of 7th international conference on social media technologies, communication, and informatics, October 2017, Athens Greece.

TRILLION Project, HORIZON 2020, http://trillion-project.eng.it/#/. Last accessed at July 2017.

UNITY Project, HORIZON 2020, https://www.unity-project.eu/. Last accessed at September 2017.

Xpose. (n.d.). https://xpose.tv/howitworks