Engineering Privacy in Mobile Health Systems

Leonardo Iwaya (Karlstad University), SWITS'2016

Mobile health (mHealth) applications have the potential to improve and dramatically change the ways of delivering healthcare. Nevertheless, like any service or product that deals with the collection, processing and use of personal data, mHealth solutions have to comply with statutory data protection regulations. The problem naturally appears when various stakeholders (app developers, app stores, device manufacturers, and other service providers) are failing to attend such legal demands, raising concern about infringements of customer's privacy. In this summary, we discuss the privacy issues of mHealth, also directing players towards practical ways tackle this problem.

In brief, mHealth results from the parallel evolution of technologies in mobile devices, sensors, computer networks and communication. Thus, when we talk about mobile health we can refer to a quite broad number of applications, ranging from wellness and fitness apps that can be used to track your daily exercises to real-time remote monitoring systems for high-risk patients. In other words, this gigantic umbrella term covers quite many different apps, which also means that their privacy assessment will have to be made case-by-case.

Breaches of leakages of health data can cause embarrassment and discrimination. The disruption of communication channels can prevent patients to receive appropriate healthcare in an emergency situation. The huge amount of generated data has to be transmitted, processed, and then stored. Viable solutions tend to use cloud computing to solve this problem. That requires and unprecedented level of coordination among healthcare institutions and cloud service providers (like Google and Amazon), in order to ensure trust in these systems. Lastly, regulations and legislations to protect personal data and ensure individual's privacy are still ongoing processes; and new areas such as mHealth will certainly demand further debate.

As one might have noticed, achieving privacy in mHealth requires interdisciplinary knowledge. Privacy-preserving mechanisms should be designed within a specific healthcare application context, following a specific legal frameworks, and making use of proper information security measures.

Information security is commonly addressed by means of the principles of information confidentiality, integrity, and availability. Privacy, in turn, stands for fundamental rights and freedoms of subjects to have their right to privacy with regards to the manipulation and processing of personal data. As a human right, privacy has precedent in the right to freedom of opinion and expression, which includes freedom to hold opinions without interference and to seek, receive and communicate information and ideas through any media and regardless of frontiers.

Privacy Infringements

There are a few main reasons why developers or health managers fail to implement privacy into their solutions: (a) they tend to focus on system's functionalities from an end-user perspective, forgetting privacy requirements; (b) they believe that privacy is an optional/added-on feature that can be later implemented; (c) they are unaware about existing legislations and regulations; (b) the task of implementing and configuring of privacy mechanisms is complex, i.e., easy to get it wrong.

For large companies, that are well-equipped with computer experts, lawyers and consultants, such privacy infringements would perhaps not happen. It's more a matter of reviewing their existing policies, procedures, and practices to ensure compliance. This situation, however, is flagrant in developing countries that are using mHealth solutions in small scale and pilot initiatives. For

instance, the Haitian government demanded that the public health organizations working in the country hand over the medical records of all patients infected with HIV. Their aim was to create national database to track the prevalence of HIV among Haitian citizens. This was a quite disconcerting case, since there are no guidelines defining how this database may be used. Not to mention the possible discrimination and violence that may result from misuse or data leakages from such database. As a result, such actions negatively affect the trust in ongoing mHealth programs for health surveillance and treatment adherence.

There are other cases of mHealth application that allow pregnant women to enroll in the system and receive by SMS updated prenatal care information, reminders about doctor's appointment, and so on. In this case, it is important to understand how mobile phones are practically used in developing countries. Not seldom the phones are shared among family members, and perhaps owned by the mother, father or any parental figure. Pregnant teenagers could become hesitant to enroll the program, because they might feel bad, ashamed or even afraid to talk about it with all family members.

All in all, communities with unserved or under-served healthcare, that could most exploit the use of mHealth might also be the most threaten by the possible privacy violations.

Privacy by Design

The concept of Privacy by Design (PbD) is probably the most remarkable example on how to address privacy in the ever-growing world of information technology. Developed in the 1990s, its objective is to take privacy into account throughout the whole systems engineering process. To do so, PbD utilizes seven foundational principles: (1) privacy should be dealt in a proactive and preventive way; (2) it should be in the system's default mode, and, (3) embedded in the system's design; (4) it should not trade-off with functionality; (5) the whole lifecycle of information processing should be secured; (6) its mechanisms should be visible and transparent to the users; and, (7) consistently respecting users privacy.

In the 21st century, the concept of PbD has spread in various related fields of research and legal frameworks. A notorious example of PbD's incorporation is the European General Data Protection Regulation (EU GDPR), replacing the EU Data Protection Directive 95/46/EC, which intends to strengthen and unify data protection for individuals within the European Union. The GDPR was recently adopted by the European Parliament, and it will enter into force in the very near-future. Its provisions will be directly applicable in all member states by Spring of 2018.

It is worthy mentioning that the EU GDPR has been enormously influenced by academia, being able to represent the state of the art research on privacy and data protection. Most countries outside EU, however, still lack such legal frameworks.

Engineering Privacy

Nonetheless, to translate law into code isn't simple. Legal frameworks still remain in a quite high-level. Developers need more accurate information regarding how to engineer privacy into their systems. PbD principles are mostly "*too vague*", displaying a disconnection between policy makers and engineers when it comes to how to technically comply with privacy and data protection. Also, the complexity of the engineering task can rarely be reduced to an easily ticked checklist; it requires deep analysis and understanding of the system in order to properly mitigate associated privacy risks.

In order to close this gap between privacy principles and software implementation, we need application-specific guiding tools. In other words, such tools should make it easier to the developers to: (1) get acquainted with privacy and data protection rules, (2) to understand possible privacy threats in a given mHealth context, and (3) to advise appropriate countermeasures.