Open Society Foundations - Armenia

POLICY ANALYSIS

THE SCOPE AND TERMS OF PROCESSING OF PERSONAL DATA

Scope and terms of processed data. The Law on Personal Data says that personal data could be collected only with the consent of an individual or in case foreseen by a law. However, lawmakers never consider limitation of data collected for even legitimate purpose, e.g. they never ask themselves is that data necessary to achieve the purpose it is collected for. *Terms of personal data storage and control over the government owned data.* Legitimate collection of data does not mean that it may be stored timeless; it must be destroyed when the purpose of its collection does not exist anymore. However, a few legal provisions providing access to personal data or granting right to collect such data define terms of its storage. The law is missing mechanisms for verification and inspection of unnecessary personal data stored by the government bodies.

One of the global privacy issues is the storage of users generated/entered data in corporate/public administration systems. Most of private companies adopt communication policies that enable them to store and review users generated data (emails, phone call logs and even in some cases conversations). Usually, such policies do not contain provisions regarding terms of storage and purposes of use of such information/data. In some cases it has been the request of celebrities who has been taken photos they do not want to retrieved, in some other cases people who has been released from penitentiary institutions demanded for removal of information that prevent them from seeking rehabilitation (applying for job, home lease).

Legitimacy and fairness of data collection and processing

The entire legal framework of the personal data protection is based on lawful and legitimate purpose of collecting and processing others personal data. Article 5 of the EU Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data states that personal data must be collected and processed fairly and lawfully, which means that it is based on legal requirements (such as, for example, the law on national census or citizens registry) and even if there is not legal requirements/rights to collect personal data compulsory it must be done with data subject's consent excluding some cases of so called sensitive data which could be processed only on the ground of the law.

The concept of fairness is not that obvious and often is very subjective. If a travel agency collects data of travelers for arranging their trip (transportation and lodging), apparently, it will collect a solid amount of data required to book a flight: name, age, number of travel document. Even more data might be required for hotel reservation: usually also name, age and passport data, but could also include some preferences such as traveling with pets (not all the hotels allows to stay with pets), chose between smoking/non-smoking rooms. Food preferences could be collected for both flight and hotel booking (kosher, halal, vegetarian). At the same time travel agent may request other information that client is willing to tell because he/she/they expect to provide all what will help to find a better travel option. Additional information may include frequency of travel, transportation and destination preferences, and other information that may look like relevant to the requested services, but not be as such. All this information is provided voluntary and stored by travel agent and, according to the law, should be destroyed as soon as it will not be necessary for the purpose it has been collected.

The above example demonstrates typical unfair collection of data through the manipulation of clients's willingness to provide information for better service. Some bank account managers may ask clients how much he/she earns or does a client has savings and justify that by the purpose to offer better services. Client may not be willing to tell it to any other service provider, but sometimes does because the banks are usually trusted institutions and client thinks they would not ask something which is not legal to ask and to know.

Apparently, only a relatively small part of the population is well aware about the information state or private organization may ask. Moreover, not all the people willing to start a dispute over the question asked by public

official or bank managers especially if the later suppose to make a decision on their inquiry or application (application for a loan or a public resource). Most of the people assume that the officials must strictly follow the rules; however, the officials may sometimes ignore rules for the corporate interests.

As an example of ignorance of the rules for corporate interest could be marketing research that bank managers carry out, but within the scope of rules, i.e. ask client's consent prior to asking question. However, some managers may want to demonstrate better performance and ignore the rule. Other managers may follow successful colleagues and the rule will be completely ignored with low risk of revealing the irregularity: all what client may do just refuse to answer the questions, and only negligibly small number of clients would report violation.

Personal data collected by banks and credit organization are often criticized, most frequently in the USA, less in the EU and very frequent in countries of Eastern Europe. Most of the banks require credit applicants to grant the crediting organization with a right to request personal data from the third party, sharing client's credit history with other banks and processing it for the purse of credit risks managing. This is unique situation which is quite similar in the most of the countries around the world; a person may terminate its contractual relationships with a bank, but his/her data will be kept forever.

Notably, in many countries (including Armenia) terms of data storage by credit bureaus is not defined and most of them keep credit histories throughout the client life. This is one of the contradictory concepts of the baking regulations that in spite of legitimacy do not compliant with the spirit of internationally accepted values of personal data protection. It is bright example when corporate lobby (banks and crediting organizations) promot rules that are not actually might be explained by public interest.

An example of abusing citizens rights by public officials while carrying out legitimate function are rare in traditional democracies, but very often happened in newly emerged democracies. For instance, while visiting households social workers may ask several questions about living conditions and also about willingness to vote on forthcoming elections or what a person thinks about current political leadership. That could be always hidden as a kind of human conversation out of protocol and many people willing to do so.

Another example could be visit of police officers in charge for a particular area (neighborhood inspectors that exist in some post soviet countries). While asking questions to ordinary citizens on their fully voluntary consent, police officer may ask question about the neighbours including: "Are your neighbors sociable", "Do they usually attend community events", "Do they go to vote on elections", etc. People get especially nervous when answering questions asked by police or detectives and most likely will not resist to answer, while police officer may have an order from political governor of the district to "survey" political mood around.

The above examples are typical abuse of fairness of obtained data. Moreover, some of them could be classified as manipulation. However, unlike illegal collection of personal data, unfair collection is very hard to reveal and even harder to prove: "data processor" can always refer to human conversation he/she have out of protocol. The only prove of unfair use in mentioned cases could be records of interviewing people and/or records of interviewed people and both evidences are very unlikely to be obtained by Data Protection Authorities, as well as very unlikely interviewed people will report irregularities.

One of the measures for combating unfair collection and storage of data is raising public awareness about the right not to answer questions which are not defined under the law and/or not relevant to services offered. Data Protection Authorities' hotline may be another measure for the prevention of unfair collection of personal data. However, as mentioned, collection of evidences and administrative proceedings related to unfair use of personal data are extremely difficult and require very high qualification of data protection officials, as well as sufficient level of awareness of the population.

Apparently lawful and fair approach is should be equally applicable to both collection and processing of personal data. The above examples might demonstrate fair and unfair use of exactly the same data. In case of above described travel agency legitimately collected (with customer consent) personal data might be used solely for offering best travel options to the customer or could be additionally used for profiling customers for further promotion of services or other marketing purposes.

Similarly public officials may collect data in a legitimate way, but process it illegally, i.e. for the purpose other than data have been collected or unfairly. For instance, social workers record people with limited mobility and use it to predict level of elections participation. This would be non-legitimate use of legitimately obtained data.

Unfair use of fairly and legitimately obtained data is not obvious. For example, a mobile operator collects data for provision of services and gets some (or every) subscriber's consent to process data for marketing purposes to provide better services and offers. Instead the operator process data to find level of consumption and use it for adjusting the tariffs in a way to get maximum profit. Another example is use of consumers' data by mobile operator to predict possible migration to its competitor (switching to other service provider) and use selective customer retention measures, i.e. propose special offers to keep.

Terms of storage

Another issue that actually missing in data protection legislations of many countries is the terms of data storage. Article 5 of the EU Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data says that personal data must be "preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored". In practice personal data is stored for much longer, and in majority of cases the only reason for that is absence of proper control and/or procedures.

Most of the CoE member states merely replicate these provisions without expanding the requirements into more practical framework to define specific circumstances that might be interpreted as a purpose for personal data collection. For instance, an interactive TV service provider may collect personal data for the purpose of providing certain services, but also use it for marketing to find out preferences of auditorium, etc., which is legitimate and almost fair use of data assuming that it is for the purpose of better serving the auditorium. After termination of the contract, the provider may keep data justifying it with possible claims from the customers.

The issue of terms of personal data preservation by public institutions is even more complicated due to the fact that nowadays information systems are often centralized and used for different purposes. Thus, for example, car registration database might be shared with other governmental institutions for other related purposes (subsidiaries, tax declaration, etc). However, it may happen that even after change of car ownership records about previous owner might (and most likely will) remain in the register database. It is relevant to ask a question: what is legitimate purpose of the preservation of complete history of car records?

Terms and conditions of storing user generated data

One of the specific phenomenon of information society is the massive data generated by users. Social networks, cloud storages, online stores and many other elements of digital economy and virtual social life are rich raw materials for commercial and political marketing. Most of people do not read terms and conditions of such services and even if some of them do, companies often change contracts without a chance to negotiate amendments and most of people are so dependent on cloud services and social networks that have no chance to reject an amendment even if it is not acceptable.

It is worth to note that even when a user of social network or cloud service unsubscribe from it he/she may not be sure that all the data have been deleted. Moreover, many social networks and cloud services preserve data explaining that by the interest of customers that may one day decide to reactivate their accounts or may found they need some information from their electronic archives. Apparently, data in cloud storages may contain personal data and other privacy information.

Processing of cloud base data and social network account is a very serious problem of global character. No one may guarantee that a provider of cloud service or owner of social network would not process stored data without consent of data subject. In fact, major cloud and social network service providers such as Google and Facebook process records of users with formally purpose of offering them better services. The fact that users asked to grant access only for processing flight details or appointments does not mean that the service provider does not process information of users' mailboxes, location services and other privacy related information for marketing purposes.

The more innovative service is, the more unexpected privacy threats it may contain. One of the brilliant examples of innovative services with potential privacy threats are Uber, Airbnb and food delivery services. Mobile taxi services have access not only to individuals' local data, but also to regular routes and even life preferences (more frequently visited restaurants, shopping areas and leisure areas, etc.) Any information that users themselves provide to that services, as well as the information collected by those services is stored for unknown period and might be used for the purposes other than it obtained.

One of the main challenges for global services like that is limited power of the national authorities to inspect and enforce providers of global services to comply with the national legislation. Chine is an example of rough and very radical compliance enforcement, but the country does not has an independent judicial, and state priorities are always override interest of private business and individuals. Russia requires providers of all online services available on its territory to keep personal data on the territory of the country thus creating mechanisms for the enforcement of the national rules for use of foreign services. Small countries, however, do not have a chance to force global providers to comply with national legislation without a risk of isolation even if such legislation is a part of international legal instruments such as Council of Europe Conventions or multi-national treaties.

Proposed actions

- Study practices of unfair collection of data by private and public institutions especially in relation of political preferences and civil activities.
- Study the level of public awareness about data protection rights, right to refuse to provide illegal or irrelevant data, as well as advocacy projects aimed at building public awareness about personal data protection rights.
- Public awareness campaigns aimed at educating wide categories of Internet users (especially youth and minors) about potential threats of storing personal data and other private information in cloud services.

Author: **Andranik Markosyan**
Digital rights expert
Email: andranik@gmail.com
November 2016

Publication of this policy analysis is supported by Open Society Foundations - Armenia. The opinions and analyses expressed in the paper are those of the author and do not necessarily represent opinions and positions of Open Society Foundations – Armenia.