Open Society Foundations - Armenia

POLICY ANALYSIS

BULK DATA COLLECTION

Bulk data collection and storage (street cams data, public and private surveillance cams, telecommunications data, public registers and archives)

Introduction

Collection of publicly available data is a rapidly penetrating phenomenon, which emerges parallel with such public services as street cameras, public and private surveillance systems, mass usage of personalized telecommunication devices (mobile phones and smartphones). Not all countries address this issue properly, however, most of the European countries has national regulations restricting the use of such data for purpose other than it supposed to be used. The Armenian legislation is mostly missing regulation on collection of bulk data. In spite of recently adopted car traffic regulation related legal acts foresee legitimacy of data obtained using street cameras, they does not stipulate legitimacy of use of cameras for other purposes, as well as do not define requirements towards the storage and usage of video archives.

Personal data massively collected by public and private institutions on legitimate bases, but without further control over it usage and destruction is another area of possible uncontrolled abuse of privacy. Very often individuals voluntarily provide data without actual knowledge whether it is mandatory, legitimate or it is an indirect abuse of power by a public or private institution. And a special area is specific category of data stored by public service suppliers, which technically is not classified as personal but contains valuable information about private life of individuals.

Video surveillance

From common point of view collection of bulk data using either technical means or voluntarily provided by data subjects does not cause serious privacy issues. Moreover, video surveillance and supply of personal data to service providers is not always and not in any jurisdiction is treated as personal data. However, street cameras have been a subject of public concern, public discussions and official guidelines of European authorities. Speaking about video surveillance issues different categories of video surveillance should be considered. European regulations usually have different approaches towards the issues of public security surveillance, hidden surveillance cameras, private community and private individual surveillance systems.

The main concerns regarding the street cameras are usually the scope of surveillance (e.g. what supposed to be subject of monitoring: specific activities in a specific time, any activity, any person or just unusual activities), for how long time video recordings might be stored, who may have access to stored video resource, what is the procedure for getting access to stored surveillance videos. Notification regarding the video surveillance is a mandatory practice formalized in operational plicy procedures or implemented as a industry ethical rules in most of European countries. Meanwhile, regulation may also include legitimate purposes of surveilling a public place and relevant limitations.

Video surveillance is done not only by public but also by private institutions for security and monitoring purposes. In particular, several companies use video cameras for monitoring working processes or just presence of employees at workplace. In some companies employees are aware about the monitoring systems, but in some are not. Even in companies where employees are aware about presence of video surveillance they usually are not informed for how long videos are kept, who may get copies and if there are limitation for the usage of the video materials by the administration.

Apparently, shortly after mass use of video surveillance, the issue has become a subject for discussion by the legislatures of the European countries and EU institutions. In spite of the adoption of a harmonized data protection

legislation at the EU level (EU Privacy Directive 95/46/EC), specific national regulations of video surveillance have been adopted prior to the adoption of the Privacy Directive and the rules imposed under these regulations are not that simple as it seems they could be. In several European countries (France, Germany, Netherlands) mass surveillance requires permission of public authorities granted on the ground of justified public purpose or privacy protection.

The relevance of surveillance to personal data protection is not that obvious. The strongest argument of those who insist that video surveillance and security out of data protection regulation is that video recording not always could identify a person while the basic definition of the personal data is linked with identification. Such approach could be right and wrong depending on jurisdiction and on ability of surveillance system to identify a person. Though, today CCTV (close circuit television) systems provide very high quality recordings, and modern image processing systems are capable to identify person by picture. The issue is not that obvious as in case of collecting biometrical and/or biographic data, but much more sensitive in terms of scope and probability of potential abuse of others privacy rights.

Potential privacy threats of video surveillance are not limited to identification of persons though. Video surveillance is a powerful tool for recording variety of information about a person, such as, car license plate (state register) number, tracking individuals' regular routes, personal contacts and several other elements of private life which usually is not allowed to monitor without court decision. The threshold between monitoring of public area and hidden video surveillance is so vague that in several court cases disputing parties have to spend dozens of arguments to convince courts to consider a particular monitoring a lawful/unlawful interference to an individual's private life.

It is not surprising that European Court of Human Rights has received several claims concerning the violation of Article 8 in regard to the use of CCTV. Thus in one of the cases (Perry v. the United Kingdom), the Court noted that there had been no indication that the applicant had had any expectation that footage would be taken of him in the police station for use in a video identification procedure and, potentially, as evidence prejudicial to his defense at trial. That ploy adopted by the police had gone beyond the normal use of this type of camera and amounted to an interference with the applicant's right to respect for his private life. The interference in question had further not been in accordance with the law because the police had failed to comply with the procedures set out in the applicable code: they had not obtained the applicant's consent or informed him that the tape was being made; neither had they informed him of his rights in that respect.

Use of hidden cameras, either private or public, is also a whole story of debates in legislative between those politicians who support the right of private community or individuals to protect his/her property by all possible means, including video surveillance and those who believe that any interference in others life, even in public places, might be undertaken only with consent of the person monitored.

Registers, archives and public services

Administrative bodies often collect personal data on the ground of a legitimate purpose. For instance, local authorities collect relevant data for property tax register purposes that must be destroyed after such data is not used for the purpose collected. However, most of the records are kept irrespective of their necessity just because no adequate controlling measures are in place. Tax and custom declarations, car and other property registers, social security and pension reforms - all these registers contain enormous quantity of personal data which have been stored legitimately and might be retained for several years in almost all countries even without actual knowledge of individuals.

Archive is a special category of data storage where personal data protection and other privacy laws are face an issue of freedom of information - getting information of public interest. In most of the European countries public archives adopt general guidelines of codes of ethics that guide employees when opening historic information containing someone's personal data, which might be subject to protection under the data protection legislation. In new democracies these issues might be even more sophisticated due to authorities unwillingness to open some archives to public.

Bulk data collection by public service suppliers is usual and normally targeted to identification of users. Though, the data is usually does not contain much information about users private live, but, if properly processed, it may reveal several information of personal nature. Thus, energy consumption during the day (produced by many smart counters) may tell how much time user spent at home and at which time. Travel information may tell a lot about an individual's personal life (preferences and accompanying people) and even nature of his/her job. Accumulated information could indicate income category (low, medium, high income) and many other characteristics of an individual. Postal services may store information about senders/recipients of the letters and packages, as well as the type of goods or periodicals a person receives.

Theoretically, information which is out of use (not necessary for purposes it was collected) must be destroyed, but public utilities companies may store it and justify storage by a legitimate purpose, for instance, payment history, protection against client claims related to provided services or other similar purposes. Special category of such services is credit bureaus that store individuals credit histories without time limits. There were several problems with correct recording and storage archives of credit data recorded on both European and US credit markets and several scandals of misuse of such data.

Credit Bureaus

Armenia has recently adopted legal framework for operation of credit bureaus (ACRA) that got powerful instruments for collecting information about users who sometimes do not have options for not providing such data.

In general, the credit unions are the institutions that have vary of sophisticated methods indirectly forcing individuals to supply personal data to third party and use such data in legitimate way, e.g. they usually have formal consent of individuals that do not have much choice to refuse providing such data.

Another issue is, when granting such consent, individuals usually do not know what kind of information about him/her could be collected and, if known, individuals may decide not to grant a consent of requesting/retrieving such information. Theoretically personal data protection legislation is applied to databases held by the credit bureaus, but they may refuse to distrust information which is not any more in use for the purpose that it has been collected by arguing that credit history is something to be kept forever because it is valuable and it is not subject for destruction.

Proposed actions

- Potential focus of civil society should be classification of data categories that may be stored by either public or private video surveillance systems, the terms of storage and the rules for accessing such data without judicial order.
- Relevant policy/legislative recommendations may also be part of civil society initiatives related to bulk data collection and processing.
- Special research may be carried out to identify potential violations of privacy by the credit bureaus or abuse of credit granting power to force to provide personal data.
- Study of the European Court of Human Rights rulings related to the protection of privacy in regard of abusing public surveillance systems may be valuable for amending relevant parts of the Armenian legislation.

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