Open Society Foundations - Armenia

POLICY ANALYSIS

ONLINE PRIVACY

Cookies, users activities tracking, online data collection and storage

Cookies

Cookies is data that website request users browser to store in their computer or mobile device. The cookie allows the website to "remember" users' actions or preferences over time. Most browsers support cookies, but users can set their browsers to decline them and can delete them whenever they like.

Web site may contain third party cookies such as featured advertisers banners (most of news websites, online stores and social media contain third party cookies). Third party cookies are usually trace users' visits to other websites and may profile users for better targeting advertisements. There were some cases of US government authorities (CIS, DEA, NSA)[1] tracking users behavior without notification of website visitors. After disclosure of those cases, US government introduced strict rules of banning using of cookie by the government authorities.

The European Union has responded to privacy threats related to cookies with a policy incorporated into EU Directive on Privacy on Electronic Communication (Directive 2002/58/EC). In spite of several criticisms, the measure introduced by the e-Privacy Directive was the first attempt of the EU to address the privacy threats that might be caused by cookies technology. Later the Directive has been amended and introduced new rules on usage of cookies:

- Some cookies can be exempted from informed consent under certain conditions if they are not used for additional purposes. These cookies include cookies used to keep track of a user's input when filling in online forms or as a shopping cart.
- The first party analytics cookies are not likely to create a privacy risk if websites provide clear information about the cookies to users and privacy safeguards.

Today website owners (content administrators and publishers) are obliged to inform visitors about use of cookies and provide them with an option to accept or reject use of cookies' instruments.

There are many threats of cookies technologies that, however, not necessary could be efficiently regulated by public authorities. Most of the threats are of criminal origin and include, for instance, such risks as interceptions of cookies related communications between users' browsers and website server or thefts of cookies from a user's computer.

Proposed action

- One of the important research questions might be the efficiency of cookies related regulations adopted in the EU or other countries, as well as possible threats of the absence of such regulations.

Search Engines

Privacy threats of search engines are of different nature from those are in case of cookies. Search engine related privacy threats are known only by a limited number of experts. Ordinary users usually are not aware about privacy issues they could be exposed to while using search engines. Typically, search engines collect detailed information that is personally identifiable or can be made personally identifiable. This information includes the search terms submitted to the search engine, as well as the time, date, and location of the computer submitting the search.

[1] CIS – US Citizenship and Immigration Service
DEA – Drugs Enforcement Administration
NSA – National Security Agency.

This information collected during the search is generally collected for marketing and consumer profiling purposes and also used by search engines for users' behaviour researches and generation of statistical usage data. Chief amongst the search engine related threats are behavioral marketing and widespread public disclosure of personal information. According to a poll conducted in 2006 on privacy related civil society groups, 1000 Google users found that 89% of respondents think their search terms are kept private, and 77% believed that Google searches do not reveal their personal identities.

The primary method of identification is IP, which makes information submitted to search engines personally identifiable. In some countries including Armenia disclosure of users IP in a particular Internet session (including time and place) is prohibited without a permission of relevant authorities (in case of Armenia, the courts). However, use of IP by the third country search engines is usually out of users' home country jurisdiction and usually less protected than home country users data. Most of frequently used search engines are out of jurisdiction of user's home country and based either in the US or the EU, but they usually keep their cache servers in users home countries for traffic optimization purposes.

Moreover, most of Internet users do not pay attention on legal notices they agree with prior to entering website with searched content and are definitely not aware about privacy rules of some search engines. Non-disclosure of session IP, place and time might not be sufficient safeguard for the protection of users' privacy. As mentioned, users often don not even realize what the privacy related consequences may have use of personal data. For that reason, privacy advocacy non-governmental organizations call governments to encourage large search engine companies to adopt corporate standards based on generally accepted principles of privacy protection.

Proposed action

Speaking about potential research and policy advocacy areas aimed at identification of privacy threats related to search engines two main directions may be outlined bearing in mind extremely limited influence of national legal frameworks on global players on Internet market, such as Google and Yahoo. These two directions are:

- Study of possible mechanisms for minimizing privacy threats of search engines at national level might be most practical initiative.
- Protection of locally cached data might be another research/policy topic.

Social Networks

Privacy threats of social networks could be assessed as highest risks, which is mainly due to massive information that users usually accumulate in their network profiles. One of such threats is identity theft, which is often happen when users upload their personal data. Use of third party applications available in social networks increases privacy threats. Thus, for example, one of the applications available in Facebook tracks users through geo-location future of uploaded photos. Users often do not pay attention to the futures of applications they use, and the applications profile social network users in a merely legitimate way.

Illegal surveillance is one of the most dangerous privacy threats of social networks. Social networks accumulate not only users' personal data, but also information about their activities, e.g. visiting places, attended events, the most importantly, the social links with other people. As mentioned, users usually do not read carefully terms and conditions of using digital products especially user agreement (notice) of the enrolment in a network based services. Meanwhile, such services usually provided with minimal requirements of applicable legislation (usually enforceable only in country of service hosting company) and consequently grant users minimal level of privacy protection.

Similar to privacy threats of using search engines social network related privacy risks are usually also out of the attention of ordinary users and could not be mitigated under a particular jurisdiction without broad international cooperation. International treaties and conventions provide some level of protection, but usually indirectly, through harmonization of relevant pieces of legislation unless the issue of a criminal character falls under the international cybercrime treaty (Council of Europe Cyber Crimes Convention). Social networks may also practice caching users data on servers based in end-users countries especially those that offer users' possibilities of exchanging heavy content (video and audio messages and files).

Proposed action

- Potential civil society involvement in policy issues related to individuals/personal data protection in social networks might be focused on users' education, awareness raising, specifically in parental control and minors protections.

Network Stored Data

Apparently, most of the data mentioned in above paragraph is stored on different data centers. However, there is special category of data which is stored on regular basis by Internet access and websites hosting service providers (ISP's)[2]. Some counties legislation obliges service providers to store traffic and access logs. In some other countries ISP's store that data even though the law does not require, but often security and law enforcement bodies demand for "voluntary" storage of user data, and ISP's do so to avoid possible trouble with officials.

The above "cooperation" of service providers and law enforcement officials is possible due to lack of mechanisms of public control over the activities of service providers and inefficient legal remedies. Civil society activists usually concerned about the legitimacy of the access to personal data is granted, but very rarely pay attention on how it granted and how long retrieved/accessed data is kept by law enforcement or other authorities.

Telecommunications is one of the most sophisticated and as a result hardly monitored area of personal data protection control. It is especially difficult to control data protection compliance among small companies that usually do not have relevant corporate policies and does not carry out regular audit of such information systems as billing and registry software.

Proposed action

- The action points in this area might be comparative study and analysis of the Armenian and the European legislation and elaboration of recommendations on improvements of the Armenian national legislation. Particularly, possibilities for introduction of regular data protection audits by independent auditing companies might be considered as a mechanism for the protection of users from unlawful interception and storage of their data by telecom service provides under the patronage of law enforcement bodies.

Big data

Big data is one of the special areas of digital society appeared parallel with development of information technologies and computer networks. Big data is usually associated with statistics, analysis of mass behavior and social forecasts, which are, however, only a part of the possible utilization of data massive accumulated by different public and private organizations. If administered correctly with sufficient level of security big data utilization may positively impact economic activities of different market players. Thus, use of telecommunications data (mobile cells dynamic statistics) helps to report car traffic by navigation service providers and shopping routes to marketing planners.

However, massive data storages are positively impact economic and social activities when they properly communicated to processors and appropriately protected. Many of the industries accumulating big data, such as telecommunication companies, privately run registers, hotels and travel intermediaries, banks and credit bureaus are required to ensure proper level of data protection. Usually, those companies require auditing their information systems to ensure compliance with relevant general or industry specific information security standards. However, in developing markets (including post soviet countries) information security audits are usually required on specific occasion or for limited categories (in Armenian financial institutions, such as, for examples, banks and credit unions).

Though, Armenian data protection legislation foresees use of adequate information security measures for database owners it does not specify methods of ensuring the compliance with such requirements as well as the obligations of public authorities to define such standards and procedures. Information security standards are

[2] ISP – Internet Service Provider

equally important for both public and private institutions and data protection authorities must at least define mandatory certification of governmental and municipal bodies' compliance with such standards and recommend applicable standards for private sector. Ideally data protection legislation must define these standards.

<u>Proposed action</u>

- Potential action points for civil society in this area could be defining basic standards based on international experience and best practices, analysis of legal framework and elaboration of recommendations concerning both best practices and legislative changes if required.

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.