POLICY ANALYSIS

RIGHT TO BE FORGOTTEN

"Right to be forgotten" is a new concept of privacy in digital world. It was enforced in European Union under the Data Protection Directive and in Argentina. In USA freedom of speech activists view this concept as a potential danger for the freedom of speech especially if applied to public persons. This issue most likely is not prioritized in Armenia, but at some point will definitely face a question "Does an individual have a right to be forgotten or not?" This challenging concept might be a topic for academic research that might be used in future policy debates.

The concept of the right to be forgotten has become a widely discussed topic since 2005 triggered by court cases initiated by individuals who demanded for removal of information about themselves from search engines databases and other sources that according to them was offensive, inappropriate or undesirable for retrieval for some other reasons.

Historically the rights to be forgotten is associated with a legal case initiated by a Spanish citizen who filed a complaint against a Spanish newspaper with the national Data Protection Agency and against Google Spain and Google Inc (Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González). The citizen complained that an auction notice of his repossessed home on Google's search results infringed his privacy rights because the proceedings concerning him had been fully resolved for a number of years and hence the reference to these was entirely irrelevant. He requested, first, that the newspaper be required either to remove or alter the pages in question so that the personal data relating to him no longer appeared; and second, that Google Spain or Google Inc. be required to remove the personal data relating to him, so that it no longer appeared in the search results.

It is worth to mention that current European legislation does not provide universal tool for the implementation of the right to be forgotten. Directive 95/48/EC requires Member States to guarantee every data subject the right to obtain from the controller the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data. Several Member States have construed this right narrowly in data protection laws implementing the Directive. For example, in the UK, the right for data subjects to apply to court for an order to rectify, block or destroy data is limited solely to where the court is satisfied that the data is inaccurate.

In spite of the rights granted to data subjects (individuals) under the Article 14 of Directive 95/48/EC data subjects' right to be forgotten is implemented on the ground of ruling of the Court of Justice of the European Union (Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González). Meanwhile, due to several changes takig place in personal data protection environment including new challenges and threats emerged in digital world a proposal on new data protection legislation has been developed by the European authorities that is currently known as a General Data Protection Regulation (GDPR).

One of GDPR articles (Article 17) specifically address the issues related to individuals right to block/stop under the certain circumstances information that is not in legitimate interest of the individual. However, fight to be forgotten is to be replaced in GDPR by the right to erasure, which, according to the European experts, has more limited scope of implication. Article 17 provides that the data subject has the right to request erasure of personal data related to him on any one of a number of grounds including non-compliance with lawfulness that includes a case where the legitimate interests of the controller is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

The above paragraphs describe European approach towards the concept of right to be forgotten. However, the concept of the right to be forgotten is not that obvious in the United States and other parts of the world. In US the concept is based on case law and depends on whether the right to be forgotten in particular case prevails over the public interest of knowing the facts. It is worth to mention that the US law does not have direct norms protecting

privacy. One is the invasion of privacy, a tort based in common law allowing an aggrieved party to bring a lawsuit against an individual who unlawfully intrudes into his or her private affairs, discloses his or her private information, publicizes him or her in a false light, or appropriates his or her name for personal gain.

Privacy rights in the US is partially might be imposed under the Fourth Amendment which declares "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. Fourth amendment is limited in the scope and applicable to cases of interfering of federal and state authorities and is not applicable to cases that do not foresee other types of interference different from "search and seizures". Moreover, it is applicable to houses and equivalents, but not to electronic data held by third persons.

In case Melvin v. Reid (1931) (a woman was charged with murder and then acquitted, but film The Red Kimono revealed her history, and she sued the producer the court ruled in favor of plaintiff. The claim was based on tort caused by public disclosure and the ruling was reasoned by a privacy right referred to "any person li[1]ving a life of rectitude has that right to happiness which includes a freedom from unnecessary attacks on his character, social standing or reputation". Opposite to the described case in another case, the court does not grant the plaintiff right on privacy on a ground that a public figure cannot enjoy the same level of privacy as ordinary people. The Defendant, F-R Publishing Corp. (Defendant), wrote an article about the Plaintiff, William James Sidis (Plaintiff) who was once a public figure. The article was of public interest; however, it intruded upon the Plaintiff's private life. The Plaintiff sued the Defendant for intrusion on his right to privacy. The court held here that there were limits to the right to control one's life and facts about oneself, and held that there is social value in published facts, and that a person cannot ignore his or her celebrity status merely because they want to.

Apart from general approach of public disclosure tort applicable to private law and Fourth Amendment protecting individuals' privacy from interference of public authorities, there are some general federal and sectoral (industry specific) legislation aimed to protect individuals privacy in a particular type of relationships, such as, for example, telecommunications, health-care, insurance, etc. Following are the examples of such regulations:

a) S. 1158 (Consumer Privacy Protection Act) would establish a federal security breach notification law and provides protection for many types of data including social security numbers, financial account information, online user-names and passwords, unique biometric data (including fingerprints), information about a person's physical and mental health, information about a person's geo-location, and access to private digital photographs and videos. The bill would pre-empt weaker state laws while leaving stronger state privacy laws in place.
b) H.R. 2092 (Student Digital Privacy and Parental Rights Act) would prohibit operators of websites, applications and other online services from selling students' personal information to third parties and using or disclosing students' personal information to tailor advertising to them. The bill would also give parents access to information held about their children and allow them to correct it, delete information about their children that schools do not need to retain, and to download any material their children have created.
c) S. 668 (Data Broker Accountability and Transparency Act) would, among other things:
    i) require data brokers to establish procedures to ensure the accuracy of the personal information they collect, assemble, or maintain; and any other information that specifically identifies an individual, (unless the information only identifies an individual's name or address);
    ii) require data brokers to provide individuals a cost-free method to review their personal or identifying information;
    iii) allow individuals to dispute the accuracy of their personal information with a written request that the data broker make a correction.
d) The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act) is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies. The FTC has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorized disclosure of personal data. The FTC is also the primary enforcer of the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501-6506), which applies to the online collection of information from children, and the Self-Regulatory Principles for Behavioral Advertising.

[1] Sidis v. FR Pub. Corporation, 34 F. Supp. 19 http://law.justia.com/cases/federal/district-courts/FSupp/34/19/1458518/

e) The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827) regulates the collection, use and disclosure of financial information. It can apply broadly to financial institutions such as banks, securities firms and insurance companies, and to other businesses that provide financial services and products. GLB limits the disclosure of non-public personal information, and in some cases requires financial institutions to provide notice of their privacy practices and an opportunity for data subjects to opt out of having their information shared. In addition, there are several Privacy Rules promulgated by national banking agencies and the Safeguards Rule, Disposal Rule, and Red Flags Rule issued by the FTC that relate to the protection and disposal of financial data.

f) The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) regulates medical information. It can apply broadly to health care providers, data processors, pharmacies and other entities that come into contact with medical information. The Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule) (45 C.F.R. Parts 160 and 164) apply to the collection and use of protected health information (PHI). The Security Standards for the Protection of Electronic Protected Health Information (HIPAA Security Rule) (45 C.F.R. 160 and 164) provides standards for protecting medical data. The Standards for Electronic Transactions (HIPAA Transactions Rule) (45 C.F.R. 160 and 162) applies to the electronic transmission of medical data. These HIPAA rules were revised in early 2013 under the HIPAA "Omnibus Rule". Compliance with these changes is required by September 23, 2013.

g) The HIPAA Omnibus Rule also revised the Security Breach Notification Rule (45 C.F.R. Part 164) which requires covered entities to provide notice of a breach of protected health information. Under the revised rule, a covered entity must provide notice of acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, unless the covered entity or business associate demonstrates that there is a low probability that the protected health information has been compromised.

h) The Fair Credit Reporting Act (15 U.S.C. §1681) (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108-159) which amended the Fair Credit Reporting Act) applies to consumer reporting agencies, those who use consumer reports (such as a lender) and those who provide consumer reporting information (such as a credit card company). Consumer reports are any communication issued by a consumer reporting agency that relates to a consumer's creditworthiness, credit history, credit capacity, character, and general reputation that is used to evaluate a consumer's eligibility for credit or insurance.

i) The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (15 U.S.C. §§7701-7713 and 18 U.S.C. §1037) and the Telephone Consumer Protection Act (47 U.S.C. §227 et seq.) regulate the collection and use of e-mail addresses and telephone numbers, respectively.

j) The Electronic Communications Privacy Act (18 U.S.C. §2510) and the Computer Fraud and Abuse Act (18 U.S.C. §1030) regulate the interception of electronic communications and computer tampering, respectively. A class action complaint filed in late 2008 alleged that internet service providers (ISPs) and a targeted advertising company violated these statutes by intercepting data sent between individuals' computers and ISP servers (known as deep packet inspection). This is the same practice engaged in by Phorm in the UK and several UK telecommunications companies that resulted in an investigation by the European Commission.

As mentioned, Armenia has adopted both general and sectoral legislations protecting individuals' personal data and privacy. General concept of privacy in the Armenian legislation is based on the rights declared under the European Human Right Convention and the Council of Europe Convention on Protection of Individuals with Regard to processing of Automatic Processing of Personal Data. The general regulation mainly address the legal grounds and procedures for interception of communications means (paper and electronic correspondence, phone conversations), search and seizure of evidences in private property, as well as video and audio interception into a private life of suspects or other individuals as required for criminal investigations. The Law on Personal Data Protection could also be considered general legislation due to mandatory application in any type of public or business relationships.

General privacy related legislation in Armenia does not contain any clause, a legal norm that might be interpreted as a right to be forgotten, imposing ban on or blocking of access to information related to person he/she does not want to be publically accessible for some reasons, unless it is information about private life of a person. The later is protected under article 144 of Criminal Code, which is "Illegal collection, storage, use or disclosure or information about private or family life". The article refers to "private or family life secrets" without explaining what that notion means, but it might be reasonably interpreted as any information, which is a) not public, b) the person considers be a secret, c) the person took reasonable measures for protecting such information from unauthorized use.

Personal Data Protection Law addresses the issues of legitimacy of the collection, storage and processing personal data and might be referred to as general privacy legislation. However, no of data subject rights described under article 15 might be interpreted as a right to be forgotten. Nevertheless, the Law on Personal Data Protection contains a very important provision concerning the publically available data (Art. 11), which introduces a notion of publically available data, which, according to the definition provided by law, is data that become available for general public in the result of data subjects act of providing such data for public use or making it public by his/herself. Traditional examples of public data are telephone and address books and publication references, but today data entered/published in social networks, blogs and other online services might be considered a public source data.

The same provision (Art. 11) provides that publicly available data could be retrieved from public sources on request of an individual or in accordance with the decision of the court. However, it does not define any circumstance that might be considered as a ground for the data retrieval, e.g. a legal ground that court or data processor may consider a legitimate request of a data subject. In cases when data is voluntarily provided by data subject, it is reasonable to expect that data processor to refuse retrieval of data, but not use it in further processes. For instance, if an address book has been published, it is not reasonable to demand for calling it back on demand of one of individuals who granted publisher a right to publish his/her data, but it is reasonable and legitimate to demand for not using the data in future editions. However, a case law is needed to see how this provision would work in practice.

Sectoral privacy legislation in Armenia includes:

a) Law on Bank Secret (adopted by the National Assembly in 1996), which provides legal grounds for the protection of individuals financial data from unauthorized access and disclosure. The Law on Bank Secret was one of the most valuable grounds for the newly emerged market economy and made vital contribution to the development of the Armenian banking system. Law no Credit Information Flow and Credit Bureaus (2008) is another part of financial legislation addressing inter alia the rights of individuals on protection of their privacy, which in this case is financial data, credit histories and credit rates.
b) Article 49 of the Law on Electronic Communication (adopted by the National Assembly in 2005) defines type of customers data (including network generated data) that operators and service providers must consider as a private and not to disclose without relevant judicial order.
c) Protection of patients' data by medical institutions is provided under several legal acts such as Law on Medical Assistance and Medical Services (adopted by the National Assembly in 1996), Law on Psychiatric Assistance (2004), Law on Transplantation of Human Organs (2002), Law on Reproductive Health and Reproductive Rights (2002).

Proposed action

Given the complexity of the right to be forgotten concept proposed civil society activities might include achievement of several goals in both academic and policy advocacy spheres.

- A comprehensive research of international practice would be of great value and will provide both policy makers and civil society with best practices in this area. The research must also contain study of possible mechanisms of implication of the right to be forgotten in Armenian political and legal realities, as well as practice of balanced approach towards the right that will protect individuals from undesirable use of their data without restricting others right to know publicly valuable information.
- Further actions of the civil society might be activities aimed to develop recommendations regarding changes and amendment to the privacy legislation (including, but not limited to Personal Data Protection Law) that will empower individuals with a right to demand for retrieval of information about their private life or personal data from public sources without affecting the right of public to search and obtain publicly valuable information.

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