Cherdantseva, 2:1
http://dx.doi.org/10.4172/scientificreports.592

Open Access Scientific Reports

Short Communication Open Access

Privacy from the Perspective Of 2012

Yulia Cherdantseva*

School of Computer Science and Informatics, Cardiff University, UK

Privacy is a long-existing and dynamic concept. In the 1970s, the period of ever increasing concerns about personal data stored in the computer systems began. With the advent of computers it was realized that the law poorly protects individuals against misuse of personal data processed by new technology. This article discusses the improvement of the privacy legislation over the last four decades. The author also suggests a four-dimensional solution of the privacy problem. The first dimension involves privacy awareness and education. It promotes two other dimensions: economic incentives (in the privacy-aware environment people only trust organizations that care about customers' privacy) and the privacy legislation enforcement (privacy activists force the legislation to develop and to be enforced). Economic incentives and the strong privacy legislation will force proliferation of the fourth dimension-privacy-protecting technologies. Finally, the crux of the matter is how much do individual's care about privacy?

The meaning people embed into the privacy concept changes inevitably following the evolution of society and technology. The importance of privacy grows over the years since personal data become easier to acquire and to expose, which increases threats to privacy. Moreover, the consequences of privacy breaches become more and more tangible.

The advent of new technology led to the growth of privacy concerns. In 1890, the highly cited privacy-related paper "The Right to Privacy", written by Warren and Brandeis, emerged as a response to the privacy concerns about new technology, allowing publication of photographs in newspapers. In this paper, the authors described privacy as the individual's "right to enjoy life" and "the right to be left alone" [1].

In the 1970s, the period of ever-increasing concerns about personal data stored in the computer systems began. Prior to the Computer Age, people relied on legislation and social norms to protect their privacy. With the advent of computers it was realized that the law poorly protects individuals against misuse of personal data processed by new technology. Legislation was either obsolete for a new situation, or simply there was no pertinent legislation [2]. This urged a need to establish standards for privacy protection. The problem was approached seriously, at the political level, and a number of guidelines and standards emerged addressing privacy protection.

In 1973, the US Secretary's Advisory Committee on Automated Personal Data Systems responded to the growing privacy concerns by the report titled *Records, Computers and the Rights of Citizen* [3]. The report brought to life the Code of Fair Information Practice (FIP) based on five principles:

1. There must be no secret personal data record-keeping systems;
2. An individual should be able to find out what information about him/her is in a record and how it is used;
3. An individual should be able to prevent information about him/her to be used for non-agreed purposes without his/her consent;
4. An individual should be able to correct or amend a record of about him/her;
5. Any organization creating, maintaining, using, or disseminating personal records must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

The FIP principles served as a kernel for the US Privacy Act of 1974, which elaborated the principles further. The Act proposed eight principles: Openness, Individual Access, Individual Participation, Collection Limitation, Use Limitation, Disclosure, Information Management and Accountability Principles.

The *Personal Privacy in an Information Society* report, published in 1977 [4], criticized the Privacy Act. It pointed out that the Act has not resulted in the expected benefits to society and on the lack of control individuals have over their personal data. The report stated that although the Act is a large step forward, some of the Act's requirements are ambiguous, which makes compliance with the Act difficult to assess. The report also noted that the Act does not address the important privacy policy issues in the required depth. The report prepared a number of recommendations for the privacy legislation improvements. Many of the recommendations have still not been implemented in practice.

In 1980, the Organisation for Economic Cooperation and Development (OECD) published the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [5], which also revised and extended the FIP principles. The Guidelines are based also on 8 principles:

Collection Limitation Principle: The collection of personal data should be limited and obtained by lawful and fair means with the consent of an individual where possible.

Data Quality Principle: Personal data should be accurate, complete, up-to-date and fit for the purpose of collection.

Purpose Specification Principle: The purposes of data collection should be specified at the time of data collection.

Use Limitation Principle: Personal data should not be used for purposes other than specified (except with the consent of an individual)

Security Safeguards Principle: Personal data should be adequately protected from loss, unauthorized access, destruction, use, modification or disclosure.

Openness Principle: Practices and policies with respect to personal data should be open. A data controller should have the means available to establish the nature of data and the purpose of their use.

***Corresponding author:** Yulia Cherdantseva, School of Computer Science and Informatics, Cardiff University, UK, E-mail: y.v.cherdantseva@cs.cardiff.ac.uk

Received October 3, 2012; **Published** December 13, 2012

Citation: Cherdantseva Y (2013) Privacy from the Perspective Of 2012. 2: 592 doi:10.4172/scientificreports.592

Copyright: © 2013 Cherdantseva Y. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Individual Participation Principle: An individual should have the right to challenge, erase, rectify, complete or amend data about him/her.

Accountability Principle: An organization controlling personal data should be accountable for complying with all eight principles.

This document is the first internationally agreed statement of the core privacy principles. It served as a foundation of the privacy legislation in the OECD countries. The aim of the OECD Guidelines is to reconcile privacy legislation and to promote systematic, consistent cross-border privacy law enforcement.

In 2007, the OECD adopted a Recommendation setting a framework for international co-operation in privacy law enforcement. The Recommendations declared a need to ensure that the privacy-protecting authorities have (1) the necessary power to prevent violations of laws protecting privacy and (2) the rights to collaborate with authorities in other countries.

The OECD initiatives have significantly advanced the privacy protection. In 1980, only a third of the OECD members had privacy laws. At present, each of the 34 OECD countries has at least one privacy-enforcing law. The OECD members gradually revise their domestic legislation to provide privacy enforcement bodies with more authority. Germany, Italy, Korea, the UK and Spain recently empowered their authorities to issue monetary penalties for privacy law violations. In 2009, the UK Information Commissioner's Office (ICO) received the power to conduct an audit of government departments [6].

Despite the progress in moving towards the privacy-law-obeying environment, there are still many holes that need to be fixed. Thus, the weaknesses of the FIP are rooted in allowing many exemptions and in self-regulation. The privacy-protecting guidance also fails to keep pace with the advances of ICT. The main problem is possibly caused by the fact that many FIP principles are still not enforceable by law and serve only as guidance for privacy aware data processing. The OECD countries are still not able to use in privacy-related cases evidence, judgments or orders obtained abroad [6].

Many privacy issues originate from the systems legacy. The majority of systems are built with the assumption that personal data is hard to obtain. Therefore, the systems use personal data for authentication purposes [7]. The rapid proliferation of social networks and e-commerce, accompanied by the growth of a number of databases storing personal data, has changed the situation: the personal data are often too easy to find and to access.

The social networks' policies contradict the existing expectations of society about privacy: they make personal information public by default and private only by additional effort [7]. A user has very little control over his/her personal data used by the social networks and e-commerce websites. How the data is stored, who may have access to it and for what purposes is not strictly regulated by law.

In 2012, Google announced that it is replacing its multiple old privacy policies with the new policy, unified for all Google products. The new privacy policy took effect from 1st March. The policy explains that, from now on, Google collects, in one place, a huge amount of information, coming from all Google Services, about all its users. The information to be collected includes [8]:

- Personal information provided by a user while creating a Google account;
- Information about the user's devices (hardware model, operating system version, unique device identifiers, mobile network information including phone number);
- Details of search queries;
- Telephone call and SMS logs;
- IP addresses;
- Location data (GPS signals from a mobile device, nearby Wi-Fi access points and cell towers).

The Google privacy policy change provoked a rising tide of debate and discontent from the side of privacy activists and privacy-protecting authorities. One of the main concerns is that Google does not provide an "opt out" option. If a user does not wish his\her information to be collected, a user has to stop using all Google services. Taking into account that Google holds virtually a monopoly on many services, this is not the best option. Users would better compromise on their privacy in order to use Google services.

The EU privacy-protecting authorities currently investigate the new Google privacy policy for legal compliance. Unfortunately, the effectiveness of the authorities' actions to date does not provide a feeling that the authority could radically change the Internet-giants privacy attitude. Obviously, organizations that are in control of the implementation of privacy protection mechanisms should have economic incentives to implement and to improve them (e.g. organizations should financially suffer from loss of personal data [7]). The fines, imposed by the privacy law enforcement authorities, are the reasonable stimuli for organizations to obey privacy law. The recent practice showed that the privacy-law-enforcing bodies mostly fine small organizations and public authorities. The attempts to control privacy law compliance in the giant multinational corporations, specializing in Internet search, advertising technologies and social networking, have only just begun.

The solution to most privacy issues is seen in a strong, well-enforced legislation. Some authors (cf. [7, p.94]) see solution in giving the ownership of personal data to individuals, rather than to organization collecting the data. The emerging technologies are expected to support the individual's privacy rights by allowing more significant user-involvement and enabling a user to express privacy preferences. The European Commission (EC) actively endeavors to overcome the lag between privacy law and rapidly evolving technology. In January 2012, after extensive consultations, the EC published a *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [9]. The proposal includes the general principles of data protection stated in the early documents, but adapts the framework to the fast advancement of technologies and globalization. The document proposes the following major changes to the European Data Protection Regulation:

1) The legislation will apply to all non-EU organisations, processing data of EU residents
2) Severe penalties (up to 2% of worldwide turnover) will be applied for non-compliance
3) "Right of portability" will allow transfer of data from one electronic processing system into another, without being prevented from doing so
4) "Right to be forgotten" will allow a data subject to request his/her personal data to be erased and no longer processed. A data

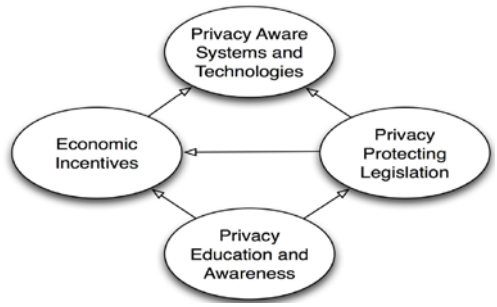

Figure 1: A Four-Dimensional Solution of the Privacy Problem.

controller will also have to inform third parties, processing such data, about the request to erase the data

5) Organisations have to notify Data Protecting Authorities and individuals affected about the data leaks within 24 hours.

The proposal endeavors to address the differences between the EU and the US approach to privacy. While the EU attempted to create coherent privacy law across all its members, the US heavily relies on self-regulation and responsible behavior of its citizens [2]. The adoption of the proposal will guarantee that the EU citizens' personal data will be used according to the EU privacy regulation, even when they processed by the US corporations.

The rapid advancement of ICT has changed the way data are collected, stored, processed and, of course, protected. Thus, on the one hand, new technologies cause the escalation of privacy concerns in society. On the other hand, technologies could put users back into control over their personal data. Generally, people are not interested in privacy as an abstract concept. The transparent control of the personal data exposure to others – this is what people most likely desire and this is what technologies are capable of offering.

No technology *per se* implies that our privacy should be invaded. Any system should be designed with privacy in mind and should use technology to protect our privacy. The privacy problem is not a question of technologies being unable to protect privacy, but an issue of the legal and economic nature. Bodies, which design systems and implement technologies, should have economic and legal incentives to enable privacy protection. The economic stimulus is rooted in customers' trust: the more customers trust an organization, the more profit an organisation makes. The surveys show that e-commerce loses an essential amount of profit due to the users' privacy-violation fears [2]. On the legal side of the problem, a law is needed which encourages organisations to protect users' privacy.

In author's opinion, the privacy problem should have a four-dimensional solution illustrated in figure 1.

The first dimension involves privacy awareness and education. Statistics show that we are still to create the privacy-conscious and privacy-educated society. According to the survey the majority of Google users are ignorant about the forthcoming policy change [10]. Nearly sixty per cent of social networking websites users have never read privacy policies. People are not able to protect their privacy if they are unaware of the privacy regulation, about their privacy right and about the way their information is used.

The first dimension promotes the other two dimensions – economic incentives and the privacy-legislation enforcement. First, in the privacy-aware environment people only trust, and, as a result, bring their money to, organizations that care about their customers' privacy. Second, privacy activists force the privacy legislation to develop and to be enforced: the increasing number of privacy activists expedites this inevitable process. The privacy legislation, in its turn, also induces additional economic incentives by imposing fines for privacy law breaches. Economic incentives and the strong privacy-legislation, supported by the privacy-conscious society, will force proliferation of the fourth dimension – privacy protecting technologies.

Finally, the crux of the matter is how much do individual's care about privacy? Therefore, in order to improve privacy protection it all comes down, first of all, to educating people and raising their privacy expectations.

Privacy is a difficult trade off. From the individual's viewpoint, privacy is an inherent human right. From the business perspective, privacy protection measures hinder productivity and induce additional costs. Nearly forty years ago, in 1973, it was mentioned: *"Although there is nothing inherently unfair in trading some measure of privacy for a benefit, both parties to the exchange should participate in setting the terms"* [3]. Significant steps are already being taken towards the privacy-law-obeying society. Nevertheless, the law still often fails to provide an environment where both parties may "set the terms" and where the rights of each party are adequately protected. Individuals have to accept services on the conditions provided and are often left vulnerable to privacy violations caused by new technology. We are still looking forward to governments finding a fair balance between privacy expectations of individuals and organizations.

This is a short opinion paper, the intension of which is (1) to sketch a current state of the privacy legislation and (2) to outline the four-dimensional solution for the privacy problem. Further research is required to justify the proposed solution.

Acknowledgements

The author is grateful to several anonymous reviewers who supported the idea of the four-dimensional solution of the privacy problem and provided valuable comments.

References

1. Warren S and Brandeis L (1890) The right to privacy [the implicit made explicit]. Harvard Law Review, 4: 75-103.
2. Smith R, Shao J (2007) Privacy and e-commerce: a consumer-centric perspective. Electronic Commerce Research 7: 89-116.
3. Records, Computers and the Rights of Citizens (1973) Report of the Secretary's Advisory Committee on Automated Personal Data Systems.
4. U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society.
5. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
6. Organization for Economic Cooperation and Development, OECD Digital Economy Papers.
7. Schneier B (2008) *"Schneier on Security"*. Wiley Pub.
8. European commission, proposal for a regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
9. ICO urged to investigate imminent Google privacy policy changes.
10. APPA Privacy Awareness Week 2011 social media survey.