Aleksandra Brodowska
Antoni Napieralski

“Concept of profiling under the EU Draft Regulation on Data Protection”

Warsaw, 2014

Table of contents

1. Introduction

The issue of profiling is nowadays one of the most urgent ones. The constant technological development changes the world we are living in. Question is, for the better or for the worse? In this paper we would like to consider the main points of the process of profiling, especially its legal side. For the sake of the essay's clearness we would focus only on the commercial aspect of profiling, leaving out the deeds of intelligence agencies all over the world. We think that the commercial aspect is far more important. The companies have larger resources of profiling-useful data than the states. What is more, as the Snowdengate has shown us, after all the intelligence agencies just take personal data from the commercial sector, rather than collect them on their own.

With regard to our legal methodology, we would like to analyze the EU Draft Regulation and the EU Directive 95/46/WE, and compare the regulations which are passing away with the new ones. We also find the context of the Transatlantic Trade and Investment Partnership Agreement really intriguing; in particular, we are interested in the way how the profiling issue may influence on the negotiations.

2. What profiling really is?

How do you imagine the future world? Let us present our point of view.

One day we will wake up in a world ruled no longer by humans. We will wake up in a world where humanity will be self-locked in a panoptikon of its own construction. A world in which a huge amount of personal information combined with the analytical tools will allow a newly born Big Brother 2.0 to control our lives. How will it happen?

Profiling, as prof. E. Moglen puts it is predicting our behavior in the Web, based on aggregating the so-called data dandruff of life[1]. This data dandruff is all of our e-activity: phrases we look up via Google, www addresses we visit, links we click on large commercial sites (Amazon, eBay), types of goods we buy in the Net, sites we like on Facebook, photos we upload on Instagram and emails we both receive and send[2]. They are called dandruff

[1] E. Moglen, Freedom In the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing, [on line] http://www.softwarefreedom.org/events/2010/isoc-ny/FreedomInTheCloud-transcript.html

[2] Google Terms of Service, 14.04.2014, "Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and

because the legal regulations are hardly ever considering them as personal data. Due to the fact that they are not allowing to identify a single person, they are not classified as personal data[3]. It is wrong. Nowadays, identifying a person, with its name and address is worthless. It is the connection of these dandruff information with a specific IP address or an ID cookie file which is crucial. As the Federal Trade Commission (U.S.) put it in their Consumer Privacy Report: the privacy framework should be applicable to "consumer data that can reasonably be linked to a specific consumer, computer or other device."[4] For Amazon or Google it does not matter that Antoni Napieralski living in Marszałkowska Str. has some habits in his Net activity. What does matter is that the IP address 80.53.214.181, identified by a specific ID cookie file has some habits in its Net activity. Every step we take in the Internet is taken to the record. The Web, unlike the humans, never forgets. It is caused by one, major technological issue called 'retention of logs'. What does it mean? To fully understand this term, let us introduce some IT background.

Contemporary architecture of the Net has nothing in common with the noble, egalitarian purpose of its fathers. The client/server structure introduced by Microsoft's Windows deprived average users of their subjectivity. In place of equal junctions able to function both as servers and clients, we received an almost global operating system which changed our computers into permanent clients[5]. As time went by the split between users and service providers was deepening. The latters were increasing their processing capacities and broadening the service offer, while the 'clients' were pushed to the fringe of the Net. How does the Internet of today look like? Look at the Web traffic map in the appendix no. 1. It presents the data flow junctions as colorful spots. Their size is proportional to the traffic these junctions operate and their color depends on the national affiliation. We can clearly see that Net is dominated by the service providers of enormous size. Google.com which is opening the world rank is said to be visited by 49,7 % of all the Internet users. Keeping it in mind, let us think for a moment about political science. What happens when limited resources are distributed via few, centralized structures? It creates the power of rulers over the subjects. In the ancient times some dukes gained power by distributing food and water. Nowadays the

spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored." [on line] https://www.google.com/intl/en/policies/terms/

[3] por. ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883), Dyrektywa 95/46/WE PE i Rady

[4] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers", March 2012

[5] E. Moglen, "Freedom in the cloud…"

Internet tycoons gain power by having the knowledge about the actual content of the Net traffic. Only these tycoons have both huge data resources and proper analytical tools necessary to understand what is really going on. Communicating through centralized platforms such as e-mail servers, social networks or WWW servers & browsers enabled Google, or Facebook or Amazon to collect data about our e-behavior, in a convenient way – by the retention of logs. Every server collects logs, that is lists of all received requests, clients' IP addresses, requests' dates and many more. The logs origin was strict technological – they enabled finding occurring problems and debugging them. Yet, as the Web-traffic on the central junctions was constantly growing the logs itself gained commercial value. Gathered together they enabled their holders to create profiles of behavior of every IP address they had noticed. This was a revolution. A solely technological decision taken by some engineers in the 90s, that the logs would be collected, lead to current legal problems, where our privacy is regularly infringed. "They put the logs where innocence would be tempted. They put the logs where the failed state of human beings implies eventually bad trouble, and we got it."[6]

Here is an example of a typical log entry where the search is for "cars", followed by a breakdown of its parts:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user's ISP (Internet Service Provider); depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet;
- `25/Mar/2003 10:15:32` is the date and time of the query;
- `http://www.google.com/search?q=cars` is the requested URL, including the search query;
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used; and
- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted

[6] Ibidem

the cookie from the computer since the last time s/he visited Google, then it will be the unique cookie ID assigned to the user the next time s/he visits Google from that particular computer).[7]

As you may see, not only the IP address is crucial for profiling, but also the cookies. Cookies are text files send from the server to the web browser, and contain such information as: preferred language, the region you are in, text size, font, and other personalized parts of web pages, information on how many times people who click on ads end up purchasing those advertised products, the pages users visit most often, and whether users get error messages from certain pages. Cookies help to personalize ads. Google uses also a cookie called 'recently_watched_video_id_list' so that YouTube can record the videos most recently watched by a particular browser.[8] Cookies are being saved in your web browser, so the Net service providers can identify a single user. Imagine, there are no cookies at all. Identification only by the IP address would be often misleading – the more users are under one IP (as it is often in a household or a public institution), the less precise profiling would be.

Retention of logs showed the silicon companies the way to make money on information retention in general. For instance, get down to Google. In 2010 they introduced a new search engine called "Caffeine"[9]. Its goal was to improve the effectiveness of searching as well as its speed. "Caffeine" is analyzing our requests, phrases we are looking up and scrupulously recording them. Then, every time we type some phrases to the search engine it is predicting what would suit us the most. Therefore Google is able to present results individualized for us – different from what other users get. However, Google is not only a search engine. The main source of its income are advertisements exposed via AdWords an AdSense. Both of them are using profiling, with the purpose of presenting us ads that will attract our attention as effective as possible.

3. Is profiling more harmful or more convenient?

While answering this question we would like to differ the consumers' and entrepreneurs' points of view.

[7] Log example presented by Google, [on line] http://www.google.com/intl/en/policies/privacy/key-terms/#toc-terms-server-logs
[8] Types of cookies used by Google, [on line] http://www.google.pl/intl/en/policies/technologies/types/
[9] W. Orliński, „Osobliwy film 'Ona', czyli Lem to wszystko przewidział", [on-line] http://m.wyborcza.pl/wyborcza/1,132748,15527181,Osobliwy_film__Ona___czyli_Lem_to_wszystko_przewidzial.html

A profiled consumer seems to be a happy consumer. Algorithms which had recognized his or her needs and interests, suggest them the most appropriate products and services. The advertisements concern only these things the consumer is willing to pay for. As it is said by Peter Leonard, many people just condone it. They: "understand that enabling geo-location on mobile devices for a particular app enables the provider of that app to target the content of offers to them based upon that location"[10] and still accept it. What is more, they are fully satisfied. While shopping on Amazon a consumer does not have to be curious, persistent and creative to find a ravishing book. He can be unusually lazy and not widely read, but Jeff Bezos's algorithms will still suggest him such a book. All in just few seconds.

Another advantage of profiling can be described from the entrepreneurs' perspective. Their income is growing, thanks to more precise targeting of both their products and advertisements. According to Andre-Yves Portnoff, "information in its raw form has no more value than a block of stone without sculptor. If you have enough good judgment to sort out the information and manipulate it you can produce knowledge"[11]. One could finish this quote up, with the phrase "knowledge on marketing".

What about the disadvantages of profiling? The vast majority of huge search engines is nowadays using profiling to adjust the search results to the users preferences. They analyze the up to now e-behavior and conclude which websites or products would be the most suitable ones. Is it hazardous for the customers? Unfortunately, it is. Using such a search engine may result in separation from information contrary to our viewpoints. Filter Bubbles, as first described by an Internet activist Eli Pariser, could strongly restrict our intellectual freedom. They are: "personal ecosystems of information that's been catered by these algorithms to who they think you are"[12]. The mechanism is quite simple – profiling systems are trying to avoid juxtaposing us with ideas we do not like. It is happening inter alia in Google, Facebook, Yahoo or Amazon[13]. We are being catalogued into groups of similar interests to whom similar goods might be sold. We are endangered of becoming nothing more but people with minds and souls tailored to the sales target groups.

[10] P. Leonard, "Customer data analytics: privacy settings for 'Big Data' business", International Data Privacy Law 2014, Vol. 4, No. 1
[11] A.Y. Portnoff, "Betting on Intelligence of Chips, Mice and Men'
[12] L. Parramore, Interview with E. Pariser "The Filter Bubble", [on line] http://www.theatlantic.com/daily-dish/archive/2010/10/the-filter-bubble/181427/
[13] Ibidem

An undoubtedly fascinating and ambiguous issue arising from the profiling mechanism is the possibility of setting different prices to different consumers. Such a possibility was examined by the United Kingdom Office of Fair Trading[14]. According to their report it is possible that in the future there will be no longer any fixed prices. The new ones will be based on peoples' commercial behavior: individual shopping preferences, purchasing history, internet-searching history and many more. Business will be able to create different prices for everything for everybody. The e-commerce will become similar to the art market. Every good will be worth as much as the business thinks the customer is willing to pay.

One may say, such a scenario will never come true. Yet, it already have come true. People are often using this mechanism and what is more interesting, are quite happy about it. These are of course the air tickets selling systems. In the budget airlines it is obvious to every passenger, that their neighbor might have paid a different price for the same flight[15]. While searching for a convenient route to an interesting place a profile of us is being quickly constructed. Every click on every button on the webpage is a valuable data for the pricing algorithms. The more interest on a specific direction we have, the less probable it is that we will find a cheap special offer. But, does it bother anyone?

Therefore, a question arises, whether you can name such a system a fair one? At first glance the idea of flexible, tailored prices appears creepy and spooky. We were raised surrounded by the heritage of the European civilization, where the art of haggling never became really popular, unlike in the Middle East or the African countries. Though, maybe this is the future? Maybe Internet will introduce the new method of conducting the global trade – with adjustable, personalized prices. Still, at this point we reach the philosophical dilemma. Would it be more fair if the price will remain a proportional part of our income, rather than a stiff nominal value? Would be justified to demand a higher price from wealthy people, and give a discount to the poor ones? We do not have a clue, what would be the right thing to do. However we are strongly convinced that this question is one of the most important ethical issues arising from the development of the profiling process.

[14] United Kingdom Office of Fair Trading, "Personalised Pricing: Increasing Transparency to Improve Trust", OFT 1489, May 2013, p. 2, [on line] http://www.oft.gov.uk/shared_oft/markets-work/personalised-pricing/oft1489.pdf

[15] B. Summers, "Airlines reveal ticket pricing strategies", Los Angeles Daily News, 28.06.2013 [on line] http://www.dailynews.com/general-news/20130629/airlines-reveal-ticket-pricing-strategies, also: R. Seaney, "Understanding Airline Ticket Prices: Why Your Seatmate's Airfare Cost More (or Less) than Yours", FareCompare, 7.01.2011, [on line] http://www.farecompare.com/ask-rick/understanding-airline-ticket-prices-why-your-seatmates-airfare-cost-more-or-less-than-yours/

4. Present regulations

Though the contemporary European 95/46 Directive does not mention profiling explicitly, one can find a number of regulations there which could apply to profiling. The article 38 of the recitals makes it clear, that: "the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him"[16]. This issue is one of the most important while considering the profiling process. It is alarming that most often people just do not realize that some information were just gathered. The article 2 defines the crucial phrases such as processing of personal data (which means: "any operation or set of operations which is performed upon personal data, whether or not by automatic means (…)")[17] or the personal data filing system ("any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis")[18]. It is quite visible that both of these definitions cover with their semantic range the pivotal elements of the profiling process. Their only weak point is the "personal data" term. The definition of "personal data", which is also in the article 2, does not cover the so-called data dandruff of life, as mentioned above. Unfortunately, the most dangerous profiling (as described in this paper) is nowadays based on this "dandruff" itself. Thus, even if the specific definitions (processing of personal data and personal data filing system) are wisely constructed, the general definition of personal data narrows the scope of implementing the whole Directive.

Article 6 could also cause a lot of trouble if referred to profiling. It says that personal data should be collected: "(…) for specified, explicit and legitimate purposes"[19]. There is a huge problem. Even assuming that data dandruff may be considered as personal data, there is no reasonable possibility to fulfill the requirements of this article. While collecting the data dandruff from the Net no one is able to predict the purpose of collecting these data.

5. Origins of the EU Draft Regulation

That would be nothing more than truism to notice that our reality is in a state of constant flux. Progress and development in technology affects more and more fields of social activities every year. Individuals make personal information available publicly and globally. The access to the information is allowed for both private companies and public authorities. They

[16] EU Directive 95/46/EC
[17] Ibidem
[18] Ibidem
[19] Ibidem

can make use of personal data on an unprecedented scale in order to pursue people activities. It significantly transformed the economy of European Union. One of flagship initiatives of 10-year strategy proposed for advancement of the economy of the European Union, named **Europe 2020** is named '**A digital agenda for Europe'**. It aims to reap the benefits of a digital single market for households and firms. That means nothing more than creating a new, comprehensive legal framework which will support economic growth. In online development a key to innovation and development is trust of consumers for online shopping to avoid risk which is always a slowdown for growth. According to statistics presented by European Commission, nine out of ten Europeans (92%) say they are concerned about mobile applications collecting their data without their consent and seven Europeans out of ten are concerned about the potential use that companies may make of the information disclosed.[20] Thus, personal data protection is a central point in current debate and resulted in a draft regulation on data protection which is supposed to replace a former one.

The regulation of 95/46 directive is simply outdated and is no longer a sufficient guarantee for data protection. It is considered as a source of 'red tape' which for sure is an obstacle to sustainable and efficient development, especially of small and medium enterprises. What is more, the political background of this regulation seems to be an important trigger in data protection reform. In globalized markets reality, according to words of Vice-President Viviane Reding, the EU's Justice Commissioner, *strong data protection rules must be Europe's trade mark. Following the U.S. data spying scandals, data protection is more than ever a competitive advantage.* [21] For digital economy, data is a kind of trade good. It should not be used without a regard to Article 8 of the Charter of Fundamental Rights of the EU, which enshrines protection of personal data as a fundamental right. For all these reasons, Europe needs one, coherent and strong regulation. As it was proposed by the Commision, three main pillars of the regulation are supposed to be the basis for achieving that aim. First: one continent – one law. Secondly, the rule of 'one-stop-shop', what means one supervisory authority gaining control and entitled to impose sanctions. Last, but not least - the same rules for all companies regardless their establishment. What are the consequences of that model, and other specific regulations, to the issue of profiling? Let us take a closer look on what every legal analysis starts from - the definitions.

[20] Flash Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union, June 2011

[21] European Commission - MEMO/14/186 12/03/2014
http://europa.eu/rapid/press-release_MEMO-14-186_pl.htm

6. Key points of the EU Draft Regulation concerning profiling

During the consultations, profiling has been a crucial issue in the works of Article 29 Data Protection Working Party. On 13 May 2013, they presented an advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation. They constructed the following definition of profiling, which was proposed to be included in article 4 containing legal definitions:

> "Profiling" means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements."[22]

The second very important document which indirectly influences the Draft is the Recommendation CM/Rec(2010)13 of the Council of Europe on the protection of individuals with regard to automatic processing of personal data in the context of profiling. [23] It contains the following definitions which influenced how the article 20 was formulated:

> *d.* "Profile" refers to a set of data characterizing a category of individuals that is intended to be applied to an individual.
>
> *e.* "Profiling" means an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

As we can see, there are two different visions of how profiling should be defined. First one is constructed on example features of natural person which can be predicted using the data; it is more 'functional'. It poses typical for casuistry problems – what is not included in the definition? It seems that the second proposition, which is one step behind and concerns just the technique of creating a profile, would be more sufficient. Nevertheless, in the Proposal

[22] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/annex_one-stop_shop_20130513_advice-paper-on-profiling_en.pdf
[23] https://wcd.coe.int/ViewDoc.jsp?id=1710949

released in 25.1.2012, profiling was not included in the chapter 1 with general provisions, but was regulated only in section 4, article 20. However, it is worth to emphasize, that having a legal definition in introductive chapter significantly increases the importance of a certain issue. That is why the query of Article 29 Data Protection Working Party, to add a proper legal definition there, seems to be justified.

What is more, the shape of article 20 is also highly disputative. In the proposal in was formulated in a following way:

> **SECTION 4**
> **RIGHT TO OBJECT AND PROFILING**
>
> *Article 20*
> ***Measures based on profiling***
> 1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.
> 2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:
> (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or
> (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or
> (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.
> 3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

It was noticed, that the regulation proposed by the Commission still merely focuses on the outcome of profiling – i.e. "a measure which produces legal effects concerning this natural person or significantly affects this natural person". It seems that profiling as such, i.e. the creation and the use of personal profiles by data controllers, before a measure or even decision is taken which has an effect on the data subject is below the scope of this article. That is why it was recommended to determine a more comprehensive approach which would contain specific legal requirements not only for the usage and further processing of personal data but already for the collection of data for the purpose of profiling and the creation of profiles as such. Thus, the following additional elements were suggested by the Article 29 Data protection Working Party to be considered once more:

a. Greater transparency and control for data subjects

It seems that what is missing in the regulation is a legal requirement for explicit consent of data subjects to process the data just for the purpose of profiling. Building on Council of Europe Recommendation CM/Rec(2010)13, paragraph B(4), Article 20 should therefore provide additional information requirements for data controllers, including information that personal data will be used in the context of profiling, the purposes for which the profiling is carried out and the logic involved in the automatic processing. Additionally, it seems that a possibility for changing the consent should also be provided. Individual should have the right to access, to modify or to delete the profile information attributed to them and to refuse further decisions based on it. This right is currently not explicitly enshrined in the Draft Regulation. In our opinion the mechanism similar to cookies could be effective, when every individual could have an instant access to what is collected through their personal ID number.

b. More responsibility and accountability of data controllers

While Article 33od the Draft specifies what processing operations should be conducted in a certain risk situations, it lacks measures adjusted strictly to profiling. Such safeguards should comprise the usage of data protection friendly technologies and standard default settings, particularly in the online world, as well as specific measures for data minimization, including obligations or incentives for controllers for anonymization or pseudonymization in the context of profiling, and data security as well as human intervention in defined cases.

c. A balanced approach to profiling

As it was already mentioned, profiling has two dimensions – positive one, as a possibility for more successful marketing campaigns and customer's satisfaction, but it also may pose a certain threat and have negative impact on data security. However, it was noticed, that profiling cannot be assessed by one measure in all cases. In article 20 the recognition that there are different types of profiling with different privacy impacts on individuals was not successful.

Sometimes the collected data is not significantly affecting the data subjects; however, in certain cases the information is more sensitive. That is why some discretionality should be involved in the assessing what measures are sufficient and proportional in certain cases. In the view of the Working Party, this task could best be performed by the European Data Protection Board, which should be empowered to issue guidelines on the interpretation and application of Article 20 in specific processing contexts.

In 1990 when the directive was implemented, the phenomenon of profiling was neither wide spread nor invasive. This situation changed only in the past decade. That is why the word 'profiling' not even appears in the 95/46 directive. However, the article 15 is deemed as a basis for a legal regulation of profiling as it refers to automated individual decisions. However, it lays restrictions only on the process of profile application, not creation. It means that opposing by the individual the application of a profile is hampered by the lack of information when and how it was created. This problem was pointed out during the consultations and the obligation was formed in paragraph 3 of the article 20. The idea of consent versus privacy by default was raised also. It means that contrary to the current regulation, when consent was required only in certain issues and in others it was supposed to be a result of previous consent, new regulation takes the reverse – without the consent the privacy is the priority.

Other significant changes can be found in Article 4 where definitions of terms used in the Regulation can be found. While some definitions are taken over from Directive 95/46/EC, others are modified, complemented with additional elements, or newly introduced just like profiling. In the definition of consent, the criterion 'explicit' is added to avoid confusing parallelism with 'unambiguous' consent and in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent. In connection with spelled out in article 40 general principle, that the compliance with the obligations of the regulation are mandatory for any transfers of personal data to third countries or international organizations, seems to be a sufficient realization of security principle. Especially if we take a look at the section 3 and the establishment of a comprehensive responsibility and liability of the controller.

7. Context of the Transatlantic Trade and Investment Partnership Agreement – how the profiling issue may influence on the negotiations?

The negotiations of the Transatlantic Trade and Investment Partnership Agreement revolve around 2 main themes: compatibility and protection. As the informative website of European Commission says, the first reason for the agreement is the fact, that cutting unnecessary red tape would reduce the cost of doing business across the Atlantic, mostly because of cost reduction regarding legal advices to comply with both American and European laws. Second, because closer cooperation with the US would make our regulation more effective. Regulators that work together can learn from each other's ideas and reduce costs by reducing the number of inspections and amendments they have to perform. Despite the fact, that data protection is not a crucial point of this agreement, it seems that the new regulation on data protection is deemed as an incentive for negotiations. Clear and coherent laws in European Union and one, independent supervisory authority (European Data Protection Board) will not only allow cutting the costs for American and European business. It also strengthens our position in negotiations and significantly improves the safety of European citizens data what stems from the proportionality principle. Regulation on European level is much more effective, and as we saw, it seems that the new regulation will protect our privacy from infringement. New regulation provides a set of rules which all companies processing data of Europeans needs to obey regardless theirs establishment. The system contains effective sanctions which in relation with the U.S. can be executed more effectively than by single European countries, also with a regard to profiling:

Article 79: Administrative sanctions

1. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

a. processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent (…)

d. does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;

There were no signals in media nor in the official communicates that profiling is a moot point of the negotiations. However, some of the European Parliament Members published their opinions in connection with eavesdropping scandal in 2013, that mutual trust was abused and further negotiations should be suspended until the privacy regulation will meet similar standards. Nevertheless, it seems that growing importance of profiling in everyday life and in the strategy of contemporary marketing, should meet with greater social interest and clearer informative campaign from big corporations. It seems that internet will become one market square, where your only privilege will be that adverts you are surrounded by will meet your previous interest. Furthermore, isn't the strategy of adjusting offers and prices to your possibilities a kind of threat to how you perceive the world? To find answers for that question we need time, but first of all – we need awareness, what the internet is nowadays about.

8. Bibliography:

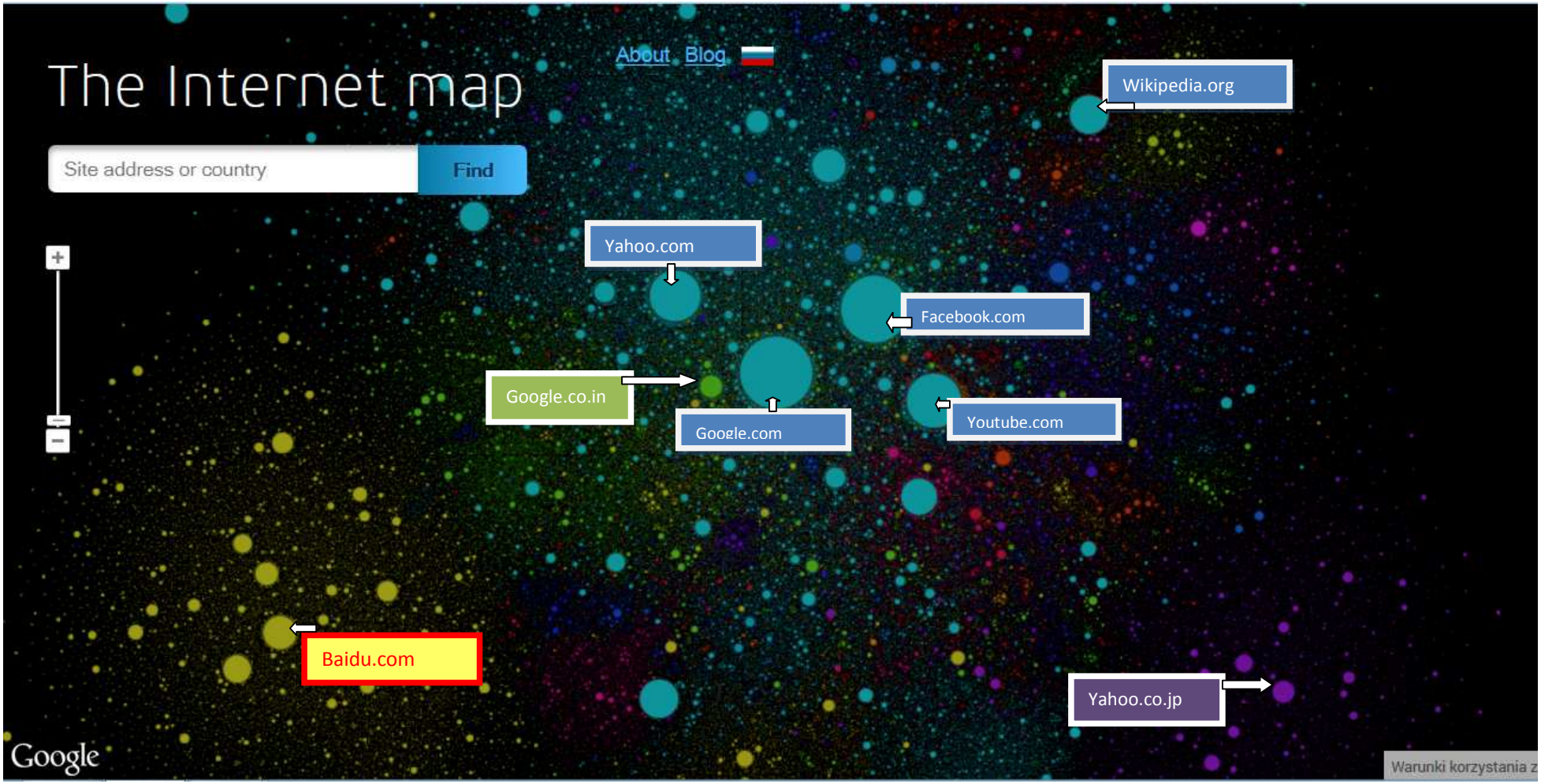
1. Source Materials:
    a. *"Proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"* [on line] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF
    b. *"Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"*, [on line] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
    c. *"Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych"*, Dz.U. 1997 Nr 133 poz. 883
    d. *"Google Terms of Service"*, 14.04.2014, [on line] https://www.google.com/intl/en/policies/terms
    e. *"Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers"*, Federal Trade Commission, 2012, [on line] http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
    f. "*Personalised Pricing: Increasing Transparency to Improve Trust"*, United Kingdom Office of Fair Trading, OFT 1489, 2013, [on line] http://www.oft.gov.uk/shared_oft/markets-work/personalised-pricing/oft1489.pdf
    g. *"Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union"*, June 2011 [on line] http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
    h. *"European Commission - MEMO/14/186. Progress on EU data protection reform now irreversible following European Parliament vote"*, 12.03.2014, [on line] http://europa.eu/rapid/press-release_MEMO-14-186_pl.htm
    i. *"Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation"*, 13.05.2013, [on line] http://ec.europa.eu/justice/data-protection/article-

29/documentation/other-document/files/2014/annex_one-stop_shop_20130513_advice-paper-on-profiling_en.pdf

2. Reference Works:
    a. *"Freedom in the Cloud"*, E. Moglen, [on-line] www.softwarefreedom.org
    b. *"Who Controls the Internet. Illusions of a Borderless World"*, J. Goldsmith, T. Wu, 2006, ISBN 978-0-19-515266-1
    c. *"Customer Data Analytics: privacy settings for Big Data business"*, P. Leonard, International Data Privacy Law, Oxford Journal, 2013
    d. *"Editor's choice: Big Data: The End of Privacy or a New Beginning?"*, I.R. Rubinstein, International Data Privacy Law, Oxford Journal, 2013
    e. *"The protection of privacy in Poland in the digital environment"*, I. Kowalczuk, K. Szymielewicz, T. Rychlicki, International Data Privacy Law, Oxford Journal, 2011
    f. *"Security, privacy and surveillance in European policy documents"*, D. Barnard-Wills, International Data Privacy Law, Oxford Journal, 2013
    g. *"The European data protection framework for the twenty-first century"*, V. Reding, International Data Privacy Law, Oxford Journal, 2013
    h. *"Betting on Intelligence of Chips, Mice and Men"*, A.Y. Portnoff, 2004, ISBN 2-84387-303-7
    i. *"The Filter Bubble: What the Internet Is Hiding from You"*, E. Pariser, 2011 ISBN 978-1-59420-300-8
    j. *"Ochrona danych osobowych w sieci"*, M. Brzozowska, 2012, ISBN 978-83-62723-22-5
    k. *"Cyberkultura prawa. Współczesne problem filozofii i informatyki prawa"*, J. Janowski, 2012, ISBN 978-837641-655-7
    l. *"Ius internet. Między prawem a etyką"*, J. Kulesza, 2010, ISBN 978-83-7644-080-4
    m. *„Ochrona danych osobowych. Komentarz"*, J. Barta, P. Fajgielski, R. Markiewicz, 2011, ISBN 978-83-264-1481-7
3. Press articles:
    a. *"Osobliwy film 'Ona', czyli Lem to wszystko przewidział"*, W. Orliński, Gazeta Wyborcza, 26.02.2014, [on-line] http://m.wyborcza.pl/wyborcza/1,132748,15527181,Osobliwy_film__Ona___czyli_Lem_to_wszystko_przewidzial.html

b. *"Interview with E. Pariser 'The Filter Bubble'"*, L. Parramore, The Atlantic, 10.10.2010, [on line] http://www.theatlantic.com/daily-dish/archive/2010/10/the-filter-bubble/181427/
c. *"Airlines reveal ticket pricing strategies"*, B. Summers, Los Angeles Daily News, 28.06.2013 [on line] http://www.dailynews.com/general-news/20130629/airlines-reveal-ticket-pricing-strategies
d. *"Understanding Airline Ticket Prices: Why Your Seatmate's Airfare Cost More (or Less) than Yours"*, R. Seaney, FareCompare, 7.01.2011, [on line] http://www.farecompare.com/ask-rick/understanding-airline-ticket-prices-why-your-seatmates-airfare-cost-more-or-less-than-yours/

Appendix 1


The Internet map
About
Blog
Site address or country
Find
Wikipedia.org
Yahoo.com
Facebook.com
Google.co.in
Google.com
Youtube.com
Baidu.com
Yahoo.co.jp
Google
Warunki korzystania z

Appendix 2

The Top Sites on The Web by alexa.com

1. Google.com
2. Facebook.com
3. Youtube.com
4. Yahoo.com
5. Baidu.com
6. Wikipedia.org
7. Qq.com (China's largest and most used Internet service portal)
8. Taobao.com (the most popular consumer-to-consumer (C2C) online marketplace in China)
9. Twitter.com
10. Amazon.com
11. Linkedin.com
12. Live.com
13. Google.co.in
14. Sina.com.cn
15. Blogspot.com
16. Halo123.com
17. Weibo.com
18. Vk.com
19. Tmall.com
20. Yahoo.co.jp