

**INTERNET PRIVACY IN THE CONTEXT OF ONLINE ADVERTISING**

...

**A COMPARATIVE ANALYSIS OF THE US AND EU APPROACHES**

by Boris Prastalo

LL.M. SHORT THESIS  
COURSE: Legal Aspects of Electronic Commerce  
PROFESSOR: Caterina Sganga, Ph.D.  
Central European University  
1051 Budapest, Nador utca 9.  
Hungary

# Contents

Abstract .....	iii
Introduction.....	1
Chapter 1: What Is Online Advertising? .....	3
1.1 Types of Online Advertising .....	5
1.2 How Does Online Advertising Work?.....	7
Chapter 2: Economic and Social Impact of Online Advertising .....	9
Chapter 3: How Does Online Advertising Impact Privacy? .....	12
Chapter 4: The US Approach to Internet Privacy and Online Advertising .....	15
4.1. Federal Trade Commission .....	17
4.2 Electronic Communications Privacy Act .....	18
4.3 Children's Online Privacy Protection Act .....	20
Chapter 5: The EU Approach to Internet Privacy and Online Advertising.....	22
5.1 Data Protection Directive.....	23
5.2 Directive on Privacy and Electronic Communications .....	25
5.3 Safe Harbor Principles .....	27
Conclusion .....	28
Bibliography.....	32

## Abstract

This thesis examines, in a comparative context, the legal approaches of the United States and the European Union in relation to the issue of online advertising and privacy. It first explains, in general terms, the concept of online advertising, followed by an in-depth elaboration of its focal characteristics. The focus then shifts to legislative acts and judicial decisions of the two aforementioned jurisdictions. Finally, remarks and suggestions as to how online advertising should be regulated are put forth. While acknowledging the fears that privacy advocates have been very vocal about, this thesis accepts the new reality which exists online, and suggests ways in which this new reality can be better regulated.

## Introduction

With the emergence of the Internet, the world as we all know it changed forever. Instead of the common frustration of going to the library and spending hours and hours locating the desired materials, one can just, after several clicks, open a scholarly database online and find those materials in a couple of minutes. Long distances no longer prevent us from keeping in touch with our friends and family thanks to a wide array of social networks. Back in the day, expressing one's artistic side to the general public tended to be a cumbersome and time-consuming task. That is not the case anymore. The Internet allows us to share our artistic endeavors online by, for example, posting a video of them on YouTube or writing a literary piece on a blog. But besides having a deep social and cultural impact, the Internet has also brought about core changes in the world of business. A quintessential illustration of this is the Internet's impact on the advertising industry. Nowadays, thanks to the cutting-edge technological improvements, online advertising appears to be more productive than conventional advertising.<sup>1</sup> For example, large search engines such as Google will, in accordance with what one searches online, target the potential consumers with advertisements. Electronic commerce companies such as Amazon will use shopping history of their clients in order to advertise similar products directly to them either via e-mail or through the consumers' user accounts. Social networks such as Facebook will turn to the contents of our profiles and social interactions in order to determine our interests, and, in accordance with that, advertisements will be displayed. Obviously, these business practices tend to be, from an economic standpoint, very efficient in a sense that they are targeting a specific consumer who could, as indicated by the history of his web search and prior shopping, actually purchase the good.<sup>2</sup> In other words, the advertisements are actually delivered to those who are likely to purchase the good or service in question, and not delivered to those who are not. However, these practices, although efficient from

---

<sup>1</sup>. David S. Evans, "The Online Advertising Industry: Economics, Evolution, and Privacy," *Social Sciences Research Network*. Accessed at January 18, 2014 at <http://ssrn.com/abstract=1376607>

<sup>2</sup>. Ibid.

an economic standpoint, also raise questions concerning privacy on the Internet.

This thesis examines the impact of online advertising on privacy, focusing on its behavioral targeting aspects. The first part of the thesis gives a general overview of the topic at hand. It explains what online advertising consists of, what types of online advertising exist, and how it actually works in practice. The second part reveals what the social and economic impact of online advertising is whereas the third part examines its effect on privacy. The fourth and fifth parts explore how online advertising is actually regulated in two major jurisdictions, the United States and the European Union, by delving into statutory regulation and judicial decisions. This is followed by the sixth part, an in-depth discussion of the scholars' views on the matter and the author's own remarks and suggestions. The thesis concludes on a note that, owing to the well-founded notion that online advertising tends to be viable and efficient from an economic and social standpoint, the law needs to reflect that by striking a satisfactory balance with the provisions on Internet privacy. The law ought not to impair the ability of companies such as Google to efficiently deliver us ads. Its aim should be to allow the gathering of personal data for certain purposes (e.g. online advertising) but in case of an unauthorized sharing of such data or any misuse whatsoever, the aim should then be to impose liability on the company responsible for such misuse or any unauthorized sharing.

## Chapter 1: What Is Online Advertising?

Advertising is defined as a communication of a commercial nature directed towards the general public or a particular group with the aim to encourage or bring about a certain type of action.<sup>3</sup> More precisely, advertising attempts to persuade potential buyers to purchase advertised goods and services. Online advertising, or Internet advertising, does basically the same thing. The only difference is that online advertising utilizes the Web to achieve its goal.

In recent years in the United States, online advertising has been enjoying significant expansion, both in terms of market share and total revenue.<sup>4</sup> In the years to come, online advertising is expected to grow even further.<sup>5</sup> Broadcast television advertising, along with the newspaper advertising, has been at the forefront of the industry for a number of years. For the sake of illustration, broadcast television advertising and newspaper advertising had virtually the same market share, and their combined revenues stood at approximately 90 billion dollars.<sup>6</sup> In contrast, online advertising in 2007 was still not as lucrative as its counterparts, with its revenues standing at approximately 20 billion dollars.<sup>7</sup> However, in 2011, online advertising scooped in 31.74 billion dollars in revenues.<sup>8</sup> Next year, online advertising saw an impressive rise in its revenues compared to the previous year. In 2012, its revenues increased by 15.2 %, and at that point they stood at 36.57 billion dollars.<sup>9</sup> Broadcast television advertising, on the other hand, experienced a decrease in its revenues when compared to year 2007. In 2009, broadcast television advertising hit its low in terms

---

<sup>3</sup>. “What Is Advertising?” *The University of North Carolina at Pembroke*, accessed March, 15, 2014, <http://www2.uncp.edu/home/acurtis/Courses/ResourcesForCourses/Advertising/AdvertisingWhatIsIt.html>

<sup>4</sup>. Evans, “The Online Advertising Industry,” *SSRN*.

<sup>5</sup>. “IAB Internet Advertising Revenue Report.” *PwC*, 2013. [http://www.iab.net/media/file/IAB\\_Internet\\_Advertising\\_Revenue\\_Report\\_FY\\_2012\\_rev.pdf](http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2012_rev.pdf)

<sup>6</sup>. *Ibid.*

<sup>7</sup>. *Ibid.*

<sup>8</sup>. *Ibid.*

<sup>9</sup>. *Ibid.*

of revenue when it managed to only receive approximately 35 billion dollars.<sup>10</sup> Since 2009, broadcast television advertising has been slowly recovering from its slump, but the figures have not been impressive when compared to those of online advertising.<sup>11</sup>

In Europe, the same trend can be observed as in the United States. Online advertising has been on its constant rise, and is expected to grow in the future as well. Since 2007, it has been experiencing impressive growth figures. In 2007, its revenues grew by 40 % when compared to the previous year.<sup>12</sup> After the economic turmoil in 2008, online advertising still managed to grow. In 2008, it grew by 20.2 %.<sup>13</sup> In 2010, the growth stood at 15.3 %, with the revenues reaching a mind-blowing 18.3 billion euros.<sup>14</sup> 2011 was another successful year, with the revenues totaling 20.9 billion euros, an increase by 15.1 % compared to 2010.<sup>15</sup> In 2012, they rose by a solid 11.5 %.<sup>16</sup>

In the light of the statistics presented above, it is clear that online advertising will continue to grow. Significant boost to its growth will be given by the smartphone industry since mobile advertising is achieving very strong growth figures. For example, in the United States in 2011, its market share stood at 5 %.<sup>17</sup> The very next year, its market share skyrocketed to 9 %.<sup>18</sup> In Europe, mobile advertising has been growing strongly as well. In 2011, the market share of mobile advertising in the UK, France, and Spain stood at 5.3 %, 5.2 %, and 3.7% respectively.<sup>19</sup> In other

---

<sup>10</sup>. Ibid.

<sup>11</sup>. Ibid.

<sup>12</sup>. “Adex Benchmark 2012: European Online Advertising Expenditure.” *Interactive Advertising Bureau Europe*, 2013. [http://www.iab.nl/wp-content/uploads/downloads/2013/08/2013\\_08\\_28\\_IAB\\_Adex\\_Benchmark.Pdf](http://www.iab.nl/wp-content/uploads/downloads/2013/08/2013_08_28_IAB_Adex_Benchmark.Pdf)

<sup>13</sup>. Ibid.

<sup>14</sup>. “Adex Benchmark.” *IAB Europe*, 2013.

<sup>15</sup>. Ibid.

<sup>16</sup>. Ibid.

<sup>17</sup>. “IAB Report.” *PwC*, 2013.

<sup>18</sup>. Ibid.

<sup>19</sup>. “Adex Benchmark 2011: European Online Advertising Expenditure.” *Interactive Advertising Bureau Europe*, 2012. [http://www.iabeurope.eu/files/9113/6852/1903/2011\\_adex\\_benchmark\\_final.pdf](http://www.iabeurope.eu/files/9113/6852/1903/2011_adex_benchmark_final.pdf)

European countries for that year the percentages were significantly lower.<sup>20</sup> But in 2012, in Western Europe as a whole, the total revenues stood at 1.2 billion euros, and the market share was 16.9 %.<sup>21</sup> Hence, it can be concluded with with a fair amount of certainty that the future of advertising lies online, and its economic and social impact shall be felt even more strongly in the years to come.

### 1.1 Types of Online Advertising

Online advertising can take on a number of different formats. Usually, online advertisements are divided into the following categories: search, banners, classifieds, mobile, digital video, lead generation, sponsorship, rich media, e-mail, and interstitials.<sup>22</sup>

Search advertising is a scheme through which Internet companies, mainly those which operate search engines, link a particular word or a phrase to a website which is to be advertised.<sup>23</sup> If a user types in the words “book a hotel” on Google, the first three delivered results are labeled with a small orange box containing the word “ad.” Those first three websites are actually paying to Google to be shown before all other websites when a user searches for particular words. This practice is referred to as paid listings.<sup>24</sup> Contextual searches and paid inclusions also fall under the scope of search advertising. Paid inclusion describes a situation when the marketer pays to have his website indexed by a search engine.<sup>25</sup> Contextual searches represent a form of advertising in which an ad is displayed on a web-page whose contents are similar or somehow related to the ad.<sup>26</sup>

---

<sup>20</sup>. Ibid.

<sup>21</sup>. “Global Mobile Advertising Revenues Surge 82.8 % in 2012, Hitting a High of \$8.9 Billion,” *Interactive Advertising Bureau*, last modified July 9, 2013, [http://www.iab.net/about\\_the\\_iab/recent\\_press\\_releases/press\\_release\\_archive/press\\_release/pr-070913](http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070913)

<sup>22</sup>. Evans, “The Online Advertising Industry,” *SSRN*.

<sup>23</sup>. Ibid.

<sup>24</sup>. Ibid.

<sup>25</sup>. Ibid.

<sup>26</sup>. Ibid.



Banners come in the shape of a rectangular, and are displayed on websites in places where they can easily grasp the target's attention.<sup>27</sup> Classifieds are advertisements which usually appear in newspapers or in online periodicals. They basically list a product or a service in return for a fee.<sup>28</sup> Mobile advertising refers to those advertising practices which target directly mobile phones and tablets. Digital video advertising is usually delivered through downloadable, live, or streaming content.<sup>29</sup> In case of a streaming content, an advertisement can be shown before, during, or after the content in question. Lead generation is a form of advertising strategy which aims to generate interest from a particular group of consumers or to determine a class of consumers which would be interested in a particular product.<sup>30</sup> A lead can be, for example, something very simple as an age or contact information of a consumer. Lead generation was mostly conducted offline in the past, but with the advance of new technologies, a lot of it has moved online. Sponsorship online usually comes in the form of re-skinning of a portion of a website or including a watermark shaped as the advertiser's logo.<sup>31</sup> Rich media refers to a type of online advertising which utilizes or incorporates animation or sound.<sup>32</sup> E-mail advertising involves sending e-mail messages with commercial content to potential customers with the aim of persuading them to buy a good or a service.<sup>33</sup> Interstitials are advertisements which are displayed during the user's transition from one website to another.<sup>34</sup>

---

<sup>27</sup>. Ibid.

<sup>28</sup>. Ibid.

<sup>29</sup>. Ibid.

<sup>30</sup>. Ibid.

<sup>31</sup>. Ibid.

<sup>32</sup>. Ibid.

<sup>33</sup>. Ibid.

<sup>34</sup>. Ibid.

## 1.2 How Does Online Advertising Work?

For the purpose of this thesis, this subchapter will describe technical aspects of how advertisements are delivered online. However, it has to be noted that only those advertising practices which impact privacy will be dealt with. Hence, the emphasis is on the behavioral targeting, and all the technical steps which make this practice a reality.

Behavioral targeting is defined as gathering of private data related to an individual's behavior online which is then used to show advertisements to that individual in accordance with his, or her, web searches and browsing preferences.<sup>35</sup> To achieve this, websites use a variety of tools, but none are as popular and as efficient as cookies. When a user is browsing a website or using a search engine, a cookie will usually be placed and stored on that user's computer.<sup>36</sup> A cookie, which is nothing more than a very small piece of data, shall notify the website which sent it in the first place about the user's previous browsing history when that user visits that particular website again.<sup>37</sup> Moreover, the cookie enables the website to recognize its repeat visitors.<sup>38</sup> The stored cookie can determine the user's browsing history going back not only months, but in certain instances even years.<sup>39</sup> Thanks to the cookies, the websites are able to determine users' preferences. More precisely, they acquire knowledge as to their personal interests, hobbies, travel inquiries, business-related information, etc. Once they obtain this, the next step is audience segmentation.<sup>40</sup> More precisely, all the data gathered in this manner are divided into segments according to their similar characteristics, and are added to the previously created data segments.<sup>41</sup> Now, if the advertiser wants to display an

---

<sup>35</sup>. Ibid.

<sup>36</sup>. "How Does Online Advertising Work," YouTube video, 1:59, posted by "Interactive Advertising Bureau UK," July 18, 2012, <https://www.youtube.com/watch?v=Y9Y4Efyxmk4>

<sup>37</sup>. Ibid.

<sup>38</sup>. Ibid.

<sup>39</sup>. Ibid.

<sup>40</sup>. Ibid.

<sup>41</sup>. Ibid.

advertisement, he chooses a segment which best fits a product or service that he is trying to sell, and the advertisement will be shown to all the users whose browsing history was put into that particular segment.<sup>42</sup> It has to be said that through these practices certain personal data such as names, e-mails, and phone numbers are not collected.<sup>43</sup>

E-mail services such as Yahoo Mail and Gmail have also entered a lucrative realm of online advertising. When signing up for these e-mail services, one should be aware of the fact that their users do not have a reasonable expectation of privacy.<sup>44</sup> Their e-mail messages are scanned, and in accordance with the content of those messages, context-sensitive advertisements are displayed.<sup>45</sup> Even users using e-mail services of a provider who does not scan its users' messages are not protected if they correspond with persons using, for example, Gmail or Yahoo e-mail services.<sup>46</sup> As was stated by Google,

“... all users of email must necessarily expect that their emails will be subject to automated processing ... Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based email today cannot be surprised if their communications are processed by the recipient's ECS [electronic communications service] provider in the course of delivery.”<sup>47</sup>

---

<sup>42</sup>. Ibid.

<sup>43</sup>. Ibid.

<sup>44</sup>. Dominic Rushe, “Don't Expect Privacy When Sending to Gmail,” *The Guardian*, August 15, 2013, <http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit>

<sup>45</sup>. Rushe, “Don't Expect Privacy When Sending to Gmail,” *The Guardian*, 2013.

<sup>46</sup>. Ibid.

<sup>47</sup>. Ibid.

## Chapter 2: Economic and Social Impact of Online Advertising

The economists say that advertising is a distinct characteristic of monopolistic competition.<sup>48</sup> This means that products which are highly differentiated from products of the same type are usually the ones which get to be advertised to the general public or a specific group of consumers. Nowadays, everybody with differentiated products is using advertising, and this, of course, eats up a huge amount of resources. It is estimated that around 2 % of the total firm revenue gets spent on advertising.<sup>49</sup> Why do companies advertise their products and services? Economic theory explains this through the concept of prisoner's dilemma.<sup>50</sup> If nobody advertised, then all the producers competing for the same consumers would be better off since none of them would be spending their earned money on advertising. Hence, their profits would be higher. If only certain producers decided not to advertise, they would be worse-off in comparison to their counterparts who did decide to advertise. This is because advertising would cause a huge number of consumers to change teams and purchase those goods which are being advertised.<sup>51</sup> Consequently, owing to the fact that one can never know what his competitors might do next, producers with differentiated products decide to use advertising instead of relying on others not to advertise. Even if producers colluded and decided not to advertise, there would always be a possibility that one or more producers might break their promise, which, of course, would be detrimental to all those who did not advertise.<sup>52</sup>

Therefore, due to their prisoner's dilemma, the inevitable reality is that all the producers with differentiated products will resort to advertising.<sup>53</sup> The question is then, what kind of advertising is the most efficient and the least resource-wasteful, both from the producers' perspective and society's

---

<sup>48</sup>. Gregory Mankiw. *Principles of Microeconomics*. Cengage Learning, 2006. PDF e-book.

<sup>49</sup>. Ibid.

<sup>50</sup>. Ibid.

<sup>51</sup>. Ibid.

<sup>52</sup>. Ibid.

<sup>53</sup>. Ibid.

perspective? According to many scholars, online advertising fits this description. Alex Blyth, for example, re-enforces this standing by describing online advertising as more affordable than conventional advertising, less risky, and more far-reaching in geographical terms.<sup>54</sup>

Online advertising, however, does share certain traits with offline advertising. Advertising, in general, is thought to provide information to the consumers about the products' characteristics and quality.<sup>55</sup> Advertising usually provides information as to the price of the good in question, entry of new products into the market, and ways in which a product can be purchased.<sup>56</sup> Hence, it is argued that advertising can make consumers more equipped with knowledge, which, in turn, enables them to make an informed decision when buying a good or a service.<sup>57</sup> Of course, a counter-argument can be made that advertising is not informative, but manipulative.<sup>58</sup> Advertising sometimes distorts prices by not including taxes and it can exaggerate the quality of the product. These can be, in certain instances, valid arguments. However, nothing can take away from advertising its informative power in a sense that it tells the consumers that the product exists and that it is out there.

Of course, no advertisement will state that a product lacks quality or durability. Nevertheless, advertising can signal to the consumers whether a product is good and if a producer believes in its success or not.<sup>59</sup> According to the well-established economic theory, advertising will entice consumers to buy the advertised product.<sup>60</sup> However, profit will not be made out of purchases of one-time consumers. If product is not of good quality, a buyer will buy it once, but next time, he,

---

<sup>54</sup>. Alex Blyth. *Brilliant Online Marketing: How to Use the Internet to Market Your Business*. FT Press, 2011. Google Books.

<sup>55</sup>. Mankiw, *Principles of Microeconomics*, Cengage.

<sup>56</sup>. Ibid.

<sup>57</sup>. Ibid.

<sup>58</sup>. Ibid.

<sup>59</sup>. Ibid.

<sup>60</sup>. Ibid.

or she, will opt for a competitor's product.<sup>61</sup> To get a profit, a product needs to attract repeat buyers. If a producer does not believe in his product, it is highly unlikely that he would invest into an expensive advertising campaign.<sup>62</sup> Hence, if an advertising campaign is expensive and well-thought out, that is a signal that the producer believes his product is good, and that he, therefore, expects his product to have repeat buyers. By the same token, if the advertising campaign is economical or non-existent, this can be interpreted as a signal that a producer does not believe the product will break through in the market.<sup>63</sup>

Another established argument in favor of advertising is that it encourages competition.

According to Gregory Mankiw,

“...because advertising allows customers to be more fully informed about all the firms in the market, customers can more easily take advantage of price differences. Thus, each firm has less market power. In addition, advertising allows new firms to enter more easily, because it gives entrants a means to attract customers from existing firms.”<sup>64</sup>

Evidently, advertising, besides serving as a tool which helps producers sell their product, has a wider economic and social purpose. It signals to the consumers whether a product is of quality or not, and it fosters market competition. Therefore, advertising, in general, provides certain benefits to the society. When one adds to this the notion that online advertising, when compared to conventional advertising, is less expensive and less resource-wasteful, but provides the same benefits which offline advertising provides, it is easy to conclude that law needs to take into account all these societal benefits of online advertising when protecting Internet privacy.

---

<sup>61</sup>. Ibid.

<sup>62</sup>. Ibid.

<sup>63</sup>. Ibid.

<sup>64</sup>. Ibid.

### Chapter 3: How Does Online Advertising Impact Privacy?

While we are in the comfort of our own homes and browsing the Web, we feel secure. What we search online and websites we visit are our own private thing, and if we delete browsing history, nobody will know what we just did online. But is that really the case? Most of the average Internet users do not think even in their wildest dreams that someone, or something, is watching their every step they take online. But that is exactly what is going on. Our search queries are remembered and stored and our personal e-mails are being scanned. Thanks to the cookies, even our previous browsing is known to those websites which had installed those cookies on our computers. Obviously, this raises some very troubling privacy concerns.

In his analysis of online privacy, Omer Tene makes frequent references to Daniel Solove's *Taxonomy of Privacy*.<sup>65</sup> According to this approach, when discussing online privacy, a focus should be on “activities that invade privacy.”<sup>66</sup> Omer Tene lists them as follows: aggregation, distortion, exclusion, secondary use, and breach of confidentiality.<sup>67</sup> When it comes to online advertising, the emphasis is on collecting personal information and then creating a profile of a particular person in order to know what kind of advertisements that person might be interested in. However, it has to be noted that personal information is not only gathered for the purpose of showing ads. This practice enables companies such as Google and Yahoo to improve the quality of their algorithms, and hence the quality of their overall services. Since online privacy issues mostly arise after the gathering of personal information, the list of the activities provided by Tene is very much relevant for the topic at hand.

Aggregation, according to Solove, is a process of collecting personal information and storing them together.<sup>68</sup> By having personal information gathered and stored, is, of course, a privacy

---

<sup>65</sup>. Omer Tene, “What Google Knows: Privacy and Internet Search Engines,” *Social Sciences Research Network*. Accessed January 23, 2014, <http://ssrn.com/abstract=1021490>

<sup>66</sup>. Ibid.

<sup>67</sup>. Ibid.

<sup>68</sup>. Ibid.

problem on its own. But what makes it an even bigger problem is the fact that “combining information creates synergies.”<sup>69</sup> For example, searching for words such as *universities in massachusetts* and *how to get into college* is already revealing enough. But if we add to these search queries a couple of more such as *apartments for rent in boston*, *how to go through a bad break-up*, *latin dance teacher jobs in boston*, *moving from miami to boston* and *how to paint your nails perfectly*, we get a very telling profile of a person who is probably a single female of Latin descent around her twenties. She is seemingly a Latin dance teacher looking to move from Miami to Boston in order to pursue college studies there. This profile has been created after only seven search queries. When we take into account the fact that an average person can, and does enter thousands and thousands of search queries over a period of one year only, it becomes evident why aggregation of personal information potentially represents a privacy problem. This problem becomes even bigger when one takes into account that an average internet user mostly uses the same search engine repeatedly. Hence, his, or her, private information is not dispersed, but is concentrated in the hands of one particular entity.<sup>70</sup>

Solove describes distortion as “the manipulation of the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public.”<sup>71</sup> With the collection of private information, distortion is something which can occur. For example, if someone types in on Google *in what ways can a person commit a suicide*, that does not mean that a person with this search query has suicidal intentions. There are numerous ways in which this search query can be justified. He, or she, may be writing a thesis on this topic, or may simply be satisfying his curiosity.

Exclusion, as defined by Solove, is “the failure to provide individuals with notice and input about their records.”<sup>72</sup> Therefore, if personal information is being collected and stored without

---

<sup>69</sup>. Ibid.

<sup>70</sup>. Ibid.

<sup>71</sup>. Ibid.

<sup>72</sup>. Ibid.



consent, and then further used without any notification to the concerned person, a privacy problem arises.

Secondary use refers to a situation in which the gathered information is used for the purpose other than the one which has been specified, either explicitly or implicitly.<sup>73</sup> Hence, if a search engine's privacy policy states, or if a user reasonably expects that gathered information will only be used to improve the quality of its search services, but then goes on to use the obtained information for advertising purposes, this might be perceived as a violation of one's privacy. Solove is of that opinion. He even goes a step further by saying that secondary use of collected information “creates a dignitary harm ... emerging from denying people control over the future use of their data, which can be used in ways that have significant effects on their lives.”<sup>74</sup>

Breach of confidentiality, in the context of the topic at hand, would arise if the search engine operator revealed to third parties sensitive information about its users, provided that there is a relationship of trust between the search engine operator and the user.<sup>75</sup> Whether this relationship exists or not, is a debatable question. However, the possibility of disclosing private information to third parties, or even to the general public, does exist, and without any doubt whatsoever, raises very controversial privacy concerns.

In the light of everything presented above, it is obvious that collecting personal information does raise some very serious privacy issues. The reality is, nonetheless, that genuine need for gathering of personal information does exist. Improvement of the quality of the offered services, for example, fits into that category. For this reason, interests of both the users and the search engine operators to have a better quality service need to be taken into account and weighed against a genuine need to safeguard online privacy.

---

<sup>73</sup>. Ibid.

<sup>74</sup>. Ibid.

<sup>75</sup>. Ibid.

## Chapter 4: The US Approach to Internet Privacy and Online Advertising

The United States has a market-oriented approach towards the issue of privacy in general.<sup>76</sup> As a matter of fact, it is quite safe to say that, at least when compared to the existing regulation in the European Union, the privacy regulation on federal level in the United States tends to be rather scarce, especially the one which is related to information privacy online. More precisely, regulation does exist to a certain extent, but it is not comprehensive.<sup>77</sup> It aims to protect private information, but as to what constitutes private information there is no consensus. One of the relatively accepted definitions is that private information is that which includes first and last name, home address, social security number, telephone number and any other information which can be used to identify an individual.<sup>78</sup> The United States Constitution does not expressly mention the concept of privacy anywhere, but a fairly accepted interpretation of certain amendments (First, Third and Fourth) had led to a conclusion that the Constitution does protect certain aspects of privacy, mainly those which arise in relations between the state and individual.<sup>79</sup>

Several acts have been enacted, and they only purport to cover certain types of information. These include financial data (covered by Gramm-Leach-Bliley Act, GLB), healthcare data (Health Information and Portability Accountability Act, HIPAA), and information provided by children online (Children's Online Privacy Protection Act, COPPA).<sup>80</sup> Another pivotal piece of legislation is the Electronic Communications Privacy Act (ECPA) which aims to protect wire, oral, and electronic communications while they are in the process of being transmitted and when they are stored on

---

<sup>76</sup>. Adam G. Todd, "Fractured Freedoms: The United States' Postmodern Approach to Protecting Privacy," *Social Sciences Research Network*. Accessed at February 26, 2014, <http://ssrn.com/abstract=892874>

<sup>77</sup>. David L. Baumer, Julia B. Earp, and J.C. Poindexter, "Internet Privacy Law: A Comparison between the United States and the European Union," *ScienceDirect*. Accessed March 18, 2014, <http://www.sciencedirect.com/science/article/pii/S0167404804000136>

<sup>78</sup>. Ibid.

<sup>79</sup>. Daniel J. Solove and Paul M. Schwartz, *Information Privacy Law* (New York: Wolters Kluwer Law, 2011), 34.

<sup>80</sup>. Ibid.

one's computer.<sup>81</sup> The ECPA is applicable to phone conversations, communication by e-mail, and electronically-stored data. In addition to this, the Federal Trade Commission (FTA), an independent agency of the US government, plays a highly important role in the realm of online privacy.<sup>82</sup> Commercial entities which operate online are not required by law to have a privacy policy. However, if they opt to have a privacy policy, then they have to abide by it.<sup>83</sup> If they fail to abide, the Federal Trade Commission will initiate a litigation process against those who do not adhere to their privacy policies.<sup>84</sup> FTA has done so in the past, but it has to be noted that majority of the claims were actually settled.<sup>85</sup> Finally, privacy is also protected in common law, through torts. More precisely, there are four torts which are related to privacy: (1) Intrusion upon plaintiff's seclusion; (2) Private disclosure of embarrassing facts about the plaintiff; (3) Publicity which puts the plaintiff in bad light; and (4) Appropriation of plaintiff's name or likeness.<sup>86</sup>

Since this thesis deals with Internet privacy in the context of online advertising, this chapter will devote its attention to legal aspects of practices which make online advertising possible. Online advertising, per se, and without any doubt, is in line with all the relevant laws on privacy. However, the manner in which certain tools, such as cookies, have been used (mainly for behavioral targeting purposes), have been often questioned and frequently debated. Therefore, the emphasis will be on those aspects which might seem problematic and controversial from legal perspective.

---

<sup>81</sup>. Ibid., 850.

<sup>82</sup>. Ibid., 820.

<sup>83</sup>. Baumer, "Internet Privacy Law," *SSRN*.

<sup>84</sup>. Ibid.

<sup>85</sup>. Solove, *Information Privacy Law*, 821.

<sup>86</sup>. William L. Prosser, "Privacy," *California Law Review*. Accessed March 2, 2014, [http://www.californialawreview.org/assets/pdfs/misc/prosser\\_privacy.pdf](http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf)

#### 4.1. Federal Trade Commission

As already briefly explained, Federal Trade Commission, or FTC, is in charge of enforcing promises that private companies make concerning privacy of their clients or users. That is, if they opt to have a privacy policy, they are expected to stick to it. This is in accordance with the Federal Trade Commission Act which states that the FTC shall have the authority to deal with deceptive acts and practices which adversely affect commerce.<sup>87</sup> Hence, posting and maintaining a privacy policy, and then not abiding by its provisions constitutes a deceptive practice which will be sanctioned by the FTC. However, it has to be said that the authority of the FTC is fairly limited in a sense that not all the companies are within the FTC's jurisdiction. For example, airline companies, financial institutions and telecommunication carriers all fall outside the scope of the FTC's jurisdiction.<sup>88</sup>

The FTC has first been invited by Congress to become an active participant in solving the consumer privacy issues in 1995.<sup>89</sup> Ever since then, the FTC has become extremely involved in these sorts of matters. Hence, it goes without saying then that the FTC has also been involved in the discussion and regulation of online behavioral advertising. It has even brought cases numerous cases concerning this issue, one of them being the case against Google Inc.<sup>90</sup> In the complaint, the FTC alleged that Google has been violating its promise not to track Apple's users and display them advertisements with the aid of tracking cookies. Safari, Apple's web browser, was delivered to their users with settings on third-party cookies already in place. More precisely, Safari's settings were blocking any sort of third-party cookies on the users' computers. However, according to the FTC's complaint, Google, even after acknowledging those settings on cookies and promising to adhere to

---

<sup>87</sup>. Solove, *Information Privacy Law*, 821.

<sup>88</sup>. *Ibid.*

<sup>89</sup>. *Ibid.*, 820.

<sup>90</sup>. "Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser," *Federal Trade Commission*, last modified August 9, 2012. <http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>

them, failed to do so. Actually, Google found a way to circumvent those settings, and display the ads to the Apple's users. This, in the view of the FTC, was a deceptive trade practice. Eventually, the case was settled, with Google paying to the FTC a record fine in the amount of 22.5 million dollars.<sup>91</sup>

The FTC has been constantly monitoring behavioral advertising practices and from time to time issuing reports. The FTC has even gone to Congress in 2011 with the agenda of convincing its members that additional legislation on this matter was needed. More precisely, the FTC has been arguing in favor of stricter regulation of behavioral advertising, justifying this with the need to protect consumers online. This resulted in several bills being introduced in the US Congress, but none of them attained the status of law. One of them was the so-called “Do Not Track Me Online Act of 2011,” sponsored by Jackie Speier.<sup>92</sup> This bill provided for an opt-out.<sup>93</sup> Therefore, the users would be able to, as the word itself plainly suggests, to opt out of being tracked online. However, this bill was never enacted.<sup>94</sup>

#### 4.2 Electronic Communications Privacy Act

Electronic Communications Privacy Act, or ECPA, came into force in 1986. It consists of three separate acts: (1) the Wiretap Act; (2) the Stored Communications Act; and (3) the Pen Register Act.<sup>95</sup> The purpose behind this piece of legislation was to prevent any sort of unauthorized access or interception of certain kinds of communications.<sup>96</sup> These include communications through wire, oral, and electronic means while they are in the process of being transmitted and when they

---

<sup>91</sup>. Ibid.

<sup>92</sup>. Ryan Singel, “Bill to Restrict Online Tracking Introduced in Congress,” *Wired*. Accessed March 3, 2014, <http://www.wired.com/business/2011/02/do-not-track-bill/>

<sup>93</sup>. Ibid.

<sup>94</sup>. Ibid.

<sup>95</sup>. Solove, *Information Privacy Law*, 850.

<sup>96</sup>. Ibid.

are stored on one's computer. In an attempt to make the ECPA applicable to commercial entities, usually, the parties would usually reach out to either the Wiretap Act or the Stored Communications Act.<sup>97</sup>

When one reads what the purpose and the scope of the ECPA are, the question immediately arises: Does it cover cookies and behavioral targeting as well? The answer to this question, at least according to the United States District Court for the Southern District of New York, is in the negative. In *In re DoubleClick Inc. Privacy Litigation*<sup>98</sup> case, the court held that neither the Wiretap Act nor the Stored Communications Act were applicable. The Wiretap Act could not be applied because, the court reasoned, the DoubleClicks's practices fell into the realm of consent exception. The Wiretap Act provides in relevant part that it will be punishable to access intentionally “without authorization a facility through which an electronic information service is provided.” Sending of cookies, per se, and retrieving information in this manner satisfies this Wiretap Act's provision.<sup>99</sup> However, according to the Wiretap Act, consent exception arises when one of two users that are involved in the communication provide consent. Here, the court interpreted, the other “user” was the website that that the user had visited.<sup>100</sup> Since the website provided its consent, the Wiretap Act's consent exception was satisfied. As for the Stored Communications Act, the court found it to be inapplicable to the case at hand since the Stored Communications Act governed only temporary storage of communications. Cookies did not fit this description since they could be stored on a personal computer for months, even years.

Therefore, the conclusion seems to be that, in the US system, the use of the cookies for gathering personal information is very much legal, even if no consent is previously obtained from the user. Certain exceptions to this apply, and one of those exceptions is entrenched in the

---

<sup>97</sup>. Ibid.

<sup>98</sup>. *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), LexisNexis.

<sup>99</sup>. Solove, *Information Privacy Law*, 855.

<sup>100</sup>. Ibid.

Children's Online Privacy Protection Act, discussed briefly below.

### 4.3 Children's Online Privacy Protection Act

Children's Online Privacy Protection Act, better known by its acronym COPPA, was enacted in 1998.<sup>101</sup> Over the course of its existence, and especially in 2012 when COPPA was amended, advertising community fought hard through lobbying to minimize its effects on advertising aimed at children.<sup>102</sup> The aim of the legislator with the COPPA was to adopt a piece of legislation which would regulate collection of information from children and its further use.<sup>103</sup> In order for COPPA to be applicable to a website, that website has to either target children under the age of 13 or have knowledge that it is collecting information from children of that particular age.<sup>104</sup> Furthermore, these websites do not have an option of whether they will maintain a privacy policy or not. Under COPPA, a privacy policy is mandatory for them.<sup>105</sup> It has to contain explanations as to what kind of information is collected and how it will be used later on.

COPPA also gives tremendous power to children's parents.<sup>106</sup> For example, the websites which target children under the age of 13 and are collecting information from them have to get a verifiable parental consent.<sup>107</sup> Only when the parent gives its consent can a website continue with its practice of collecting and using information in accordance with its privacy policy. However, parents are not required to give their consent if the information given by their children is not stored or in

---

<sup>101</sup>. Ibid., 847.

<sup>102</sup>. Katy Bachman, "FTC Restricts Behavioral Targeting of Kids," *Adweek*. Accessed March 20, 2014, <http://www.adweek.com/news/technology/ftc-restricts-behavioral-targeting-kids-146108>

<sup>103</sup>. Solove, *Information Privacy Law*, 847.

<sup>104</sup>. Ibid., 848.

<sup>105</sup>. Ibid.

<sup>106</sup>. Ibid.

<sup>107</sup>. Ibid.

any manner retrievable.<sup>108</sup> Furthermore, parents can at any time ask the website to disclose the information that has been collected, and if a parent so requests, the website may not use the gathered information in any manner that the parent disapproves of.<sup>109</sup>

COPPA is not only applicable to direct collection of information which could lead to a child being personally identified, but is also applicable to the use of cookies for compiling children's private information.<sup>110</sup> What is more, it is applicable to the collection through cookies of information on children's browsing preferences, hobbies and school interests if these could lead to them being personally identified.<sup>111</sup>

The enforcement of COPPA is entrusted to FTC.<sup>112</sup> This is owing to the fact that violations of COPPA are perceived as “a violation of a rule defining an unfair or deceptive act or practice.”<sup>113</sup> Thus, private individuals cannot rely on COPPA to establish a private cause of action. However, states do have the right to bring suits under COPPA if they deem that that is in the best interests of their citizens.<sup>114</sup>

---

<sup>108</sup>. Ibid.

<sup>109</sup>. Ibid.

<sup>110</sup>. “COPPA – Children's Online Privacy Protection Act,” coppa.org. Accessed March 11, 2014, <http://www.coppa.org/comply.htm>

<sup>111</sup>. Ibid.

<sup>112</sup>. Solove, *Information Privacy Law*, 848.

<sup>113</sup>. Ibid.

<sup>114</sup>. Ibid.



## Chapter 5: The EU Approach to Internet Privacy and Online Advertising

The European Union has a fairly different approach to the issue of Internet privacy than the United States has. The EU, as a matter of fact, chose not to follow the market-oriented approach of Uncle Sam. Instead, the EU opted for a command and control approach. This means that the EU does not leave the issue at hand half-regulated, as the US does, but is determining directly what is allowed and what not. Before mentioning relevant directives on this matter, it would be useful to note that, unlike the United States Constitution, both the Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union explicitly mention the phrase “the right to private life.”<sup>115</sup> It is these provisions that served both as an inspiration and a catalyst for the introduction of two quintessential directives in the field of privacy in the European Union.<sup>116</sup>

The EU began its command and control approach by introducing the EU Data Protection Directive in 1995.<sup>117</sup> However, this directive was not directly aimed at the regulation of information on the Internet, which, at that time, was still “an infant.” In 2002, another Directive was promulgated. It was the Directive on Privacy and Electronic Communications, with the aim of filling exactly that gap.<sup>118</sup> The aim of this directive was to face the challenge of information privacy online in the ever-changing digital world.<sup>119</sup> Since the EU legislation on this matter is covered by directives, it is upon the member states of the EU to implement and enforce the provisions of the said directives. Thus, in the EU, no agency such as the Federal Trade Commission exists with similar authority on the matters of Internet privacy and privacy in general. If there are violations, the EU has to initiate infringement proceedings against the Member State that is failing to abide by

---

<sup>115</sup>. “The European Legal Context: The EU Privacy Directives,” *Legal Information Institute*, accessed March 19, 2014, [http://www.law.cornell.edu/wex/inbox/european\\_legal\\_context\\_privacy\\_directives](http://www.law.cornell.edu/wex/inbox/european_legal_context_privacy_directives)

<sup>116</sup>. Ibid.

<sup>117</sup>. Ibid.

<sup>118</sup>. Baumer, “Internet Privacy Law,” *SSRN*.

<sup>119</sup>. Ibid.

EU law on privacy.

Furthermore, unlike in the US where there is no widely accepted definition of what constitutes personal information, in the EU the definition can be found in the 1995 Information Directive itself. The Directive actually refers to personal data, and defines it as “any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity...”<sup>120</sup>

This chapter, just like the previous one on the United States, will devote its attention to legal aspects of practices which make online advertising possible. Online advertising, per se, and without any doubt, is in line with all the relevant laws on privacy. However, the way in which certain tools, such as cookies, have been used (mainly for behavioral targeting purposes), have been often questioned and frequently debated. Therefore, the emphasis will be on those aspects of online advertising which might seem problematic and controversial from legal perspective.

### 5.1 Data Protection Directive

The Data Protection Directive, although enacted with the aim to regulate the use of private data in general, is still very much applicable to the developments online. It was basically a follow-up to the OECD Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data.<sup>121</sup> According to these recommendations, in order to efficiently protect data subjects and personal data, the following seven measures ought to be implemented: notice (one should be aware of the fact that his or her personal data are being

---

<sup>120</sup>. *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*, Official Journal L 281 , 23/11/1995 P. 0031 – 0050

<sup>121</sup>. Neil Robinson, Hans Graux, Maarten Botterman, and Lorenzo Valeri, “Review of the European Data Protection Directive,” *Rand Europe*, accessed March 18, 2014, [http://www.hideproject.org/downloads/references/review\\_of\\_eu\\_dp\\_directive.pdf](http://www.hideproject.org/downloads/references/review_of_eu_dp_directive.pdf)

collected), purpose (the data should only be used in accordance with the pre-stated purpose of their future use), consent (a consent should be obtained from data subjects before proceeding with the use of private data), security (the data that has been obtained must be safe from any misuse whatsoever), disclosure (one should know who the entity is that is collecting the personal data), access (data subjects ought to have the right to access and view the collected data), and (the data subjects ought to be able to hold accountable those that have collected their personal data, but failed to abide by the previously mentioned principles).<sup>122</sup>

The United States was working on the endorsement of the OECD Recommendations, but eventually, failed to adopt any sort of legislation in support of those recommendation.<sup>123</sup> To contrast this with the the EU approach, the Data Protection Directive implements all of the OECD Recommendations.<sup>124</sup> It even goes a step further by requiring the principle of proportionality to be applied.<sup>125</sup> More precisely, the collected data may only be used to a achieve a certain aim if the use of the collected data is not disproportionate to the aim which is to be achieved.

The Data Protection Directive, as already stated, was not enacted with the purpose of regulating online behavioral advertising and the use of cookies. This has been dealt with later on, by adopting the Directive on Privacy and Electronic Communications. However, this Directive, in provisions which are relevant for the topic at hand, makes numerous references to the Data Protection Directive. Hence, these two pieces of EU legislation are complimentary.

---

<sup>122</sup>. Ibid.

<sup>123</sup>. Anna E. Shimanek, "Do You Want Milk with Those Cookies? Complying with the Safe Harbor Privacy Principles" *Social Sciences Research Network*, accessed March 16, 2014, <http://ssrn.com/abstract=264857>

<sup>124</sup>. Ibid.

<sup>125</sup>. Charolte B. Tranberg, "Proportionality and Data Protection in the Case Law of the European Court of Justice," *Oxford Journals*, accessed March 16, 2014, <http://idpl.oxfordjournals.org/content/early/2011/08/11/idpl.ipr015.full>

## 5.2 Directive on Privacy and Electronic Communications

The Directive on Privacy and Electronic Communications has often been referred to as a continuation of an earlier effort by the European Union to regulate the use of private data and to safeguard the interests of data subjects.<sup>126</sup> Adopted in 2002, it aimed to reflect the never-ending expansion of the Internet and other tools of the digital world and their impact on privacy. One of the major concerns of the EU, which was to be regulated after the adoption of the Directive on Privacy and Electronic Communications, was of course, the use of cookies.

Article 5(3), among other things, deals with the issue of cookies.<sup>127</sup> However, it has to be noted that Article 5(3) does not mention the word cookie or any other synonym. It only focuses on the final result of the use of tools such as cookies. This is owing to the fact that the Directive on Privacy and Electronic Communications is a technology-neutral directive.<sup>128</sup> This means that it acknowledges that the development of law cannot keep pace with the development of technology. So, in order to remain up-to-date and applicable to future technologies which will probably be able to do the same thing as cookies, but more efficiently, the drafters decided not to refer to any specific type of present-day technology. Article 5(3) is a clear illustration of this approach since it refers to information storing or gaining access to information stored in the users' terminal equipment without any mention of cookies:

“Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as

---

<sup>126</sup>. The European Legal Context: The EU Privacy Directives,” *Legal Information Institute*.

<sup>127</sup>. Baumer, “Internet Privacy Law,” *SSRN*.

<sup>128</sup>. “European Data Protection Roundtable,” *European Commission*, accessed March 17, 2014, [http://ec.europa.eu/justice/news/consulting\\_public/0003/contributions/organisations\\_not\\_registered/edpr\\_en.pdf](http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/edpr_en.pdf)

strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.”<sup>129</sup>

The approach of the Directive on Privacy and Electronic Communications whereby the users first must be informed in accordance with the Data Protection Directive and then given the opportunity to decide whether they want to be part of the processing or not is referred to as the opt-in regime.<sup>130</sup> There are, however, types of cookies for which no users' consent is required.<sup>131</sup> These, for example, include cookies which are used to collect information from the previous page when the user is shopping online or those cookies which enable the provider to remember user preferences such as website's language.

An example of an enforcement of the EU's privacy policy can be seen in the case which the Commission had initiated against the UK.<sup>132</sup> Phorm, a UK-based company, was involved in the advertising business. More precisely, it was delivering ads by using the behavioral targeting practices without notifying those concerned or obtaining consent from them. The UK law provided that interception of communication is not unlawful provided that the intercepting party reasonably believes that the consent is present.<sup>133</sup> The Commission perceived this to be a clear violation of the EU's directives on privacy.<sup>134</sup> However, eventually, the Commission dropped the case against the UK, stating that the UK had altered its laws so that they now fully comply with the EU law.

---

<sup>129</sup>. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, Official Journal L 201 , 31/07/2002 P. 0037 – 0047

<sup>130</sup>. Lisa Arthur, “Eu e-Privacy Directive Takes Effect May 26 – Will Your Cookies Crumble?,” *Forbes*, accessed March 16, 2014, <http://www.forbes.com/sites/lisaarthur/2012/05/22/eu-e-privacy-directive-takes-effect-may-26-will-your-cookies-crumble/>

<sup>131</sup>. “Cookies,” *Information Commissioner's Office*, accessed March 15, 2014, [http://ico.org.uk/for\\_organisations/privacy\\_and\\_electronic\\_communications/the\\_guide/cookies](http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies)

<sup>132</sup>. Hogan Lovelles, “European Commission opens proceeding against the UK in connection with Phorm’s behavioral advertising technology,” *Association of Corporate Council*, Accessed March 15, 2014, <http://www.lexology.com/library/detail.aspx?g=28bd35d8-7773-49f9-acfd-8e961d0e5461>

<sup>133</sup>. *Ibid.*

<sup>134</sup>. *Ibid.*

### 5.3 Safe Harbor Principles

As one can clearly see, the European Union gives privacy a lot more attention than the United States does. After the adoption of the Data Protection Directive, countries with laws providing lesser degree of privacy protection found themselves in trouble. More precisely, their companies would face heavy restrictions when attempting to transfer private data outside the EU.<sup>135</sup> This, in turn, posed dangerous consequences on economy. In light of this hovering danger, the United States decided to implement the so-called Safe Harbor Principles.<sup>136</sup> In order to be able to transfer private data, US companies have to show that they adhere to the seven principles on which the Data Protection Directive is based on. If they do, they get a certificate, and are free to transfer private data to the United States from the European Union.<sup>137</sup>

---

<sup>135</sup>. Baumer, “Internet Privacy Law,” *SSRN*.

<sup>136</sup>. *Ibid.*

<sup>137</sup>. *Ibid.*

## Conclusion

As it was shown, the United States and the European Union have very much different approaches to the issue of online privacy in general. The United States law is more market-oriented. Companies are not required generally to have privacy policies, but most opt to have them. This is because having a privacy policy might make users feel safer knowing that there is a privacy policy in place. Hence, if a competitor does not have a privacy policy, the users may be more inclined to use the website of a company which actually has one. However, this approach is not universally applied. For example, in case of websites whose main users are children under the age of 13, or if the operator of a website has reasons to know that he is obtaining private information from children, then privacy policy is mandatory. However, many have questioned COPPA's efficiency? What is it that COPPA is trying to achieve? If it is trying to protect children online, it is doing a bad job. Children are many times browsing through websites which are not intended for them. For example, most of Google's services are available, according to their Terms of Service, only to people who are older than thirteen.<sup>138</sup> Do we really believe that no 13 year old child has never watched a video on YouTube? Do we really believe that Google is not aware that even children under the age of 13 are using YouTube? When opening an account with Google, we are required to provide our real age. However, nothing prevents a child who is 13 to indicate that he, or she, is actually 17, and then the child can proceed with giving personal data such as name, surname, etc. Yes, COPPA does require parental consent, but even its efficiency is highly questionable. Some parents might be uninterested in the whole concept of consent, and end up giving their children free rein. If the aim of COPPA is to teach children the importance of self-care online in relation to privacy, it again is not that efficient. As Anita Allen notes, "it will be difficult for children to get the message that privacy is a duty of self-care... [since]... everyone under the age of forty seems to be freely sharing personal facts, ideas, fantasies, and revealing images of themselves all the time."<sup>139</sup>

---

<sup>138</sup>. "Age Requirements on Google Accounts," *Google*, accessed March 25, 2014, <https://support.google.com/accounts/answer/1350409?hl=en>

<sup>139</sup>. Anita Allen, "Unpopular Privacy." (2011). Quoted in Solove, *Information Privacy Law*, 850.

The inefficiency of privacy laws is only one aspect. The other important aspect is their economic impact. As was shown in chapter 2, online advertising can be very efficient from an economic standpoint. It can encourage competition, enable new companies to win their portion of market share, and inform consumers. But in the European Union, where the command and control approach is favored, these benefits may be impaired by current legislation. The European Union is fairly more populous than the United States and its GDP is higher, but revenues from online advertising are still higher in the United States. For example, in 2012, total revenues from online advertising in the United States stood at 36.57 billion dollars<sup>140</sup> whereas in Europe in 2012 they stood at 24.3 billion euros.<sup>141</sup>

As already stated, online privacy concerns are not without merit. But, technological developments are rapid, and legislation, which is slow-paced, cannot efficiently deal with all the problems which might arise. The fact is, technology for gathering of private data is there, and it is widespread. David Brin is of the opinion that “it is already far too late to prevent the invasion of cameras and databases [since] [t]he djinn cannot be crammed back into its bottle. No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases.”<sup>142</sup> Cookies, for example, are one of the most efficient tools for information gathering. Why not ban the cookies then? First of all, cookies perform other significant functions which are necessary for proper functioning of the Internet and e-commerce. For example, in online shopping, cookies, as already pointed out, are highly relevant. Second of all, many websites and Internet services that we take for granted are actually funded through online advertising. Cookies are crucial for them, and they use them to maximize the impact of their advertisements in order to achieve higher revenues. Without efficient advertising, companies such as Google, Facebook,

---

<sup>140</sup>. “IAB Report.” *PwC*, 2013.

<sup>141</sup>. “Adex Benchmark.” *IAB Europe*, 2013.

<sup>142</sup>. David Brin, “The Transparent Society.” (1998). Quoted in Solove, *Information Privacy Law*, 804.



Yahoo, and many others would actually have to charge for their services. Moreover, Google has, by gathering private data and analyzing various search queries, managed to improve its search service by leaps and bounds. Thus, banning the cookies would only cause more harm than it would bring benefit.

But what would be the solution then? Kevin Kelly, a founding executive editor of *Wired* magazine, points out that “the answer to the whole privacy question is more knowledge. More knowledge about who is watching you [and] [m]ore knowledge about the information that flows between us.”<sup>143</sup> If one is really worried about the prospect of being surveilled, several privacy enhancing technologies are at his, or her, disposal. These include encryption tools, Internet browsing settings, cookie management, and anonymization schemes.<sup>144</sup>

As for the legislative approach, the law should aim not to impair the ability to collect private data if they are to be fairly and discreetly used, for, say, advertising purposes. Advertising can be annoying at times, but the user still has an option to install an ad-block extension. This option does not exist when one watches his favorite show on TV, and the commercials start. As already explained, benefits of online advertising are enormous. Therefore, the legislator ought to aim to establish a relationship of trust between the company and the person from whom private data has been collected. In case of misuse, the company ought to be held liable. Fines could be imposed. Additionally, the aggrieved party should be given the opportunity to find redress in the court of law.

To conclude, owing to the well-founded notion that online advertising tends to be viable and efficient from an economic and social standpoint, the law needs to reflect that by striking a satisfactory balance with the provisions on Internet privacy. The law ought not to impair the ability of companies such as Google to efficiently deliver us ads. Its aim should be to allow the gathering of personal data for certain purposes (e.g. online advertising) but in case of an unauthorized sharing of such data or any misuse whatsoever, the aim should then be to impose liability on the company

---

<sup>143</sup>. Ibid.

<sup>144</sup>. Tene, “What Google Knows,” *SSRN*.

responsible for such misuse or any unauthorized sharing.

## Bibliography

- “Adex Benchmark 2011: European Online Advertising Expenditure.” *Interactive Advertising Bureau Europe*, 2012. [http://www.iabeurope.eu/files/9113/6852/1903/2011\\_adex\\_benchmark\\_final.pdf](http://www.iabeurope.eu/files/9113/6852/1903/2011_adex_benchmark_final.pdf)
- “Adex Benchmark 2012: European Online Advertising Expenditure.” *Interactive Advertising Bureau Europe*, 2013. [http://www.iab.nl/wp-content/uploads/downloads/2013/08/2013\\_08\\_28\\_IAB\\_Adex\\_Benchmark.Pdf](http://www.iab.nl/wp-content/uploads/downloads/2013/08/2013_08_28_IAB_Adex_Benchmark.Pdf)
- “Age Requirements on Google Accounts,” *Google*, accessed March 25, 2014, <https://support.google.com/accounts/answer/1350409?hl=en>
- Arthur, Lisa. “Eu e-Privacy Directive Takes Effect May 26 – Will Your Cookies Crumble?,” *Forbes*, accessed March 16, 2014, <http://www.forbes.com/sites/lisaarthur/2012/05/22/eu-e-privacy-directive-takes-effect-may-26-will-your-cookies-crumble/>
- Bachman, Katy. “FTC Restricts Behavioral Targeting of Kids,” *Adweek*. Accessed March 20, 2014, <http://www.adweek.com/news/technology/ftc-restricts-behavioral-targeting-kids-146108>
- Baumer, David L., Julia B. Earp, and J.C. Poindexter, “Internet Privacy Law: A Comparison between the United States and the European Union,” *ScienceDirect*. Accessed March 18, 2014, <http://www.sciencedirect.com/science/article/pii/S0167404804000136>
- Blyth, Alex. *Brilliant Online Marketing: How to Use the Internet to Market Your Business*. FT Press, 2011. Google Books.
- “Cookies,” *Information Commissioner's Office*, accessed March 15, 2014, [http://ico.org.uk/for\\_organisations/privacy\\_and\\_electronic\\_communications/the\\_guide/cookies](http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies)
- “COPPA – Children's Online Privacy Protection Act,” *coppa.org*. Accessed March 11, 2014, <http://www.coppa.org/comply.htm>
- “European Data Protection Roundtable,” *European Commission*, accessed March 17, 2014, [http://ec.europa.eu/justice/news/consulting\\_public/0003/contributions/organisations\\_not\\_registered/edpr\\_en.pdf](http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/edpr_en.pdf)
- Evans, David S. “The Online Advertising Industry: Economics, Evolution, and Privacy,” *Social Sciences Research Network*. Accessed at January 18, 2014 at <http://ssrn.com/abstract=1376607>
- “Global Mobile Advertising Revenues Surge 82.8 % in 2012, Hitting a High of \$8.9 Billion,” *Interactive Advertising Bureau*, last modified July 9, 2013, [http://www.iab.net/about\\_the\\_iab/recent\\_press\\_releases/press\\_release\\_archive/press\\_release/pr-070913](http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070913)
- “Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser,” *Federal Trade Commission*, last modified August 9, 2012. <http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>

- “How Does Online Advertising Work,” YouTube video, 1:59, posted by “Interactive Advertising Bureau UK,” July 18, 2012, <https://www.youtube.com/watch?v=Y9Y4Efyxmk4>
- “IAB Internet Advertising Revenue Report.” *PwC*, 2013. [http://www.iab.net/media/file/IAB\\_Internet\\_Advertising\\_Revenue\\_Report\\_FY\\_2012\\_rev.pdf](http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2012_rev.pdf)
- Lovelles, Hogan, “European Commission opens proceeding against the UK in connection with Phorm’s behavioral advertising technology,” *Association of Corporate Council*, Accessed March 15, 2014, <http://www.lexology.com/library/detail.aspx?g=28bd35d8-7773-49f9-acfd-8e961d0e5461>
- Mankiw, Gregory. *Principles of Microeconomics*. Cengage Learning, 2006. PDF e-book.
- Rushe, Dominic. “Don’t Expect Privacy When Sending to Gmail,” *The Guardian*, August 15, 2013, <http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit>
- Prosser, William L. “Privacy,” *California Law Review*. Accessed March 2, 2014, [http://www.californialawreview.org/assets/pdfs/misc/prosser\\_privacy.pdf](http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf)
- Robinson, Neil, Hans Graux, Maarten Botterman, and Lorenzo Valeri, “Review of the European Data protection Directive,” *Rand Europe*, accessed March 18, 2014, [http://www.hideproject.org/downloads/references/review\\_of\\_eu\\_dp\\_directive.pdf](http://www.hideproject.org/downloads/references/review_of_eu_dp_directive.pdf)
- Shimanek, Anna E. “Do You Want Milk with Those Cookies? Complying with the Safe Harbor Privacy Principles” *Social Sciences Research Network*, accessed March 16, 2014, <http://ssrn.com/abstract=264857>
- Singel, Ryan. “Bill to Restrict Online Tracking Introduced in Congress,” *Wired*. Accessed March 3, 2014, <http://www.wired.com/business/2011/02/do-not-track-bill/>
- Solove, Daniel J. and Paul M. Schwartz. *Information Privacy Law* (New York: Wolters Kluwer Law, 2011), 34.
- Tene, Omer. “What Google Knows: Privacy and Internet Search Engines,” *Social Sciences Research Network*. Accessed January 23, 2014, <http://ssrn.com/abstract=1021490>
- “The European Legal Context: The EU Privacy Directives,” *Legal Information Institute*, accessed March 19, 2014, [http://www.law.cornell.edu/wex/inbox/european\\_legal\\_context\\_privacy\\_directives](http://www.law.cornell.edu/wex/inbox/european_legal_context_privacy_directives)
- Todd, Adam G., “Fractured Freedoms: The United States’ Postmodern Approach to Protecting Privacy,” *Social Sciences Research Network*. Accessed at February 26, 2014, <http://ssrn.com/abstract=892874>
- Tranberg, Charoltte B. “Proportionality and Data Protection in the Case Law of the European Court of Justice,” *Oxford Journals*, accessed March 16, 2014, <http://idpl.oxfordjournals.org/content/early/2011/08/11/idpl.ipr015.full>
- “What Is Advertising?” *The University of North Carolina at Pembroke*, accessed March, 15, 2014, <http://www2.uncp.edu/home/acurtis/Courses/ResourcesForCourses/Advertising/AdvertisingWhatIsIt.html>