PERSONAL DATA PROTECTION IN ONLINE MARKETING:

THE ROLE OF SELF- AND CO-REGULATION

By

Andreana Stankova

Submitted to

Central European University

Department of Public Policy

in partial fulfilment for the degree of Master of Arts in Public Policy

Supervisor: Professor Kristina Irion

Budapest, Hungary

2008

Abstract

This thesis examines self- and co-regulation practices as a possible solution to the enforcement problem of data protection legislation in the European Union. The work focuses on the application of these mechanisms in the online marketing field since this is a business whose development heavily depends on the use of personal information. In addition, it is the only sector which has elaborated and currently applies a community level code of conduct controlling the data processing practices of companies. The methodology applied consists of a survey, document analysis and elite interviews. The conducted research has shown that existing self- and co-regulatory documents and the standards they establish are good at addressing consumers' concerns with regard to online marketing practices. However, some amendments are needed in order to better protect the interests of individuals. Nevertheless, is currently impossible to assess whether self- and co-regulatory procedures are an effective means of improving data protection practices of online marketers due to the lack of proper control mechanisms over the implementation of the rules.

Table of Contents

List of abbreviations

Article 29 Working Party	Working Party on the Protection of Individuals with regard to the Processing of Personal Data
BEUC	European Consumers' Organisation
CoE	Council of Europe
Data Protection Directive	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
DMAs	Direct Marketing Associations
DPAs	Data Protection Authorities
DRM	Digital rights management
EASA	European Advertising Standards Alliance
EDPS	European Data Protection Supervisor
ePrivacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 24 October 1995 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector
EU	European Union
EDMA	European Direct Marketing Association
FEDIM	Federation of Direct and Interactive Marketing
FEDMA	Federation of European Direct and Interactive Marketing
IP	Internet protocol
NGOs	Non-governmental organisations
PETs	Privacy Enhancing Technologies
RFID	Radio frequency identification

ROI	Return-on-investments
UDHR	Universal Declaration of Human Rights
US	United States

Introduction

Let me introduce two men[1]. The first, Winston Smith, a civil servant at the Ministry of Truth, lives in a world where every word he says and every move he makes are observed and recorded. The second, Joseph K., a senior bank employee, lives his ordinary life until one day, all of a sudden, he is arrested by the officials of the Court of Inquiry, an institution he has never heard of, for committing a crime never revealed to him. During his trial, K. finds out that these people know everything about him, his preferences, his habits. One of the common features between the two men is that they both live without privacy. However, while Smith is aware that he is observed all the time and can act consciously in order to avoid doing (or hide when doing) the things he is not supposed to do, Joseph K. does not know that he is watched and his personal data, carefully collected. This does not allow him to protect his privacy, even if he would like to.

George Orwell's 1984, where Smith is the main character (Orwell 1984), is the classic metaphor of a world without privacy. However, it is Franz Kafka's The Trial (Kafka 1969), where Joseph K. is the protagonist, which better describes the way in which personal data is used and sometimes abused in today's world. Nowadays, many public and private organisations collect information about people in order to perform their activities. One of the sectors whose lifeblood is personal information is online marketing. Professionals in the area rely on creating and sustaining a personalised relationship with their target customers. For this purpose, they accumulate huge databases with details about their clients and prospects. Later, this data, often inaccurate and partial, is stored and employed for purposes different from the one for which it was originally collected. Sometimes it is used to make important decisions about individuals' lives, thus depriving them of the control of their destinies.

[1] The metaphor presented here was first used to illustrate the different aspects of privacy by Solove (2004).

Some of the practices of data controllers clash with the fundamental right to privacy. In order to protect privacy by preventing abuses of personal data and secure a good working environment for companies, policy makers elaborate special legislation. The existence of explicit rules however, does not *per se* guarantee the effective protection of personal data. For this purpose, adequate and good enforcement of the legal provisions is needed and here is where policy makers have detected a problem. A possible solution is the application of self- and co-regulation mechanisms, which will be the focus of this thesis.

Most of the research dedicated to the effectiveness of existing data protection frameworks has examined the United States (US) context (Cate 1997, Solove 2004). Some studies look at the relevant legislation in the European Union (EU) as a whole (Ciocchetti 2008a) and with regard to eCommerce (Noll 2001, Gasser and Haeusermann 2007). However, little attention has been paid to the effectiveness of regulation with regard to the online marketing sector. The literature on direct and online marketing largely focuses on practical issues related to the application of these commercial communications techniques (Stone 1988, Kotler 2000). While much literature examines self- and co-regulation in general, only a few authors look at it within the EU context (Senden 2005a, Senden 2005b), in the online environment (Newman and Bach 2004, Price and Verhulst 2005) and in the electronic communications sector (Just and Latzer 2004). One study concentrates on the effectiveness of self- and co-regulation in the broader advertising sector (Harker 2003).

By bringing together the research on information privacy, online marketing and self- and co-regulation, this thesis will answer the question whether self- and co-regulation mechanisms are an effective means of improving the enforcement of existing data protection legislation in the online marketing business. Apart from being an industry which heavily depends on the use of personal data, the sector is the first and only one to have elaborated a document of self- and co-regulation at a community level, namely the European Code of Practice for the Use of

Personal Data in Direct Marketing of the Federation of European Direct and Interactive Marketing (FEDMA) (FEDMA 2003). Its text is currently being complemented by an annex, referring to marketers' practices on the Internet, to be referred as the Online Annex. With it, the industry demonstrates willingness to improve its data protection practices and it is worth examining whether its efforts lead to the desired outcome or are just a way to boost the image of the sector.

The unit of analysis of the thesis is the process of self- and co-regulation with regard to data protection as applied by the online marketing sector in Europe. The research methodology consists of a survey, document analysis and elite interviews. In order to understand whether consumers are concerned with data protection online and which are the most important issues for them, a short non-representative survey among users of the social network Facebook was carried out. It shows the opinions of the most attractive consumer group for marketers, which uses new technology on a daily basis and is constantly bombarded with commercial communication messages via the Internet. Document analysis of papers issued by the European Commission and other authorities was used to identify the enforcement problem of data protection legislation and to outline self- and co-regulation by the private sector as a possible solution. Later, the code of FEDMA was examined to find out to what extend it meets legislation and consumers' concerns as raised in the Facebook survey. In order to better research the way in which the code is enforced and study the relationships between the different stakeholders involved in the process of its elaboration and implementation, elite interviews were conducted. They took place in person, in Brussels, from May 15 to May 17, 2008. The people interviewed were from FEDMA, the association representing the interests of online and direct marketers across Europe, the European Advertising Standards Alliance (EASA), the organisation promoting soft law practices in the commercial communications sector in Europe, the European Consumers' Organisation

(BEUC), the body in charge of protecting consumers' interests in the EU decision-making process, and the Data Protection Unit of Directorate-General Justice, Freedom and Security. The unit represents the Commission in the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, the so called Article 29 Working Party. The Working Party is a special body established to deal with data protection issues on an EU level, including the approval of community-level codes of conduct by private sector actors. Therefore, the views expressed by the official from the Commission also give insight in the work of the Article 29 Working Party.

The structure of the thesis is the following. Chapter 1 presents the conflicting interests of online marketers and consumers with regard to data use and protection. Chapter 2 provides a short overview of the existing legislation aimed at striking a balance between the opposite needs and shows the enforcement problem it faces. Chapter 3 suggests self- and co-regulatory practices as a possible solution and demonstrates how these mechanisms are being implemented in the online marketing sector in Europe. Chapter 4 examines their effectiveness, detects certain weaknesses and makes suggestions for improvement.

Chapter 1 – Two perspectives to the use of personal data in the online marketing

This chapter will present the areas of potential conflict between online marketers and consumers with regard to the processing of personal data. For this purpose, it will explain the importance of data for this business and show how technological developments give almost unlimited possibilities to handle information. At the same time, each operation through which industries enrich the profiles of their customers is a step inside people's private sphere. Thus, the more data companies gather, the more uncovered and transparent individuals become. At the end, the results of a survey aimed at detecting whether people are concerned about this phenomenon will be presented.

1.1 The online marketers' perspective

One of the most popular advertising formats ever, the 30 second television spot, is losing its attractiveness as a channel to reach consumers and prospects (Berte et al. 2007, p. 123). The reasons for this are the new possibilities offered by information technology, the altered media usage patterns of audiences and the demand for higher accuracy in measuring return-on-investments (ROI) (PQ Media 2008, p. 5). Instead of the traditional advertising channels, *i.e.* radio, television and print media, companies opt for techniques such as sponsorship, product placement, direct marketing, outdoor and online advertising, to reach their target audiences and sell their products. These channels mainly rely on the individualised and interactive approach to contact customers and gain their goodwill.

One of these techniques is online marketing. It is a corporate communications tool which uses the Internet to establish and maintain a personal and interactive relationship with those people interested in acquiring a particular good or service. The definitions of online marketing

vary in scope from including email marketing and electronic shopping only (Kotler 2000, p. 272) to incorporating all kind of commercial communications techniques online. The latter include pay per click advertising, banner adds, interactive advertising, search engine marketing and blog marketing (FEDMA 2007, p. 2). The present research will focus on those online marketing tools which involve the intensive use of personal data. Therefore, this thesis will refer to online marketing as commercial communications technique which employs email, internet website or a portal in order to reach a pre-determined audience, offer it goods and services and carry out a transaction.

One typical example of online marketing could be a travel agency sending email offers for holidays at the Croatian seaside to people who spent their last summer in Italy or Spain. In order to carry out the mailing, the company needs a database with the names and email addresses of individuals who had a vacation in one of the Mediterranean countries. Another example would be an online bookshop which gives a 10% discount for a second purchase within a 30-day period. For this purpose, the firm needs to create and maintain lists with some item of personal identification information (names, email addresses or credit card numbers) plus purchase histories of its clients.

The possibilities to handle personal data have increased tremendously with the development of information technology and its wide application by marketers. In the offline world, direct marketing practices were limited to the mailing of catalogues and standardised product offers to the physical addresses of existing or potential customers. Over the time, companies accumulated relatively little new information about individuals, the biggest portion of it collected in the course of the commercial relationship with them. Nowadays, industries can amass almost unlimited amounts of data simply because everything people do is recorded and kept in databases. What is more, technology makes it possible to combine data from different sources, thus enriching the profiles elaborated on the basis of the relationship with

one firm only. Later, this data can be stored for long periods of time at a very low cost, further modified with the addition of new details and the revision of the irrelevant ones and used for new purposes. Thus, it is technically possible to gather information about customers, create profiles and apply data-mining techniques to find those individuals who best match certain criteria.

At the beginning of its relationship with individuals, a company has only the minimum data necessary to carry out a transaction: name, email and/ or physical addresses, credit card number. Online transactions produce further data, *e.g.* internet protocol (IP) address and type of web browsers. Over the time, more information is added to the initial profiles: socio-demographic, socio-economic and professional characteristics, details describing their reaction to the firm's promotions and offers or showing their online behaviour, *e.g.* if they opened, forwarded or deleted the emails sent to them, how much time they spent on a webpage and on which items they clicked. The new data comes from further transactions with the individuals or other online sources: publicly available databases, *e.g.* public mail directories or lists, news groups or chat rooms, telephone directories (Working Party 2000, p. 74); or data brokers, whose business is to gather, classify and disseminate personal information. While for a company's own needs it may be sufficient to have only the minimum data required to carry out a transaction, agencies offering online marketing services and data brokers are interested to have as many details as possible. In this way, they can identify groups of individuals corresponding to criteria established for the purposes of different campaigns.

The various data processing activities by online marketers could be described though a cycle, which starts with data collection, passes through storage, analysis and use (Zarsky 2006) and should finish with deletion. The most accurate information is that directly stemming from individuals. It can be collected either directly soliciting it from them or using

special technological applications. In the first case, companies ask for the data in order to carry out some kind of operation, either a commercial transaction, *e.g.* sale of products or services, or provide a free service, *e.g.* email account or social network profile. In these cases, consumers voluntarily give their information in order to perform the service. Sometimes, it is up to users how much data they will reveal and it is often the case that they provide more details than the minimum required by the website operator. There are also cases when individuals are incentivised to give their data by a present or the possibility to participate in a promotion, lottery or game.

The tools designed to automatically collect data online include cookies, web bugs, spyware and adware (Solove et al. 2006, p. 185-191). These trace and record users' behaviour on the Internet and make profiles with their habits. Very often they are installed on computers without the knowledge of their owners and therefore people are not always informed that their actions are tracked. Sometimes, with the use of tools such as radio frequency identification (RFID) tags and digital rights management (DRM), the two ways are combined. These make it possible for companies to collect data about customers' identities at the time and place of acquisition of products and gather further information about users' behaviour online through solutions installed on the acquired goods.

One of the important requirements for the data used in online marketing is that it should be accurate. Otherwise, marketers cannot reach exactly those consumers who might be interested in acquiring the products and services offered in each campaign. That is why businesses dedicate enormous resources to constantly updating and enriching their databases. This is of the one challenges which technological developments pose to marketers: while it is extremely convenient to merge two databases and add more details to the profiles of individuals, there is always a risk of mistakes which could mix the different pieces of

information, thus making the data in the newly created database inaccurate and practically useless. Therefore, special efforts are needed to ensure the accuracy of the information.

In line with the later stages of the data cycle, information technology offers nearly unlimited storage capacity at a very low price, as well as multiple options to sort the information. Given these conveniences, many data controllers find it unnecessary to delete the data they have collected because they may need it in the future. Thus, they can store data literally forever and have enough reasons to do so. The need of online marketers for detailed and accurate information, on the one hand, and the possibilities to collect and store data, on the other hand, seriously clash with individuals' fundamental right to privacy, which will be examined in the next section.

1.2 The consumers' perspective

The desire of marketers to collect as much information about people as possible collides with individuals' right to privacy, protected as a fundamental right under the Universal Declaration of Human Rights (UDHR) (United Nations 1948). The concept, originally defined as "the right to be left alone" (Warren and Brandeis in EPIC and Privacy International 2007, p. 1), has evolved and "control over personal information - the ability to exercise control over information about oneself" is currently one of its key dimensions (Solove 2002, p. 1092). This work will approach privacy as "the flow of personal data – information about ourselves" (Kang and Buchner 2004, p. 231) because it encompasses exactly those aspects which marketers intrude with their activities.

Technological developments are gradually depriving people of their privacy in the same way that they are constantly increasing the possibilities for marketers to develop their businesses. In the offline world people went to the shop, paid cash and did not necessarily

reveal any information about them to retailers. Even if they returned to the same outlet again and again, the assistants learnt to recognise their faces and the products they would most likely buy, but never knew their names, addresses or professions. Nowadays, people make their purchases via the Internet using credit cards or give their discount cards to salesmen in supermarkets before paying. Daily, they carry out many transactions with various public and private organisations, every time leaving pieces of personal data. What is more, it is often the case that a single transaction leaves a track of personal information with more than one controller. For example, when somebody buys plane tickets online, data about the purchase is recorded by their Internet service provider, the airline company and the bank, which has issued their credit card. Thus, even the simplest transaction reveals pieces of each individual's personality to various controllers. As a result, nobody can stay anonymous, unless they are refusing to use technology.

The information which people give to companies is kept and elaborated further. At the beginning, everybody gives data controllers only the minimum information needed to carry out a transaction: name, physical and email address, credit card number. Over the time, new pieces of data are added to the clients' profiles: preferences, habits, the way in which they behave online. Technology makes it possible to store the information for almost unlimited periods of time at a very low cost, enrich it by adding new details or correct the inaccuracies. In this way, every change in a person's life is reflected in his "digital dossier" (Solove 2004, p. 1). Moreover, there is not just one digital dossier but many, controlled by different companies. While each data controller holds track of a different aspect of one's actions, if combined, this information could reveal everything about an individual. People could not prevent the possible merger of various databases simply because they do not know who controls information about them. The speed at which data spreads makes it impossible to correct potential inaccuracies or delete details which should not be publicly known

(Ciocchetti 2008, p. 19b). Thus, from anonymous customers in the neighbouring supermarket, people are becoming transparent puppets living in a "cube of glass" (Popkostadinova 2007). In this way, the technological solutions, which make it possible for marketers to develop their businesses, are depriving people of individualism and threatening the heterogeneity of the society.

The way in which data is processed in the online world has further disadvantages for individuals. This information, accumulated by different controllers over large periods of time, is often used to make judgments about them and thus to influence their lives (Solove 2004, p. 52). In this way, somebody may be refused certain goods because of their bad credit history or may not be given a job because of disorderly conduct during their teenage years. Sometimes, data is illegally acquired and used by unauthorised third parties, which can lead to identity thefts, *i.e.* the criminal exploitation of another individual's personality.

Today's data collection practices also have advantages for consumers by offering them personalised and easy-to-use services. Consumers sometimes receive benefits from having their information processed by online companies. If they agree that a company installs a cookie on their computer, they will be identified next time they visit a website and will not have to insert all their details again. In the context of online marketing, the profiling practices make it possible that users are advertised products and services they may actually need and want to buy. Having these goods offered directly and the possibility to purchase them by only a mouse click save them lots of time and efforts. Despite the benefits they get, users seem really concerned about their privacy online. In order to identify their main worries, a survey was carried out, the results of which will be discussed in the next section.

1.3 Consumers' concerns about data online

A 12-item questionnaire was distributed through convenience sampling to 285 individuals from the social network of the author though Facebook. The website was used to distribute the questionnaire for three main reasons. First, the social network is often a means to collect personal data on the Internet. This is done both by the platform operator, which notifies users for this practice in the terms and conditions to which each new subscriber has to agree (Facebook 2007), and unauthorised third parties. Therefore, Facebook users have revealed their personal information at least once, to register for the services of the platform, and should be aware of the advantages and threats related to providing their data to online companies. Second, through the platform and the contact list of the author it was easy to access the most attractive target group for advertisers: people aged between 20 and 45, who are active Internet users and therefore likely to be interested in new products and services. As a result, they are often bombarded with commercial communications messages. A third argument justifying the choice of Facebook to carry out the survey is that the platform's subscribers most probably utilise other services online which require identification and therefore should have an opinion on the issue of how their data is handled. Although convenience sampling does not grant external validity to the research, the results can provide a snapshot about the attitude towards online personal data protection of the consumer group which is most strongly affected by the practice.

The survey was conducted between 19 May and 5 June 2008. Out of those polled, 140 people filled in the questionnaire. The respondents were residents of Bulgaria, Romania, Hungary, the United Kingdom, Spain, Italy, Germany, Austria. Most of the participants filed the questionnaire directly on Facebook, using a special application of the platform. However, seven of them were so concerned with their privacy that they preferred to send their opinions by email. Their contributions were later added to the rest of the answers.

The main purpose of the survey was to identify the main areas of concern for Internet users in line with their privacy online. Therefore, the questions concerned the different stages of the data cycle: collection, processing, storage and deletion. In addition, the inquiry aimed to find out whether users would take any actions to counteract possible abuses of their data. Most of the questions referred to the data collection stage of the cycle since here is where users have the strongest level of control over their personal information (Annex 1).

To begin with, the survey showed that most respondents were either very (25%) or fairly (47%) concerned that Internet companies collect and store their personal data. Less than one third said that they were not very concerned and only 1% said they were not at all concerned. This means that privacy online is an important issue for the Internet users approached. Still, they give their data when they get something in return: in most cases, a free service, *e.g.* email account or a social network profile (56%), or the possibility to buy a good or a service online (40%). Very rarely (2%) they reveal personal details to participate in a promotion or a game. Most of the participants in the survey said that they did not give Internet companies more data than the minimum required (93%), which means they have a protective attitude towards their information. These results make it possible to conclude that the majority of people are concerned about their data online, which is why they reveal as few details as possible.

The Internet users approached were not always aware that their personal data is occasionally collected without their knowledge: 15% said that they did not know that sometimes companies tracked and recorded their movements on a website. This shows either that some users do not pay much attention to the terms and conditions they agree when registering for a service, or that companies do not always properly inform individuals about the practices they use. However, while only 21% said they had never heard about technologies limiting the collection of personal data online, just 26% said they had used them. The reasons for this may be different. One respondent pointed out that the use of these

technologies blocked his access to some websites. Consequently, although most people are informed that their data is sometimes collected without their knowledge, only a small fraction of them try to protect themselves by using special tools.

In terms of processing, most of the respondents (95%) said they considered it a problem if a company to which they had given their personal data transferred it to another firm. However, few of those polled commented that it is not a problem as far as it is mentioned in the terms and conditions they have to agree. As far as storage and deletion are concerned, the biggest portion of the respondents (98%) said that it is important for them that Internet operators protect their data. At the same time, about two thirds of the Internet users approached said that they thought it was a problem if companies kept their data for as long as 20 years. Therefore, security measures used by companies and terms of storage of data online are important issues for people. About 85% of the respondents said that they would take some action if they found out that their personal data is lost or misused. Their readiness to counteract possible data abuses shows once again that the security of personal information online is an important issue for them.

The results of this questionnaire make it possible to conclude that Internet users care about how their personal information is handled. Another finding is that they are not always aware that their data is collected when they visit a webpage. In addition, there are some issues of particular importance to them: security measures which online companies apply in order to protect their data, period during which it is held, operations featuring its transfer to third parties. These are exactly the practices employed by marketers in their business operations, which once again shows that there is a potential conflict between people's concerns and industry's interests.

Policy makers have detected the existence of this problem and have been faced with the question how to strike a balance between the nearly opposite stances. On the one hand, it is

their obligation to protect individuals, especially in situations where their fundamental rights are involved. On the other hand, direct marketing is a legitimate business of over 100 billion euro, which employs over 2 million people directly and many more indirectly, in the EU only (FEDMA 2008a)[2], and it needs legal certainty for a good working environment and business growth. The solution to this puzzle is data protection legislation, which also applies to the online marketing sector. The next chapter will examine the way in which the relevant provisions in Europe address citizens' concerns and marketers' needs.

[2] No explicit data about the volume of the online marketing sector was available. Estimated investments in Internet advertising in Europe total 7.3 billion euro (The European Advertising and Media Forecast in FEDMA 2008b).

Chapter 2 – The policy approach to the personal data processing problem

This chapter will present the legislative tools which apply to the data processing activities of online marketers. The existence of good rules *per se*, however, does not give enough protection to individuals. The reason for this is the poor enforcement, a problem presented in the second part of the chapter.

2.1 The regulatory framework

The history of privacy protection regulation starts as early as the Bible (EPIC and Privacy International 2007, p. 5). However, it was not until the 1960s and 1970s that special information privacy protection legislation was elaborated by some European countries and the US. The first explicit data protection document on an international level is the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD 1980). The guidelines consist of eight basic principles, which require that personal information must be obtained fairly and lawfully, used only for the originally specified purpose, adequate, relevant and not excessive to purpose, accurate and up-to-date, accessible to the data subject, kept secure and destroyed after its purpose is completed. Despite their non-binding character, they remain a benchmark in the field. A year later, the Council of Europe (CoE) adopted its Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe 1981), which includes basically the same provisions.

On an EU level, privacy has been recognised as one of citizens' fundamental rights. Article 7 of the Charter of Fundamental Rights of the European Union grants people respect for private and family life, while Article 8 deals especially with personal data protection

(European Parliament 2000, p. 10). It summarises the provisions of the EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (European Parliament 1995), known as the Data Protection Directive. The main purpose of the document is to protect individuals' fundamental right to privacy, as well as to "contribute to economic and social progress, trade expansion and the well-being of individuals", *i.e.* the development of the common market. In other words, the Directive is aimed at ensuring both personal data protection and a good environment for market growth. The principles of the Directive are comparable with those stipulated in the international frameworks. In addition, it introduces clear rules how the regulation of data protection should be organised at national and EU level. The document requires from each Member State to set up a supervisory authority to observe and regulate the data protection process in the country. In this way, the supervision of data protection activities is delegated to special enforcement bodies operating at national level. At community level, this task is carried out by the European Data Protection Supervisor (EDPS). The country level authorities, the EDPS and the Commission, represented by the Data Protection Unit in the Directorate-General Justice, Freedom and Security, together form the Article 29 Working Party (European Parliament 1995).

In line with technological developments, the general Data Protection Directive was complemented, in 2002, by the Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, also known as the Directive on Privacy and Electronic Communications or the ePrivacy Directive (European Parliament 2002). The document does not grant citizens additional rights, but establishes specific provisions relevant to the electronic communications sector. It is currently being reviewed under the EU initiative to update the pool of documents regulating the telecommunications sector, the so called "Telecoms package". The ePrivacy Directive is

modified with the intention to "enhance the protection of personal data and the privacy of individuals in the electronic communications sector" (Working Party 2008b, p. 2). Since the review process has not finished yet, this research will refer to the original text of the Directive as adopted in 2002.

These Directives form the general data protection framework in the EU. Although they are considered to ensure good level of legal protection for individuals and a sound working environment for industries, the rules are seen as ineffective due to their poor enforcement (European Commission 2003). The next section will outline the main reasons for this problem and suggest a possible solution.

2.2 The enforcement problem

Legislation could only be useful if it is successfully put into practice. Under the legal tradition, enforcement stems from two sides: public authorities entitled to monitor if rules are observed, and citizens who complain if their rights are infringed. In the data protection field, enforcement problems as detected by the European Commission in its First report on the Implementation of the Data Protection Directive (2003), result from both the inability of supervisory bodies to fully carry out their obligations and the fact that individuals do not exercise their rights (p. 12). The Commission finds out that the supervisory authorities are under-resourced and have to deal with a large number of issues, which prevents them from closely monitoring the activities of data controllers. Even if they were not, however, it is practically impossible to oversee every single data processing activity by a public or a private entity in a country. The reason for this is the proliferation of actors who handle personal information and the large number of operations they carry out on a daily basis. Therefore,

even if supervisory bodies were allocated larger financial and human resources, it would be still difficult to solve the enforcement problem.

At the same time, the Commission discovers a "low level of knowledge of their rights among data subjects" (European Commission 2003, p. 12). Therefore, people would not file a complaint with the respective data protection authority, simply because they are not aware what their rights are. Although the Facebook survey revealed that large number of the participants (85%) would take an action if they found out that their data was abused, which shows they are aware that they have the right to privacy protection, it is not certain if they would know whom to contact. Therefore, they might not be aware of all of their rights, which they would need for successful enforcement of the Data Protection Directive.

This is also the conclusion of a survey on personal data protection carried out among the 27 EU Member States at the beginning of 2008 (The Gallup Organisation 2008). It showed that only a quarter of the respondents were fully informed about the variety of rights they had regarding their personal information. Although the majority of the participants knew that they could oppose the use of their personal data for marketing purposes (88%), had to give their consent in order for their information to be further processed (81%), could correct inaccurate or unlawfully obtained information (78%), could go to court with a complaint related to their personal data (71%) and ask for a compensation (61%), as well as access their personal data held by others (59%), only 27% of the participants in the survey knew that they had all these rights. Therefore, even if they know that they have the right to access information about them stored by a marketing company, they might not know that they could complain if the firm refuses to give them access to it.

These two enforcement problems lead to a third: "very patchy compliance by data controllers" (European Commission 2003, p. 12) due to the relatively low risks of getting

caught. As Emilie Barrau, the BEUC representative interviewed for the purposes of this research, pointed out:

> "Today they [companies] know that even if they don't obey the law, they would not have problems or whatsoever, because data protection authorities have so much work they cannot deal with it, consumers will not go to court because it will be too expensive and they are afraid of it. These are all benefits for them. If I do not apply the law, I will be better off when compared to my competitors who apply the law and I will not have cost or whatsoever because nobody is going to enforce the law."

Thus, the existence of good data protection legislation does not guarantee adequate protection to citizens because of the poor enforcement of the law. In this way, the balance of interests which policy makers aimed at achieving through the elaboration of special information privacy protection frameworks is being disturbed. Urgent intervention is needed to recover it. A possible solution of the enforcement problem is the issuing of interpretative communications to clarify the understanding of certain provisions (EDPS 2007, p. 9). An alternative is the adoption of sector-specific rules, e.g. in domains such as the RFID technologies (EDPS 2007, p. 8), which shall provide details on the implementation of the provisions. A means to avoid "excessively detailed legislation" (European Commission 2003, p. 26) and provide details relevant for particular sectors is the adoption of non-legislative instruments, *e.g.* self- and co-regulatory mechanisms, benchmarking, best practices, third-party privacy audits (EDPS 2007). The next chapter will concentrate on self- and co-regulation practices as a possible solution to the enforcement problem of data protection legislation in Europe.

Chapter 3 – Self- and co-regulation: solution to the enforcement problem

This chapter will present self- and co-regulatory mechanisms as a potential solution to the enforcement problem of data protection legislation. For this purpose, the work will define the practice and show its evolution in the EU in general and in the information privacy field in particular. The next section will introduce the community-level self- and co-regulatory tool adopted in the data protection sector, the European Code of Practice for the Use of Personal Data in Direct Marketing, and present the incentives of the different stakeholders involved in its elaboration, implementation and enforcement, to participate in the process.

3.1 Self- and co-regulation mechanisms in data protection in Europe

Self- and co-regulation practices are procedures whereby public and private actors interact in the elaboration and enforcement of rules regarding certain areas of activity, often using codes of practice or good conduct. A comprehensive definition envisages "the existence of some form of relationship between binding legislation and voluntary agreements in a particular area" (Best in Senden 2005a, p. 11). In the EU context, there is a difference between the two practices. Co-regulation requires the prior adoption of a legislative act delegating the enforcement of certain rules to a range of stakeholders (European Parliament 2003, p. 3). Therefore, a public actor is necessarily involved in the process. This is not the case with self-regulation, where the elaboration of rules and their enforcement lies in the hands of non-public actors only (European Parliament 2003, p. 3). Although Price and Verhulst (2005) use the term self-regulation to describe the introduction of rules both with and without their prior prescription by the government, Price (personal communication, 31.03.2008) admits that self-regulation *per se* does not exist, because even when an industry

decides to impose certain restrictions by itself, it is always in an attempt to prevent stricter governmental control. In order to avoid disagreement over the exact terminology applied to the practice and for the sake of integrity, this paper will use the generic term self- and co-regulation. When a differentiation is needed, the terminology suggested by the EU will be applied.

The EU started promoting these tools at the beginning of the 21st century under its strategy to more actively involve the society in the governance process. Several policy papers build up the framework encouraging the more active use of soft-law instruments. In 2001, the Commission adopted the White Paper on European Governance, which suggests switching from predominantly top-down to more bottom-up approach, combined with non-legislative policy instruments, such as "recommendations, guidelines, or even self-regulation within a commonly agreed framework" (European Commission 2001, p. 20). In 2002, the Action Plan on Simplifying and Improving the Regulatory Environment was approved, which deals with a broad range of modes of governance, including the use of soft law (recommendations), co-regulation, voluntary sectoral agreements, benchmarking, peer pressure, networks and the open method of co-ordination (European Commission 2002). A year later, the European Parliament, the Council and the Commission concluded the Interinstitutional Agreement on Better Law-Making. As Senden (2005a, p. 5) points out, the document sets out, for the first time, the general framework and conditions for the use of self- and co-regulation in the EU. The provisions which the framework includes regarding the use of these mechanisms closely follow those established nearly a decade earlier in the data protection field through the Data Protection Directive.

Article 27 of the Directive encourages the adoption of sector-specific codes of conduct by industries as instruments of self- and co-regulation. These documents, aimed at interpreting the provisions of the Directive with regard to the particular needs of different industries, have

to be approved by the Article 29 Working Party before entering into force. This requirement is relevant only for Community-level codes. Later, the application of self- and co-regulatory mechanisms in the data protection field has been promoted at public events (Bolkestein 2002) and in further documents of the Commission (European Commission 2003, European Commission 2007).

The implementation of self- and co-regulatory mechanisms is particularly important in the information privacy field for several reasons. First, the proliferation of private actors who carry out data processing activities and the large number of operations they perform make "privacy protection through pure reliance on formal government regulation practically impossible" (Newman and Bach 2004, p. 403). What is more, there is market asymmetry between data processors and data subjects, which makes data protection an example of a market failure (Ibid.). The reason for this is that businesses possess bigger possibilities to process and control the information, while citizens do not have the resources to oppose them. In addition, the knowledge of industries about the quantity and quality of data gathered is often superior, which automatically makes them better off.

In addition, self- and co-regulatory mechanisms could successfully address all the three aspects of the enforcement problem of the Data Protection Directive. Their implementation will remove part of the enforcement burden from the supervisory authorities, transferring it to data controllers themselves and to the organisations whose members they are. The voluntary commitment to certain rules on behalf of the industry will ensure higher level of compliance. Besides, once businesses have realised the benefits they could get from the application of self- and co-regulatory mechanisms in terms of image and customers' trust, they will promote these procedures by mentioning them in their reports and referring to them on their webpages. This will increase the awareness of data subjects about their rights in the information privacy field and possibly make them require better data protection on behalf of controllers.

Currently, the direct and interactive marketing sector in Europe has a Community-level code of conduct, elaborated and approved in line with the procedures established by the Data Protection Directive and the Article 29 Working Party (European Parliament 1995, Working Party 1998). The instrument was submitted for formal approval by the Article 29 Working Party in 1998 and adopted in 2003 (Working Party 2003). The procedure took as long as five years because it was returned to FEDMA several times with different comments, which the organisation had to include in the final version of the document. In addition, the Article 29 Working Party asked the opinion of BEUC and insisted that FEDMA considered their concerns as well (Ibid.). The document does not directly regulate the data processing activities of marketers, but sets the minimum standards which the direct marketing associations at a country level, members of FEDMA, have to establish and follow in the national codes they prepare. The code is currently complemented by the Online Annex (FEDMA 2007b). It gives details about specific online marketing activities with regard to data processing. The first draft of the Annex was filed with the Article 29 Working Party in March 2007 and the final version is expected to be approved in September 2008 (Brandau interview).

Given the fact that the European direct and interactive marketing sector in the only industry which has adopted a community-wide code of conduct in line with the procedures established by the Data Protection Directive, it is interesting to understand the motivations of the various stakeholders to participate. For this purpose, the ideas of the representatives of the institutions involved in the self- and co-regulatory process will be presented as put forward during the interviews conducted with them. The officials are Goetz Brandau, Legal Affairs Manager of FEDMA, Richard Knubben, Policy and Implementation Manager of EASA, Emilie Barrau, Junior Legal Officer at BEUC, and Jose Manuel de Frutos Gomez, Policy Officer at the Data Protection Unit of Directorate-General Justice, Freedom and Security of the European Commission. As it has already been explained, the views expressed by De

Frutos Gomez give insight both into the work of the Commission and the Article 29 Working Party. For the sake of integrity, the motives they presented will be combined with theoretical arguments.

3.2 Stakeholders' incentives to commit to self- and co-regulatory practices

The main reason why companies agree to adopt self- and co-regulatory practices is that this is a way to avoid more costly and restrictive government regulation (Boddewyn in Price and Verhulst 2005, p. 12). The FEDMA official agreed with this argument (Brandau interview). In addition, these procedures can enhance marketers' credibility among the various groups of stakeholders with which they have relationships in general and consumers in particular (Boddewyn in Price and Verhulst 2005, p. 12, Knubben interview, De Frutos Gomez interview). What is more, self- and co-regulation procedures are quicker and more flexible than state regulation (Just and Latzer 2004, p. 45), especially in terms of implementation and enforcement. As Knubben from EASA explained, by the time a statutory court issues its decision on a problem, its ruling will be no longer useful for the company which filed it.

Businesses adopt these mechanisms because this is usually a condition for membership in the interest groups which have adopted the guidelines. Interest groups are organisations, separate from the government, which aim at influencing public policy by defending the interest of their members (Wilson 1990, p. 8). Individuals are incentivised to organise in groups because in this way they can more efficiently achieve their common interests (Olson 1993, p. 26). Since the actions of interest groups would benefit non-members operating in the same sector as well, affiliates are normally provided with additional "selective" benefit (Olson 1993, p. 34). In the case of FEDMA, this is a direct access to the lobbying process (FEDMA

2004). Therefore, if online marketers want to better pursue their interests in front of the EU institutions, they have to commit to the organisation's rules, including to follow the standards established by its codes of conduct.

Public authorities also have several reasons to encourage self- and co-regulation practices in online marketing. In this way, businesses use their sector specific know-how to tailor rules which are applicable to their particular area of activity (Just and Latzer 2004, p. 45). Statutory regulators are often incompetent to deal with the problems of some industries, especially those that are technologically complex. The reason for this is that "detailed regulations are rapidly overtaken by events and can often easily be circumvented" (Verrue 1999). By transferring certain regulatory obligations to industries, public authorities avoid the necessity to constantly try to catch up with new developments. What is more, the EASA representative noted, in the commercial communications sector it is difficult to make statutory rules applicable to the country specific context, while self-regulatory organisations can apply more flexible criteria in their judgments (Knubben interview). In addition, by committing to self- and co-regulation, businesses relieve part of the regulatory burden from the often under-resourced public sector. This argument is particularly relevant to the data protection sector. As Brandau from FEDMA explained "we have to monitor our members and ensure they also follow our code". Just and Latzer point out that this reduces the regulatory cost to the state (2004, p. 45). What is more, by adopting self- and co-regulation practices, firms voluntarily commit to follow them, which "is an effective way to ensure compliance with the privacy principles in a specific sector", De Frutos Gomez from the Commission said.

Consumers also benefit from the adoption of self- and co-regulatory practices by industries. By ensuring better compliance with data protection rules by companies, these mechanisms guarantee higher level of security and control over personal information to citizens. Another benefit is that customers have their complaints handled more quickly and

less expensively, since they do not need to hire a lawyer, Barrau from BEUC pointed out. For this purpose, a complaint mechanism has to be in place, which is not always the case with codes of conduct. Another problem Barrau identified is that in many cases codes of conduct practically repeat the text of the law without any added value, which does not further consumers' interest beyond the protection which users already get by law. Additional criticism she advanced is enforcement:

> "If you have a code of conduct, made for the industry and by the industry, what is the incentive for them to sanction and give proportionate sanctions whenever there is something wrong? You are not going to bind the hands which feed you!"

To wrap up, public authorities, private actors and consumers all have incentives to implement self- and co-regulatory mechanisms. Still, in order for a code of conduct to be in the interest of citizens, it has to meet all the three criticisms advanced by BEUC: the existence of a complaint mechanism, added value of the document and proper enforcement. In addition, it has to address people's concerns as identified by the Facebook survey carried out for the purposes of the present research. Thus, it order to assess the effectiveness of the self- and co-regulatory mechanisms as applied by the online marketing sector in Europe with regard to data protection, particularly FEDMA's European Code of Practice for the Use of Personal Data in Direct Marketing and its Online Annex, it is necessary to analyse them in the light of the aforementioned criticisms. This will be done in the next chapter of the thesis.

Chapter 4 – Assessing the effectiveness of self- and co-regulation in Europe's online marketing

This chapter will first establish a set of criteria to assess the effectiveness of FEDMA's European Code of Practice for the Use of Personal Data in Direct Marketing and its Online Annex. Then, the thesis will analyse the two documents and detect their strong and weak points. At the end, the chapter will make recommendations for improvement of the code and its annex in order to enhance the effectiveness of the self- and co-regulatory practices of online marketing.

4.1 Establishing the criteria for effectiveness

Four main sources of information were consulted in order to elaborate a comprehensive set of effectiveness criteria. The first one is a decision of the Article 29 Working Party in which it stipulates that a code of conduct should be in accordance with the data protection directives and of "sufficient quality and internal consistency and provides sufficient added value" in order to receive an approval (Working Party 1998, p. 4). The second source is an academic research by Harker (2003) where the author summarises the main conditions for the effectiveness of the practice in the advertising sector. Those relevant to the online marketing will be used in this work. The third document is a report of the Directorate-General Health and Consumers, prepared as a result of the Round Table on Advertising Self-Regulation, held in 2006. At this event the Commission, interested non-governmental organisations (NGOs), including BEUC, and EASA, identified the Best Practice Model in self- and co-regulation in advertising (European Commission 2006). Again, those relevant to the online marketing sector will be used for the purposes of this research. Fourth, the comments made by Emilie Barrau from BEUC will be taken into account. By combining the criteria of the different

groups of stakeholders, this work aims to provide a framework which meets the effectiveness requirements of all the parties involved. The resulting set of criteria is as follows:

1. **Formal criteria**
   - legitimacy of the organisation elaborating the code
   - enough funding for the activity
   - participants in the drafting process: involvement of all the interested stakeholders
   - endorsement by public authority
   - regular audit of the rules, including the publication of annual reports

2. **Substantive criteria**
   - compliance with the law
   - added value, *i.e.* sector-specific provisions

3. **Implementation criteria**
   - education of the industry with regard to the standards established by the code
   - ease of access to the code
   - creation of public awareness

4. **Enforcement criteria**
   - complaint mechanism
   - sanctions for non-compliance

The next section will look at each of these criteria and compare FEDMA's procedures against them. In order to fully assess online marketers' practices, it is necessary to evaluate

both the European Code of Practice for the Use of Personal Data in Direct Marketing and its Online Annex. Therefore, the analysis will look at both documents, specifying to which of the two it refers. If no explicit note is made, the activities of FEDMA in general are considered. It is important to remember that the version of the Online Annex, which this thesis considers, is preliminary and has not been approved by the Article 29 Working Party. It will be further amended in the near future in order to meet the formal requirements of the public authority. The provisions it establishes only give an idea about what could be part of the final version of the document.

4.2 Evaluating the code and its annex

The evaluation will be carried out following the order of the criteria as established above. Conclusions will follow the section relevant for each criterion. The assessment will start with the formal criteria, which refer to the procedures followed and the actors involved in the elaboration, implementation, enforcement and monitoring of the European Code of Practice for the Use of Personal Data in Direct Marketing.

4.2.1 Formal criteria

Legitimacy of the organisation elaborating the code

Legitimacy means that the organisation elaborating and administering a code of conduct should be representative for the particular industry. In order to find out if FEDMA meets this requirement, a short overview of the organisation's history and structure is needed. It was established in 1997 through the merger of Europe's first direct marketing organisation, European Direct Marketing Association (EDMA), created in 1976, and the younger Federation of Direct and Interactive Marketing (FEDIM), set up in 1992. Currently, it is the

only European wide direct and online marketing organisation. Its members are 28 national Direct Marketing Associations (DMAs), of which 24 are European, and about 250 companies using direct and online marketing as part of their commercial communications strategies. Through the national DMAs, the organisation represents over 10,000 firms, most of them in Europe. It defines itself as "the single voice of the European direct and interactive marketing industry" (FEDMA 2008a). The organisation's mission is to protect the interests of its members from restrictive legislation, to promote European direct and interactive marketing industry and to inform the different groups of stakeholders about the sector. This information makes it possible to conclude that FEDMA is sufficiently representative for the direct and online marketing sector in Europe to legitimise the self- and co-regulatory documents it has elaborated.

Enough funding for the activity

Information about the finances allocated to the administration of the code would be a proof of the importance of the activity for the organisation. However, FEDMA does not publicly reveal data about its budget. What is known is that the organisation and its various activities are funded through membership fees. Given the large number of members that FEDMA has, it can be assumed that it has sufficient budget to carry out its operations, including the elaboration, implementation and enforcement of its European Code of Practice for the Use of Personal Data in Direct Marketing and its soon-to-be-approved Online Annex. What is more, FEDMA has been involved in self- and co-regulation for more than ten years. The longstanding commitment to the activity is a further proof of the fact that it allocates sufficient finances to it.

Participants in the drafting process

In order for a code of conduct to be effective, it has to address the interests of all the stakeholders concerned by it: public authorities, industry and consumers. For this purpose, the involvement of all of them in the drafting process is needed. The FEDMA code is a result of the joint efforts of the industry and the Article 29 Working Party (FEDMA 2003, p. 1). The Article 29 Working Party is composed by officials of the Data Protection Authorities (DPAs) of all the Member States, the EDPS and the European Commission. The presence of officers from 29 institutional bodies makes it a balanced and impartial representative of the public interest. In addition, in the process of approving the document, the Article 29 Working Party consulted BEUC (Working Party 2003, p. 3). This is not a procedural step required by law, but a decision taken in order to more actively involve consumers in the process of elaboration of the code and thus make sure that their interests are well safeguarded (Working Party 2003, p. 3). BEUC concerns related to the protection of minors were taken into account in the final version of the code. The organisation also recommended that FEDMA introduced provisions related to its members' online practices. The marketing activities on the Internet are considered in the code's annex, which is in the process of adoption.

With regards to the Online Annex, BEUC has not been informed that FEDMA is preparing such a document, the representative of the organisation said (Barrau interview). Brandau from FEDMA pointed out that it is in the competence of the Article 29 Working Party to contact BEUC and consult the annex with them. Following its practice with the code, the Article 29 Working Party should ask the opinion of the consumers' organisation in order to make sure that the interests of Internet users are well represented.

Endorsement by a public authority

Such a step is needed in order to ensure the legitimacy of the document. Article 27 of the Data Protection Directive, regarding codes of conduct, stipulates that "Draft Community

codes, and amendments or extensions to existing Community codes, *may* be submitted to the Working Party referred to in Article 29" (emphasis added). The formulation poses certain ambiguity whether the approval is actually mandatory. De Frutos Gomez from the Commission commented that a formal approval is the only way to secure "political backing" of the document and to make sure it is good enough to be enforced on the members of an organisation. The FEDMA representative agreed that coordinating the document with the Article 29 Working Party a necessary part of the process of adopting the code:

> "If they say it is desirable they mean they expect it. (…) But that's pretty much saying that if we don't do it we are going to have another Directive. Or they are going to put it into a law. And it's gonna be much more difficult for us to negotiate. (…) In this process, with the self-regulatory code, at least we can negotiate." (Brandau interview)

The Article 29 Working Party approved the European Code of Practice for the Use of Personal Data in Direct Marketing and is currently reviewing its Online Annex. Therefore, a public authority is actually endorsing the document.

Regular audit of the rules

Regular audit of the rules is needed in order to ensure they are good enough to address the different activities of practitioners. The FEDMA code envisages that a special committee within the organisation should consider annually if a revision of the code is necessary and provide the Article 29 Working Party with "an annual report on the functioning of the code at national level and in cross-border activities" (FEDMA 2003, p. 18). However, the organisation does not prepare annual reports for the Article 29 Working Party. Therefore, it cannot be sure if the code is effective.

Although the organisation does not prepare regular reports in writing, FEDMA gathers information about possible problems with the implementation of the code from its national members. It later discusses them at its frequent meetings with the Article 29 Working Party:

> "This works both ways, meaning that the Article 29 Working Party also approaches us when they become aware of problems with the code." (Brandau, personal communication, 07.07.2008)

Therefore, FEDMA does take some measures to ensure that the code is properly implemented and is relevant to the current market situation. Still, the organisation only relies on the complaints it receives to serve as a control mechanism. What is more, the existing reporting system is only verbal, which does not make it reliable enough. This does not mean that the rules are outdated and not applied properly. The case may be exactly the opposite, but FEDMA does not have an adequate report mechanism to prove that. This is not a good proof that the procedures applied are actually effective in protecting the interests of consumers and ensuring a sound working environment for businesses.

Conclusions on formal criteria

The European Code of Practice for the Use of Personal Data in Direct Marketing and its Online Annex fully comply with three out of the five formal criteria: legitimacy of the organisation drafting the code, enough funding for the activity and endorsement by a public authority. The involvement of all the stakeholders concerned by the activities of online marketers is only relevant for the code, but not for the annex. However, it would be easy to involve consumers' representatives more actively in the process of composing the annex by inviting BEUC to comment on the draft. In addition, the enforcement of FEDMA's code at a national and international level is not systematically monitored by the organisation, which is another weak point of the document for three reasons. First, in this way FEDMA is not aware whether the standards established by the code are actually applied. Second, this practice is contradictory to the text of the code. Thus, the organisation itself does not enforce the requirements of its own code, which questions both its willingness to involve in self- and co-regulatory procedures and its reliability. Third, this creates the risk of manipulating the compliance with the code: it is relatively easy that an organisation says it is following the

standards the instrument establishes without actually doing it, because nobody is checking whether this is true. FEDMA transfers the responsibility to national DMAs to supervise their members on a country by country basis. However, the marketing organisation does not monitor whether DMAs actually do it. In addition, it does not exercise any control over the activities of its direct corporate members.

The elaboration of the annex makes up for the content drawback to a certain extent, because it is intended to meet the challenges posed by technological developments and their application by the sector. Nevertheless, the annex is based on the text of the code. Therefore, if it has certain shortcomings, they will be transferred to the annex as well, which will enlarge the problem. Therefore, FEDMA needs to start elaborating and publishing written reports on the functioning of the code as stipulated in the text of the document, which will help it detect areas where it would need possible amendments and strengthen the control over the compliance with the code.

4.2.2 Substantive criteria

These criteria are aimed at assessing the content of the code and checking to what extent it complies with the data protection directives, what is its added value and how it addresses consumers' questions regarding the information privacy practices of online marketers. In order to answer the last question, the concerns raised by the participants in the Facebook survey were taken into account.

Compliance with the law

This is one of the two criteria which a code of conduct has to meet in order to get the approval of the Article 29 Working Party. According to its opinion issued in support of FEDMA's code, it is "is in accordance with the Directive and the national legislation in

place" (Working Party 2003, p. 3). With regard to the Online Annex, the Article 29 Working Party concludes that "some work needs to be done in order to bring it in line with Directives 95/46/EC and 2002/58/EC" (Working Party 2008, p. 9). It is to expect that FEDMA will consider the Working Party's comment and the final version of the annex will be adjusted to better comply with statutory regulations.

Still, in order to identify the level of compliance with the law, it is necessary to see how exactly the provisions of the directives are transposed into the code and its annex. For this purpose, this subsection will analyse the way in which FEDMA's self- and co-regulatory documents address consumers' concerns as raised by the participants in the Facebook survey, namely:

- information that data is collected
- security measures by Internet companies
- period of data retention
- data transfers to third parties

The Data Protection Directive requires that data controllers inform data subjects about their identity and the purposes of processing at the time of collection of data. The same provision is included in the code and the annex. Although the directives do not have special provisions about data collected automatically, the ePrivacy Directive requires that the stipulations of the Data Protection Directive shall refer to these practices as well. Thus, data subjects should be informed when such tools are used, given the opportunity to refuse the collection of data and explained what the consequences of a refusal could be (European Parliament 1995). These requirements are included in the draft of FEDMA's Online Annex (FEDMA 2007). In addition, the documents prohibits data controllers to use information collected via cookies to sell products or services to data subjects that have not expressed their

explicit interest in an offer, which is a clause that goes beyond the minimum requirements stipulated in the legislative provisions.

Both directives have special terms regarding the security measures which data processors have to implement with regard to the information they handle. The FEDMA code broadly repeats the same provisions. In addition, it suggests companies to employ Privacy Enhancing Technologies (PETs) and gives sector-specific examples for practices which businesses could employ. The draft of the annex does not have a section dedicated to the issue. However, given the possibilities to store data online, it would be reasonable to reiterate the importance of data security by including a specific provision on the issue in the final version of the annex.

Regarding data retention, the Data Protection Directive requires that data should be: "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed". The same provision is repeated by the FEDMA code. However, neither the code, nor its Online Annex, recommends a period of maximum data retention. In order to more effectively meet users' concerns, explicit stipulation of this term should be provided. This is particularly important in the case when a consent was generated after a single transaction between a company and a consumer, which happened long time ago.

The Data Protection Directive requires data subjects "to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses". This provision is included in the code and its Online Annex. Thus, it is up to users themselves to decide whether they will allow that their data is transferred.

The analysis of these provisions makes it possible to conclude that the code and its annex duly follow the texts of the directives. Still, certain areas have been identified where amendments are needed, particularly the implementation of security measures and the period

of data retention. Nevertheless, the two documents introduce a few requirements which go beyond the text of the directives, which is the case with certain practices related to cookies. Whether the self- and co-regulatory documents provide further added value, which would be a sign for real willingness to protect consumers' interests, will be discussed in the next subsection.

Added value

This is the second criterion which a code of conduct has to meet in order to get the approval of the Article 29 Working Party. In its assessment of the FEDMA code, the Article 29 Working Party finds out that it is "sufficiently focused and deals with a good number of significant matters in the direct marketing sector". These include: definitions, enumeration of the possibilities to collect data, practices regarding specific sector issues (*e.g.* host mailings, disclosure of lists), provisions on the protection of children, detailed elaboration on the right to object the processing of data for direct marketing purposes (Working Party 2003). For example, while the Data Protection Directive does not require specific measures to ensure that children are adequately protected, the code stipulates that "Data Controllers should always make every reasonable effort to ensure that the Child and/or the Parent are properly informed about the purposes of the processing of the Child's data". Another prominent example of added value is the recommendation that data controllers should deal with data subjects' requests within 20 working days (FEDMA 2003, p. 14), a provision which is not included in the legislation. A third example is the requirement that data processors should designate a person within the organisation to deal with data protection issues. In addition, the code includes examples which substantiate the provisions that are also considered as a manifestation of added value, the representative of the Commission said (De Frutos Gomez interview).

The draft of the annex contains provisions related to the categories which the Article 29 Working Party identifies as manifestations of added value of the code. These include definitions, enumeration of the possibilities to collect data online and specifications in what cases this data can be used for marketing purposes, practices relevant for the sector (*e.g.* online member-get-member campaigns, host mailings). It also introduces the requirement that FEDMA members should elaborate privacy policies explaining users how their personal information will be handled.

Following Article 29 Working Party's recommendations, FEDMA has agreed to introduced clauses on the protection of children in a revised version of the code, the official from the organisation said (Brandau interview). Therefore, it is possible to conclude that the code has added value as well.

Conclusions on substantive criteria

The code and its Online Annex largely comply with the substantive criteria for effectiveness. However, in order to fully meet consumers' concerns, it would be reasonable to include provisions on security measures which data processors have to apply in the final version of the annex, as well as stipulate the period of maximum data retention. This will improve the texts so that they better address consumers' interests.

4.2.3 Implementation criteria

These criteria are aimed at identifying to what extent the code is known by the industry and consumers. This would make it possible to understand whether the standards it establishes have the chance of being respected by the industry and if consumers would rely on it to complain and have their problems resolved.

Education of the industry with regard to the standards established by the code

FEDMA members should be well aware of the existence of the code and the standards it establishes because compliance with the document is one of the requirements for membership in the organisation (FEDMA 2004, p. 4). In addition, the association held a workshop on data protection in 2007 and plans to continue with the practice in the future (FEDMA 2007c). The organisation includes the topic in the agenda of events dedicated on the latest developments in the sector (FEDMA 2007a). FEDMA does not forget to mention the code at public events at which it takes part (FEDMA 2008b, p. 2). Therefore, the organisation is putting in efforts to popularise the document among the industry.

Ease of access to the code

FEDMA's code is published on the organisation's webpage and on the one of the Commission, which means that it is easily accessible. What is more, most national DMAs have their domestic codes available at their respective websites so that anybody who would be interested to read them could do so.

Creation of public awareness

FEDMA does not make explicit efforts to popularise the code among the general audience (Brandau interview, FEDMA 2008b, p. 3). However, considering the fact that the code is meant to serve as a basis for the preparation of country self- and co-regulatory instruments by the organisation's national members, it would be more relevant to examine how each of them raises the awareness of the public with regard to the code. Given the EU focus of the present work, this issue could be addressed by further research.

Conclusions on implementation criteria

FEDMA is complying with two out of the three criteria: education of the industry and ease of access to the code. In terms of the third criterion, the awareness of the code among the general audience, it is impossible to assess the compliance with it without examining the situation at a country level, which could be the subject matter of further research.

4.2.4 Enforcement criteria

The purpose of these criteria is to identify how possible complaints based on clauses of the code would be handled and what the consequences for those who have violated the good practices would be.

Complaint mechanism

The existence of such mechanism is important for the sake of counteracting possible infringers of the code. The code of FEDMA requires that national DMAs establish compliant mechanisms in their country codes. In case FEDMA receives a compliant, which is related to a problem at a country level, it forwards it to the respective national DMA, which should resolve it (Brandau interview). FEDMA itself only deals with the resolution of cross-border complaints (FEDMA 2003, p. 18). The body in charge of dealing with complaints is the Data Protection Committee, which is composed of members of the national DMAs, a person within FEDMA and three representatives of direct company members (FEDMA 2003, p. 18). However, an independent element is missing from the complaint resolution body. Such would ensure impartiality of the procedures and guarantee the objectivity of the decisions which have been taken. Therefore, the inclusion of an independent agent should be considered as a means of improving the effectiveness of the code in terms of this criterion.

Sanctions for non-compliance

Sanctions are needed to ensure high level of compliance with the standards established by the code. In the document, FEDMA envisages expelling the member which has violated the rules from the structures of the organisation. Brandau from the association confirmed that this has happened. FEDMA may also consider imposing "other sanctions", including legal actions, in case of violation of the rules (FEDMA 2003, p. 17). However, the organisation does not impose fines for non-compliance, which could possibly be stronger incentives for companies to follow the standards established in the code. Brandau commented that this would be a measure difficult to enforce, considering the fact that companies have to pay membership fees and being required to pay in addition could make them reconsider their membership. Instead, he suggested that good image is a strong enough incentive. De Frutos Gomez from the Commission agreed that the risk of bad image is the only enforceable sanction in the case of organisations with a voluntary membership. Considering the fact that it would be almost impossible and not enforceable to introduce monetary sanctions in a body like FEDMA, it can be assumed that existing penalties are a good option to ensure the effectiveness of the sanctions mechanism. Therefore, it is possible to conclude that they do not have to be changed.

Conclusions on enforcement criteria

These findings show that FEDMA's practices meet the effectiveness criterion demanding sanctions for non-compliance with the self- and co-regulatory rules introduced by an organistaion. The other requirement, referring to the complaint mechanism in place, is not fully addressed, since an independent element is missing from the body entitled to resolve complaints. In addition, the organisation has to amend part of its practices to be able to fully comply with the formal, substantive and implementation requirements for effectiveness. The next section will make suggestions for improvement.

4.3 Recommendations for improvement

Participants in the drafting process

Following its practice with the code and in order to ensure that consumers' interests are well represented in the Online Annex, the Article 29 Working Party should send the document to BEUC for consultation. Then, the legitimate concerns raised by the organisatison should be taken into account in the final version of the code.

Regular audit of the rules

FEDMA should start preparing annual reports about the implementation and enforcement of the code both at European and country level. In this way, it will be able to monitor whether the document's provisions are implemented by its members and are adequate to solve the problems emerging from the practices of direct marketers in general and online practitioners in particular. Thus, the organisation will be capable of more precisely assessing the effectiveness of the provisions it has elaborated, which would be a sign of real concern about the proper functioning of existing self- and co-regulatory mechanisms. This will also help the organisation solve the problem with being in a situation in which it does not comply with the rules it has introduced itself.

The reporting mechanism should be organised in a vertical way: indirect corporate members should be accountable to the national DMAs, which should report to FEDMA. Direct corporate members should prove their compliance with the standards established by the code directly to FEDMA. FEDMA should prepare and submit reports to the Article 29 Working Party, as established in its code. In addition, it should publish them on its webpage for the sake of transparency and to prove its willingness to ensure high level of compliance with the mechanisms it has established. This will make it possible to enforce the self- and co-

regulatory instrument and guarantee it is really applied, and consumers' interests, well protected.

Security measures

In the final version of the annex, FEDMA should include special provisions requiring direct and online marketers to introduce strict security measures regarding data stored in an electronic format. It could even give concrete examples for such tools. In this way, it will encourage its members to be more responsible towards the storage of data, which would possibly reduce the risk of personal information losses, as well as the negative consequences from it.

Period of data retention

Each company working online collects data for different purposes and therefore needs it for varying periods of time. However, as the Facebook survey showed, people are concerned about the length of the period for which companies keep their data. Therefore, the annex should stipulate a maximum period of data retention, which would strike a balance between the needs of direct marketers and the privacy of consumers. The period should vary with regard to the intensity of the relationship of a consumer and a company. In order to balance the interests of users and businesses, it would be reasonable that FEDMA stipulates a period starting from the last date when the two parties were in contact. In order to identity the length of the period, further research should be carried out.

Creation of public awareness

Since FEDMA's code is not intended to directly resolve the complaints of European citizens, but is a benchmark for national DMAs in their efforts to elaborate country level self-

and co-regulatory tools, it is the national codes which should be popularised among individuals. Therefore, FEDMA should assist national DMAs in the efforts to raise the awareness about the code at a country level and actively encourage citizens to use it as a conflict resolution tool.

Complaint mechanism

FEDMA should require that national DMAs include an independent element in the complaint resolution body, called when a problem has to be solved. This would mean "somebody who is not paid by the industry" (Knubben interview). Their role would be to better represent consumers' interest. In addition, FEDMA should include as independent element in its Data Protection Committee every time when it has to deal with a complaint at a cross-border level.

These amendments would address the weaknesses of current procedures and improve the effectiveness of existing self- and co-regulatory practices. Those recommendations concerning the substance and enforcement criteria could be implemented in the Online Annex and be considered in future amendments of the code itself. If online marketers consider the findings of this work, they will show real willingness to protect consumers' interest, not just desire to polish their images. In this way, self- and co-regulatory mechanisms will prove to be effective way of addressing the enforcement problem of the data protection legislation in the EU.

Conclusion

Data protection is a policy area where there is a potential conflict between businesses and individuals: while the former need personal information in order to carry out their activities, the latter want their privacy, individualism and control over their lives. The conflict becomes even more persistent with industries whose everyday operations depend on the processing of accurate data, *e.g.* online marketing, and given the possibilities which technology offers to gather, analyse and store information. In an attempt to strike a balance between the opposite stances, policy makers have elaborated special data protection legislation. In the EU, it includes the Data Protection Directive and the ePrivacy Directive. However, legislation can only be effective if duly enforced and here is where policy makers have detected a problem.

This thesis has suggested self- and co-regulatory mechanisms as a possible solution to this puzzle. The work has explained why these practices would be useful in the data protection area and shown how they have been applied by the online marketing industry in the EU. In order to find out whether these mechanisms really work, the thesis has analysed the self- and co-regulatory tools of direct and online marketing practitioners in Europe, the European Code of Practice for the Use of Personal Data in Direct Marketing and the draft of its Online Annex. For this purpose, a set of criteria based on contributions by the different stakeholders involved has been used.

The analysis has shown that the two documents and the standards they establish are good at addressing consumers' concerns with regard to online marketing practices. However, some amendments are needed in order to better protect the interests of individuals. Nevertheless, at this stage it is impossible to conclude whether self- and co-regulatory mechanisms are an effective way to improve the enforcement of data protection legislation in the online marketing field in Europe. Even if the recommended amendments are made, this will not be

enough to ensure good enforcement. The reason for this is the lack of proper reporting mechanisms. Thus, direct and indirect FEDMA members may claim they follow the standards established by the code and its Online Annex but nobody makes sure this is true. In this way, the enforcement problem of statutory legislation may be a problem of the self- and co-regulatory instruments as well.

Therefore, the most urgent change which FEDMA has to make in line with its code of conduct and the Online Annex is to introduce strict reporting mechanisms. This will make it possible to assess whether self- and co-regulatory mechanisms are really an effective way of improving the enforcement of data protection legislation in the online marketing sector. If these practices are effective in this sector, they could be adopted by other businesses and in other policy fields, thus ensuring the balance between the interests of individuals and businesses. If not, other means have to be considered to guarantee there is a balance between the interests of citizens and businesses with regard to data protection. This is the only way to ensure that today's world is not turning into the reality of 1984, where everything Winston Smith does is known by the Big Brother, or The Trial, where Joseph K. has lost control over the information about himself. Because both situations are detrimental to individualism and heterogeneity, values which humanity highly appreciates and which has allowed it to reach its current stage of development.

Appendix 1

Facebook questionnaire

1. **Are you concerned that Internet companies collect and store your personal data (e.g. name, age, address, telephone number, bank card number)?**

- Very concerned
- Fairly concerned
- Not very concerned
- Not at all concerned

2. **In what occasions do you voluntarily reveal personal data to companies online? (Multiple answers are possible)**

- To register for a free service (e.g. free email/ social network account)
- To purchase a good/ service
- To participate in a promotion/ game
- Other (please, specify)

3. **Are you aware that your personal data is sometimes collected without your knowledge (e. g. when you visit a website they track where you go and what you read)?**

- Yes
- No

4. **Is it important for you that Internet companies protect your personal data?**

- Very important
- Fairly important
- Not very important
- Not at all important

5. **Would you take any action if you understand that your personal data has been lost or misused?**

- Yes
- No

6. **Do you consider it a problem if your data is kept and still available in 20 years?**

- Yes
- No

7. **Do you think it is a problem if a company to which you have given your personal data transfers it to another company?**

- Yes
- No

8. **Do you give Internet companies more data than the minimum required for a certain service?**
- Yes
- No

9. **Are you aware of the existence of technologies limiting the collection of personal data on the Internet (e.g. cookie filters)? Have you ever used any of them?**
- No, I have not heard about them
- Yes, I have heard about them, but I have never used them
- Yes, I have heard about them and I have already used them

10. **Age**
- Under 20
- 21-25
- 25-30
- 30-35
- Over 35

11. **Sex**
- Male
- Female

12. **Country**

Bibliography

Bolkestein, F., 2002. *Closing remarks at European Commission conference on "Data Protection"* [online]. EUROPA, European Union. Available from: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/02/439&format=HTML&aged=1&language=EN&guiLanguage=en [Accessed May 31, 2008].

Berte, K. et al., 2007. Advertising in Digital Media Environment (ADME): An Interdisciplinary Approach to a User-Centered Advertising Model for IDTV. *In:* Urban, A., Sapio, B. and Turk, T., eds. *Digital Television Revisited. Linking Users, Markets and Policies. Workshop proceedings*. Budapest, 123-131.

Brandau, G. (gbrandau@fedma.org), 07.07.2008. RE: Reminder. e-mail to A. Stankova (andreana_stankova@abv.bg).

Cate, F., 1997. *Privacy in the Information Age.* Washington, D.C.: Brookings Institution Press.

Ciocchetti, C., 2008a. *The Privacy Matrix* [online]. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1090423 [Accessed Feb 27, 2008].

Ciocchetti, C., 2008b. *Just Click Submit: the Collection, Dissemination and Tagging of Personally Identifying Information* [online]. Available from: http://ssrn.com/abstract=1090432 [Accessed Feb 27, 2008].

Council of Europe, 1981. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* [online]. Available from: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm [Accessed April 10, 2008].

EDPS, 2007. *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the Follow-up of the Work Programme for Better Implementation of the Data Protection Directive* [online]. Available from: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf [Accessed July 26, 2008].

EPIC, Privacy International, 2007. *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*. USA.

European Commission, 2001. *European Governance: A White Paper* [online]. Available from: http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0428en01.pdf [Accessed July 26, 2008].

European Commission, 2002. *Action Plan "Simplifying and Improving the Regulatory Environment"* [online]. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0278:FIN:EN:PDF [Accessed July 26, 2008].

European Commission, 2003. *First Report on the Implementation of the Data Protection Directive* [online]. Available from: http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm [Accessed Feb 27, 2008].

European Commission, 2006. *Self-Regulation in the EU Advertising Sector: A report of some discussion among Interested parties* [online]. Available from: http://ec.europa.eu/consumers/overview/report_advertising_en.pdf [Accessed July 23, 2008].

European Commission, 2007. *Communication from the Commission to the European Parliament and the Council on the Follow-Up of the Work Programme for Better Implementation of the Data Protection Directive* [online] Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:EN:PDF [Accessed April 10, 2008].

European Parliament, 1995. *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* [online]. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [Accessed Feb 27, 2008].

European Parliament, 2000. *Charter Of Fundamental Rights Of The European Union* [online]. Available from: http://www.europarl.europa.eu/charter/pdf/text_en.pdf [Accessed July 20, 2008].

European Parliament, 2002. *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* [online]. Available from: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=32002L0058&model=guichett&lg=en [Accessed July 20, 2008].

European Parliament, 2003. *International Agreement on Better Law-Making* [online]. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:321:0001:0005:EN:PDF [Accessed April 10, 2008].

Facebook, 2007. *Facebook Principles* [online]. Available from: http://www.facebook.com/policy.php [Accessed June 5, 2008].

FEDMA, 2003. *European Code of Practice for the Use of Personal Data in Direct Marketing* [online]. Available from: http://web3.custompublish.com/getfile.php/342991.1014.xacscqtseu/FEDMACodeEN.pdf?return=www.fedma.org [Accessed April 10, 2008].

FEDMA, 2004. *Articles of FEDMA* [online]. Available from: http://www.fedma.org/membership-policy.60464.en.html [Accessed July 23, 2008].

FEDMA, 2007a. *FEDMA Seminar on Direct and Interactive Marketing* [online] Available from: http://fedma.custompublish.com/fedma-seminar-on-direct-and-interactive-marketing.430247-74828.html [Accessed July 26, 2008].

FEDMA, 2007b. *European Code Practice for the Use of Personal Data in Direct Marketing On-line Annex*. Unpublished.

FEDMA, 2007c. *FEDMA Holds successful Data Protection workshop* [online] Available from: http://fedma.custompublish.com/fedma-holds-successful-data-protection-workshop.537103-74828.html [Accessed July 26, 2008].

FEDMA, 2008a. *Federation of European direct and interactive marketing - Your unique resource for pan-European direct and interactive marketing* [online]. Available from: http://www.fedma.org/ [Accessed July 20, 2008].

FEDMA, 2008b. *Public Seminar - Data Protection on the Internet (Google-DoubleClick and other Case Studies)* [online]. Available from: http://web3.custompublish.com/getfile.php/627466.1014.atxxcttrtx/FEDMA///'s+Discussion+Paper+for+European+Parliament+public+seminar+on+data+protection+on+the+Internet.pdf?return=fedma.custompublish.com [Accessed July 20, 2008].

Gasser, U., Haeusermann, D., 2007. *E-Compliance: Towards a Roadmap for Effective Risk Management* [online]. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=971848 [Accessed Feb 27, 2008].

Harker, D., 2003. Towards effective advertising self-regulation in Australia: the seven components. *Journal of Marketing Communications*, 9 (2), 93-111.

Just, N., Latzer, M., 2004. Self- and Co-Regulation in the Mediamatics Sector: European Community (EC) Strategies and Contributions towards a Transformed Statehood. *Knowledge, Technology & Policy,* 17 (2), 38-62.

Kafka, F., 1969. *The Trial*. New York: Random House.

Kang, J., Buchner, B., 2004. *Privacy in Atlantis* [online]. Harvard Journal of Law and Technology. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=626942 [Accessed April 10, 2008].

Kotler, P., 2000. *Marketing Management, Millenium Edition.* Custom Edition for University of Phoenix. Boston: Pearson Custom Publishing.

Newman, A., Bach, D., 2004. Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States. *Governance: An International Journal of Policy, Administration, and Institutions,* 17 (3), 387–413.

Noll, J., 2001. *The European Community's Legislation on e-commerce* [online]. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=288942 [Accessed Feb 27, 2008].

OECD, 1980. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [online]. Available from: http://www.oecd.org/document/18/0,3343,en_2649_201185_1815186_1_1_1_1,00.html [Accessed April 10, 2008].

Olson, M., 1993. The logic of collective action. *In:* J.J. Richardson, ed. *Pressure groups.* Oxford: Oxford University Press, 23-37.

Orwell, G., 1984. *1984*. Commemorative 1984 Edition, New York: The New American Library.

Popkostadinova, N., 2007. Da zhiveesh v staklen kub. (Living in a cube of glass) *Capital*, 27 December , [online]. Available from: http://www.capital.bg/show.php?storyid=410273, Брой 52, 27 декември 2007 [Accessed July 20, 2008].

PQ Media, 2008. *Alternative Media Forecast 2008-2012: Report Summary* [online]. Available from: http://www.pqmedia.com/execsummary/AMF08-Report-Summary.pdf [Accessed July 20, 2008]

Price, M., Verhulst, S., 2005. *Self-regulation and the Internet*. The Hague: Kluwer Law International.

Senden, L., 2005a. *Soft Law, Self-Regulation And Co-Regulation In European Law: Where Do They Meet?* [online]. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=943063 [Accessed March 30, 2008].

Senden, L., 2005b. *Soft Law and its Implications for Institutional Balance in the EC* [online]. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=991550 [Accessed June 16, 2008].

Solove, D., 2002. *Conceptualising Privacy* [online]. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103 [Accessed April 10, 2008].

Solove, D., 2004. *The Digital Person: Technology and Privacy in the Information Age.* New York University Press.

Solove, D., Hoofnagle, C., 2006. *A Model Regime of Privacy Protection (Version 3.0)* [online]. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=881294 [Accessed July 20, 2008].

Solove D., Rotenberg M., Schwartz, P., 2006. *Privacy, Information and Technology*. New York: Aspen Publishers.

Stone, B., 1988. *Successful Direct Marketing Methods*. Fourth Edition. Lincolnwood: NCT Business Books.

The Gallup Organization, 2008. *Data Protection in the European Union: Citizens' perceptions* [online]. Available from: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf [Accessed July 26, 2008].

Verrue, R., 1999. Electronic *Commerce in Europe: the present situation* [online]. Available from: http://ec.europa.eu/comm/information_society/speeches/verrue/ecommerce_en.html [Accessed May 26, 2008].

United Nations, 1948. *Universal Declaration of Human Rights* [online]. Available from: http://www.un.org/Overview/rights.html [Accessed April 10, 2008].

Wilson, G., 1990. *Interest groups.* Oxford: Basil Blackwell.

Working Party, 1998. *Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct* [online]. Available from: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp13_en.pdf [Accessed July 26, 2008].

Working Party, 2000. *Privacy on the Internet: An integrated EU Approach to On-line Data Protection* [online]. Available from: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf [Accessed July 26, 2008].

Working Party, 2003. *Opinion 3/ 2003 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing* [online]. Available from: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp77_en.pdf [Accessed July 26, 2008].

Working Party, 2008a. Assessment of the Article 29 Working Party to the Amended Version of the Online Marketing Annex to the Data Protection and Direct Marketing Code. Unpublished.

Working Party, 2008b. *Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)* [online]. Available from: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf [Accessed July 20, 2008]

Zarsky, T., 2006. *Online Privacy, Tailoring and Persuasion* [online]. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=946428#PaperDownload [Accessed July 20, 2008]