JOURNAL OF INFORMATION, LAW & TECHNOLOGY

Journal of Information, Law & Technology

The 'Credit Scoring Pandemic'[1] and the European Vaccine: Making Sense of EU Data Protection Legislation

Dr. Avv. Federico Ferretti
Lecturer in Law
Brunel Law School, Brunel University
fed.ferretti@libero.it or federico.ferretti@brunel.ac.uk

This is a **refereed article** published on 28 May 2009.

Citation: Ferretti, F., 'The Credit Scoring Pandemic and the European Vaccine: Making Sense of EU Data Protection Legislation', 2009(1) *Journal of Information, Law & Technology (JILT)*, <http://go.warwick.ac.uk/jilt/2009_1/ferretti>

Abstract

This article explores credit scoring systems as a tool used by the credit industry to evaluate consumers' credit applications and creditworthiness within the context of the EU. After an analysis of the technologies and techniques behind the scoring of individuals, it investigates the most relevant issues behind the reporting of consumer financial information, i.e. the prejudicial side of sharing people's reputation exacerbated by ever-advancing information technologies and the disrespect of the privacy of consumers. This is put in context with an analysis of the values that the right of informational privacy protects and the dangers that data protection legislation aims to prevent. Ultimately, this article aims at showing that a correct application of the existing EU data protection legislation should prevent, or at least repair, the flaws of the uses of credit scoring and concerns over the respect of established privacy rights.

Keywords

Credit Scoring, Data protection, Privacy and Information Technology.

1. Introduction

This work is concerned with the practice shared by the credit industry of scoring consumers to underwrite lending decisions. Lenders, in fact, access credit reference databases managed by third party providers (the so-called 'Credit Reference Agencies', or Credit Bureaus, hereinafter 'CRAs') in order to score consumers and evaluate their credit application and creditworthiness, as well as the profitability that may result from each application. Such scores are calculated on the information contained in credit reports, and they are drawn from the latest technologies in statistics and artificial intelligence. Significantly, at least in Europe, the reporting or scoring of consumer credit information is not mandated by law.

It is necessary to separate the type of organisations involved in consumer credit reporting and scoring activities from the type of credit reporting carried out in many EC countries by public organisations involved in the centralisation of financial information. The latter are information systems operated or controlled by the State through public institutions, usually central banks or other authorities engaged in the banking or financial supervision/regulation. Their function in the economy is to monitor the safety and soundness of the financial system as a whole, and they are involved in the prudential regulation that relates to it. As such, these databases must be consulted by law in the general interest, and no scoring of individuals occurs.

For the avoidance of doubts, this article is concerned with those organisations which operate outside the sphere of the State or other public institutions and do not have any public function but simply provide services to those financial intermediaries engaged in the provision of credit to their customers. Indeed, as this work intends to show, they raise different problems and legal issues that must be addressed separately.

Karen Gross (2005), looking at the phenomenon of credit scoring in the US, emphasises that although deep flaws exist in how these systems operate both to grant and price credit, there has been an expansion of their use to arenas beyond credit. This exacerbates the existing concerns about how these systems operate and multiply the opportunities for unfair treatment of entire segments of the population. For this reason, the author urges caution before an existing problem gets worse through its transposition into other arenas, warning other jurisdictions around the world to avoid the same wrongs of the US. Suggestively, credit scoring has been marked as the new ‘influenza’ that, ‘like the real flu, is spreading’ as a ‘flu pandemic’ (Gross, 2005, p.332).

Thus, the aim of this article is to understand consumer credit scoring and identify its flaws in the context of their original use. In particular, it focuses on the legal framework of the EU in order to assess if there are any ‘defences’ available for the Member States in order to avoid, or at least cure, the ‘influenza’. Therefore, it will concentrate precisely on the original use of credit scoring, making the assumption that, to the extent that remedies indeed exist in the law for the EU to tackle the original problem, these will solve any expanding use beyond its origins, restraining the pandemic.

2. Credit Scoring

Credit scoring may be described as a systematic method used by lenders for evaluating the credit risk of each credit applicant. This provides an analysis of the factors that have been predetermined to cause or affect the level of risk in lending. When used to assess consumers, it is essentially a way of recognising different groups in a population according to certain features, expressed by a combination of personal data and other non-personal information, and differentiating them on grounds of parameters and classifications set *a priori* from statistics for a predictive purpose. It is an analysis of customer behaviour having the objective to classify them in two or more groups based on a predictive outcome associated with each customer. The probability of given events (for example, a default in the repayment of a loan) is assumed to depend on a number of characteristics of the individuals (Fractal Analytics, 2003). The factors relevant for such a classification purpose are usually determined through an analysis of consumers' past payment history together with other descriptive information provided in the credit application form and other data from a number of different sources.

Traditionally, the decision to grant credit to an applicant has been taken using human judgement to assess the risk of default. Human judgement, as a decision-making tool, is indeed an essential element of every business in the commercial arena.

The development of credit scoring techniques is based on the assumption that ‘humans are not good at evaluating loan applications (Handzic et al., 2003, p.98). The scientific literature believes that the reasons for such poor judgemental capabilities of humans are said to be (i) the subjectivity and the large grey area where the decision is up to the officers (cases not immediately obvious for decision making), (ii) humans being prone to bias, for instance in presence of a physical or emotional condition which may affect the decision making process, (iii) personal acquaintances with applicants distorting the decision making process, (iv) humans considering the evidence sequentially rather than simultaneously, (v) the difficulty for humans of discovering useful relationships or patterns from data and the knowledge hidden in the same data (Bridges and Disney, 2001; Yobas and Crook, 2000; Glorfeld and Hardgrave, 1966; Bigus, 1996; Desay et al., 1997). Moreover, humans are costly and time consuming (Jensen, 1992; Diana, 2005; Orgler, 1978).

Nowadays lenders have substituted human judgement with credit scoring systems which give points to various pieces of information on the customer’s application form, such as age, job, income level, marital status, etc. as well as historical data taken from the credit records processed by CRAs. CRAs, that are private for-profit companies, collect a variety of financial information on individuals, producing a 'credit report' that contains details of the payment and credit history of an individual, his/her financial accounts and the way these have been managed, as well as other information of interest to the credit industry. By compiling databases of consumer financial data, they have evolved as organisations providing information sharing devices in the financial system in order to meet the problem of asymmetrical information between borrowers and lenders. By providing rapid access to standardised information on potential borrowers, they play a pivotal role as a borrower discipline device as consumers would know that a default in re-payment compromises their reputation with all the other potential lenders in the marketplace (Stiglitz and Weiss, 1981; Diamond, 1991; Berger and Udell, 1995; Jappelli and Pagano, 2002).

The practice of scoring customers has developed all over Europe to the point that it is widely accepted by lenders that it helps them to predict whether the applicant is an acceptable risk although no scoring system, even the better ones, may predict with certainty any individual repayment performance (Mester, 1997).

3. Data Mining

In technical terms, credit scoring models, or 'Scorecards', are mathematical algorithms or statistical programmes that determine the probable repayments of debts by consumers, assigning a score to an individual based on the information processed from a number of data sources and categorising credit applicants according to risk classes. They involve data mining techniques which include statistics, artificial intelligence, machine learning, and other fields aiming at getting knowledge from large databases (Liu, 2002).

Credit scoring is a classification issue, where the input characteristics are the answers to the application form questions and the result of a check with CRAs databases, and the output is the division between 'good' and 'bad' or something in the between: in short, lenders use data on previous applicants to determine the features that are useful in predicting whether an individual is or will be a 'good' or a 'bad' risk (Thomas, 2000). In such a process, also to avoid a selection bias, account has to be taken not only of the characteristics of borrowers who were granted credit but also of those who were denied it (Mester, 1997).

Scorecards are typically constructed making use of a diverse range of techniques. The most commonly used techniques for building scorecards rely on (i) 'linear probability models', (ii) 'logits', (iii) 'probits', and (iv) 'discriminant analysis' (Hand and Henley, 1997). Bridges and Disney offer a clarification of such techniques: 'the first three techniques use historical data on credit performance and the characteristics of the borrower to estimate the probability of default. These results are then used to calculate the predicted probability of default for each new applicant. Discriminant analysis differs in that instead of estimating a borrower's probability of default, it divides borrowers into high and low default-risk classes' (Bridges and Disney, 2001).

What seems to be the most used classification of types of systems in the literature is the one differentiating between judgmental/rules-based systems and statistical based systems. Judgmental/rules-based systems evaluate creditworthiness using rules or formulas based upon consumers' past credit experience. Statistical-based systems utilise statistical analysis to estimate the probability a customer will default. The main difference between the two systems is that in the latter the factors used and their weights are based on statistics while in the former on human judgement. Both involve an extensive use of historical personal data (Fensterstock, 2005; Diana, 2005).

A newer method of scoring is beginning to be used in the decision-making process. It is based on neural networks, consisting of the use of sophisticated technologies and artificial intelligence techniques applied to the modelling of the human brain, the idea of neurons as its building blocks, and the simulation of the way neurons work in the human brain (Bridges and Disney, 2001; Handzic et al., 2003; Yobas and Crook, 2000). Neural networks, consisting of layers of interconnected neurons, process inputs and produce outputs but do not require the specification of 'if-then rules' but they just need examples to create rules, also becoming able to learn and store associations. They are particularly good at pattern recognition in the personal data and in databases. This system is applied to historical personal data to find relationships between account characteristics and the probability of default (Jensen, 1992).

As noted, the most important feature of neural networks is their ability to learn. Just like human brains, neural networks can learn by samples and dynamically modify themselves to fit the data presented. Moreover, neural models are able to learn from distorted or incomplete sample data. The second most important feature besides learning is that of being capable of generalisation, which is intended as the neural network producing standardised output results for data inputs that were not encountered during training (Bridges and Disney, 2001; Handzic et al., 2003; Yobas and Crook, 2000).

4. Expanding Uses and the Ultimate Goal of Credit Scoring

Within the described technological framework, there are increasing trends in the use of scoring systems. Although they have traditionally been used to predict risk, they are also more and more used to assess affordability or the level of a person's indebtedness. In the words of a spokesman of a major multinational CRA, 'although a prospective borrower may have a range of existing credit facilities all of which are being paid on time, he/she may be so heavily committed that one more facility may result in that individual becoming over-indebted across his/her total borrowings' (Bradford, 2004, p. 11).

Even if the use of credit scoring is increasingly encouraged to prevent individuals' over-indebtedness in the thrust of a responsible lending policy throughout Europe, there is a recognised tension between the two which leads to contradiction. Responsible lending by the financial industry would require lenders to refrain to lend money to overcommitted consumers. Apart from the inherent conflict of interest faced by lenders, this would rather require a more individualised lending process avoiding any form of generalisation or classification (Ramsay, 2005).

Another recent trend practiced by most lenders is the one of scoring potential customers to price loans and calculate profits on the classification of individuals, based on the forecast of their future performance. For example, also high risk applicants may be profitable provided that a higher rate of interests is charged on top of the charges borrowers pay in case of default. In this respect, scoring systems assume some real correlations between risk and price, a circumstance likely to penalise vulnerable people (Gross, 2005).

In addition, the same lenders score their customers on a regular basis, thus ensuring that they are the first ones to contact the customers when an early delinquency sets in, not only to renegotiate the repayment but also to better secure the credit and limit exposure (Lund, 2004; Hand and Henley, 1997; Thomas, 2000; Baesens et al., 2003).

Finally, there are warnings of the spreading in the US of credit scoring individuals for insurability, employability, and tenancy purposes, where credit riskiness is becoming to be used as a proxy for other types of risks – i.e., insurance claims, trustworthiness at the workplace, payment of rent (Gross, 2005).

In short, the goal of credit scoring systems in the lending process is that of predicting the creditworthiness of consumers and the profitability of lenders over each one of them. It is now used for all consumer credit operations, in issuing credit cards and managing accounts, as well as in mortgage origination and securitisation operations of consumer loans. Although credit scoring was originally employed to seek to minimise the percentage of consumers who default, lenders are now using them to identify the customers who are most profitable and to maximise profits through risk based pricing according to their profile so obtained, blurring this all with direct marketing activities (Thomas, 2000). Indeed, classification and profiling to maximise profits, by mean of a score, are precisely what credit scoring systems do.

The search for commercial advantage and profitability pursued by using credit scoring represent certainly a legitimate business interest of lenders, though it is certainly not a right. When and to the extent that the use of technologies interferes with, and abuses of, the established rights of individuals, the underlying business interests that they enhance should be limited. In the situation at study, therefore, the question is to assess to what extent credit scoring systems hinder the rights of individuals and how the protection of these rights should be addressed to guarantee the evolution of a modern society based not simply on the idea of ever-increasing search for the maximisation of profits but rather on the respect of freedoms of individuals.

5. Trust and Reputation

Although credit scoring is something distinct from the provision of credit reports, there is a critical link between credit referencing and credit scoring. The latter, in fact, includes credit reports as one of its core elements. Indeed, credit scoring systems in the credit granting process would not exist without CRAs databases.

As noted, the systems at study originated from, and respond to, an asserted need to minimise risk in contractual relationships involving credit, i.e., the advancement of money, services, or goods that will be repaid with interests at a later stage with a profit for the lender.

Accordingly, trust is a precondition of many social relations, especially, though not exclusively, those involving risks. In this context, trust can be intended as ‘one's expectation that another will act in a way that is advantageous to oneself, supplemented by one's ability to act upon such expectation, accepting the corresponding risks’ (Sartor, 2006). Certainly, many other definitions of trust exist in the literature, but all make reference to a component of rational expectations by a party on the counterparty's behaviour.[2] Arguably, without trust there could not be any active social relationship, including business and the underlying contracts that are one expression of the many social relations that exist. Trust, therefore, presupposes a decision to expose oneself in a relationship involving others that inevitably contains a risk towards the performance of the counterpart. In commercial relations it is well known that risk is part of the business itself and the taking of the risk is compensated by profit or penalised by failure. In this regard, every business involves risks because risk is entrenched in the nature of business. Trust and risk are necessary preconditions for business to exist.

Then, on those occasions where trust is misplaced or it has been breached, the law provides an alternative to the spontaneous cooperation, or correct performance, of the counterpart (the trustee). The law, therefore, not only provides a means for repairing the failure of trust but also provides a reason for relying upon others and contributing to the rational formation of trust in those social relations that it covers. At the same time, the law provides a disciplinary mechanism for the trustee who knows that there are in place tools accepted by the large society for the enforcement of his/her obligations and the punishment for having breached someone else's trust (Sartor, 2006).

Credit references, by contrast, have developed as informal social accountability mechanisms that contribute to the formation of trust and serve as disciplinary devices for the borrower (Klein, 2001). As such, they have self-established as an alternative to the law in the formation of trust. In this way, they replace the law which remains a remedy once trust has been breached.

Although judicial procedures have the undisputable advantage of the certainty and rule of law, they are also lengthy, have an uncertain outcome, and could be expensive on those occasions where the debt is unrecoverable. Therefore, in the name of the minimisation of risk and the consequential maximisation of profits for lenders, CRAs bring into play the reputation of consumers to favour the formation of trust, or supplement it.

As social accountability mechanisms, they create and disseminate reputations that give rise to rewards for standardised good behaviour, and punishments for standardised bad behaviour (Klein, 2001). In this way, however, it could be maintained that from social accountability mechanisms they also become social control mechanisms and impose a set discipline via surveillance.

Once more, Sartor provides a useful definition of reputation, considered as ‘the evaluative opinion that people (the public in general or certain sections of it) have on a particular person, and the social mechanism which produces such an opinion’ (Sartor, 2006). In the logics of the credit referencing business, as in every section of a society, reputation results from shared beliefs. A meaning, or a score, is given to the various pieces of personal information and persons (lenders) form opinions concerning other persons (borrowers), sometimes on the basis of personal experiences but many times on the basis of the experiences of others. Such experiences are adopted by others, they are further conveyed through CRAs, and they are subjected to a scoring (Sartor, 2006).[3]

As a result, reputation provides a cognitive basis for people to trust others based on the positive or negative experience or opinion of an external party. This confers a personal evaluation of a fact that has not gone through that formal mechanism of declaratory action that is a judicial proceeding and that confers to the judgement force of law for that particular situation. From a different angle, reputation puts a person in a position towards others that can be alternatively that of reliance by others, resulting in the invitation to enter social relationships (inclusion), or that of distrust by those same persons resulting in refusal to enter those relations (exclusion).

Problematically, reputation can be associated with, and inevitably becomes, identity: someone is not his/her real self but rather becomes the result of the judgement of his/her individual achievements and verification of corresponding credentials by others. It becomes a fact when it becomes a story shared by many, as this gives authority to the story. Someone is what others say, not what he/she truly is (Sandage, 2005, ch. 4-6). On its negative side, a bad reputation (for example, failure) becomes one person's achieved identity and, in the case of credit referencing, a market commodity for the risk-management of trust. Also, a negative reputation can be easily related to prejudice and stigmatisation: negative conclusions are drawn from certain reported information about, or feature of a person. Choices are then made accordingly, but these may damage that person further. In turn, this information, which is built on previous information, spreads in society contributing to consolidate such a reputation in a spill-over fashion. In this way, not only reputation fails as a cognitive mechanism, but it is also intrusive and bears with it issues of social exclusion and discrimination based on one's achieved identity, precisely what Sandage calls the achieved identity of a ‘born loser’ (Sandage, 2005).

Certainly, reputation is a natural and unavoidable component of the dialectical interaction between the individual and the community where he/she lives. However, the evolution and use of sophisticated information technologies exacerbate and contribute to the dissemination and diffusion of reputation, therefore marking more neatly and spreading comprehensively, if not completely, on the marketplace such a reputation, i.e. the inclusion or exclusion of persons in/from social relationships beyond the community where they live, together with the consequences that follow expressed above. Technologies, thus, may become the arbiters of achieved identities, standardising, sorting, monitoring, and labelling people. The meaning of reality as an explanation of the physical world and as an explanation of individual identity gets distorted through the filter of data mining systems, so that growing areas of personal existence are invested in rival achieved realities.

The problem is that the informal social surveillance mechanism operated by credit referencing and then scoring lacks the certainty of the law. As described by Klein, who writes in defence of credit reporting, it generates reputations and ‘is akin to gossip in that it gathers, interprets, formats, stores, retrieves, and transmits information’ (Klein, 2001, p.343). This reputation, however, crucially misses the authority of judicial recognition, i.e. the rule of law. Indeed, such a phenomenon has been at the centre of the recent attention of the Article 29 Working Party on Data Protection set up by EC Directive 95/46/EC. According to the data protection authorities, entering individuals onto databases in which they are identified in connection with a specific situation or facts, i.e., on reputation, represents an intrusive phenomenon known as 'blacklist', and defined as:

> ‘the collection and dissemination of specific information relating to a specific group of persons, which is compiled to specific criteria according to the kind of blacklist in question, which generally implies adverse and prejudicial effects for the individuals included thereon and which may discriminate against a group of people by barring them access to a specific service or harming their reputation’.[4]

The insertion in a database of a group of people based on their reputation is precisely what CRAs do. The assessment of consumers' creditworthiness is based on past financial behaviour, and information about such a past has a meaning that forms one's reputation within the credit sector and that is reflected in a final score. Obviously, CRAs would reject that they make blacklists or that they provide opinions, one reason being that they provide cold data that lenders independently evaluate in making decisions, and that credit files and scoring systems are also formed including positive information. This assertion, however, lacks legal basis and credibility. Each piece of information - a single datum - has a meaning, it is read in conjunction with all other reported data, and it eventually contributes to generate a score. Every credit file and score undoubtedly pictures and reports a consumer's behaviour, forming a reputation. Even if the intention may not be that of stigmatising a group of people according to certain features (expressed by the data), their widespread use has taken the same effect and result. The use of positive information, moreover, not only fails to stem the above concerns but, if any, exacerbates them by way of positive discrimination: anyone who has no positive information in his/her credit file, or else elements contributing to a positive reputation, has a bad or at least suspect reputation. This includes those who are not at all present in the database, thus in theory should not have a reputation but get (a suspicious) one for not having a credit history.[5]

The use of credit information sharing and scoring systems represent already the current practice in consumer credit and banking relationships in every European country. In many ways, in fact, the development of the credit industry has reflected the intuitions developed in the economic theoretical literature on information sharing arrangements and scoring, with the addition of the industry's substantial investments in technologies that were not in place when data sharing was initially considered. At the same time, European legislators have not responded with the same speed to the new concerns brought by such mechanisms, leaving them under the regulatory umbrella of general principles of existing legislation.

Given the type and number of personal data involved, legislators across Europe mainly need to rely on at least one law that have a significant impact on consumer credit referencing and scoring activities, namely the EU Data Protection Directive as transposed in national law.[6] Yet, reliance based upon reputation through data sharing, the formation of blacklists, and scoring seem *prima facie* to conflict with the European legal framework of data protection as the omni-comprehensive legislation regulating the sector.

How is the formation and diffusion of reputation impaired by data protection? May a system that relies on the creation and dissemination of the reputation of consumers and their profiling ever be lawful vis-à-vis a law that protects the processing of their personal data? To answer to this set of questions, that entail an intrinsic conflict and fundamental tension between the right to privacy of an individual living in a society and his/her interaction within such a community, it seems inevitable to make an evaluation of the reasons behind both the enactment of data protection laws and the interest of lenders. The latter has already been examined earlier in this work. The next section, therefore, will concentrate on the significance for European countries of protecting consumers' personal data and the value placed upon such a notion.

6. The importance of data protection and the reasons for EC legislation

In collecting, processing, and disseminating the personal data of consumers in credit operations, CRAs must, like any other European data controllers comply with data protection legislation. Before turning to the relevant provisions applicable to credit scoring, however, it is necessary to put such complex technological mechanisms in context with the rationale of data protection law, recalling the origins and evolution of such a distinctly European innovative piece of legislation.

a) The concept of privacy

The concept of privacy can have a multitude of meanings to different people in different countries at different times and has been the subject of much scholarly debate. There are so many wide differences of views as to its significance, depending on the context and environment in which they are taken, that by general consensus the concept of privacy is seen as still under construction or always in transition, in any event almost impossible to define (EPIC and Privacy International, 2002; Jay and Hamilton, 2003).

Nonetheless, the recognition of the idea of privacy has a long tradition and is deeply rooted in history. However, it was only in the 19th century that the concept of privacy was developed as an independent legal value, when Professors Brandeis and Warren in *The Right to Privacy* identified such a right as a tort action, defining it as ‘the right to be left alone’ (Warren and Brandeis, 1890). Since that publication, it has been widely accepted that in its most general accession, privacy protection is seen as a legal way of drawing a line at how far society or other individual subjects may intrude into a person's own affairs. It entails that such a person should be left able to conduct his/her personal legitimate affairs relatively free from unwanted intrusions. As such, privacy is unquestionably considered to be an expression of freedom and dignity of the individual.[7] Within such a broad notion, then, privacy typically encompasses the following four separate but related aspects:

(i) Information privacy or privacy as self-determination over one's personal data. This aspect relates to the data subject's power of decision over his/her own information (i.e. control over his/her personal data);

(ii) Bodily privacy. It concerns the protection of one's physical self against invasive intrusions or procedures in his/her body (for example, genetic or blood tests, cavity searches, etc.);

(iii) Privacy of communications. This covers the security and privacy/confidentiality of all forms of communications (for example, mail, telephone, electronic mail, etc.);

(iv) Territorial privacy. It refers to the individual's intimate space setting the limits from unwanted intrusions (home, workplace, etc.) (EPIC and Privacy International, 2002).

b) Directive 95/46/EC

Data protection is a distinctive European innovation in law that over the last few years has been gaining acceptance and has been emulated over the world outside the EC. The atrocities of Nazism, fascism, and communism pushed Western nations into attaching great importance to the right to privacy, as it had been demonstrated how easily it could be violated, and the extreme consequences of such violations. Privacy was soon elevated as a human right and its standard at international level was enshrined in the 1948 Universal Declaration of Human Rights and later, at European level, incorporated in the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms.

Certainly, the horrors of recent European history and the international conventions that followed played an important role in the development of privacy laws across Europe and, ultimately, in the adoption of Directive 95/46/EC. Two other factors, however, proved decisive for the enactment of the latter piece of legislation: (i) the progressive development in computers and information technologies, i.e. ultimately in the information society, together with the dangers that this could represent for individuals; and (ii) the need for the free movement of personal data within the Community to solve trade disputes arising from separate national privacy regimes, hence the harmonisation of data protection laws of the Member States.[8]

In the end, as a result, the real aims and scope of Directive 95/46/EC were (i) the protection of fundamental rights and freedoms of Europeans, and (ii) the achievement of the Internal Market. Both objectives were equally important, though in mere legal terms the existence of the Directive, and the jurisdiction of the EC rather than the national ones, rested on Internal Market grounds, having its legal basis in Article 100a (now Article 95) of the EC Treaty. However, the recent proclamation of the Charter of Fundamental Rights of the European Union, that in its Article 8 incorporates the right to data protection, has given added political emphasis to the dimension of the protection of the fundamental rights of individuals contained in Directive 95/46/EC. Certainly, one cannot overlook that at present the exact nature of such a solemn proclamation is still uncertain. However, the recognition of those fundamental rights made by the Member States and the EC institutions provides an indubitable indication of their importance, a source of inspiration, and a valuable point of reference for all the actors involved in the EC legislative, administrative, and judicial process (thus transcending its mere declaratory character). Significantly, also, the Charter is embedded in the EU Reform Treaty substituting the Constitutional Treaty, which means that in future data protection will also enjoy added legal value once the Reform Treaty will be ratified by the Member States, thus giving it recognition at the highest level of binding legislation in the EU.[9] Indeed, to reach its two main stated goals, the result of Directive 95/46/EC was not the protection of privacy in its broad significance but the protection of personal data, that is to say solely one specific aspect of privacy protection: information privacy. The Directive, in fact, is about the right of informational self-determination of the individual, a right which - as said - is related, but not identical, to the wider right to privacy.

c) Data protection as a civil liberty

In a broad sense, informational privacy is a right of the personality of the human being, an individual condition of life characterised by exclusion from unwanted knowledge of his/her personal information from outsiders, i.e. exclusion from publicity. More specifically, though, the basic concept of informational self-determination entails that an individual should have control over data generated about him/her, that there should be certain rules about how information is processed, and that data processing activities by data controllers should be as transparent as possible.

From this perspective, someone's informational privacy can be infringed by means of the acquisition of personal information by outsiders contrary to the determination of that concerned individual, insofar as such individual is identified or identifiable. This can take place in two ways that is through intrusion and/or disclosure. The former occurrence happens through the illegitimate collection and storage of personal data by a third party contrary to the data subject's determination. Infringement through disclosure, by contrast, entails that a third party communicates illegitimately to other third parties personal data, once again contrary to the data subject's determination. Certainly, it goes without saying that the communicating party may hold such information illegitimately in first place, in which case there is a double infringement or as many infringements depending on the spill-over communication of data (data dissemination). For infringements to occur and liability to be established, it is sufficient that the simple illegitimate processing (collection, storage, or communication) of personal data by a third party, its intent - or knowledge and/or will to perpetrate the violation - being irrelevant.

Each one of these basic principles is reflected in the provisions of Directive 95/46/EC, such as those that require that data processing must be done for legitimate and precise purposes which have to be previously notified to the concerned individual; or, again, those requiring that there should be a valid legal basis for the data processing, such as consent of the data subject, another overriding right, or a legal obligation.

d) Data protection and technologies

Informational self-determination seems particularly important today in the era of the so-called information society characterised by ever-evolving technological innovations, as also made clear by Recital (4) of Directive 95/46/EC in recognising the frequent recourse in the Community to the processing of personal data in the various spheres of economic and social activity 'whereas the progress made in information technology is making the processing and exchange of such data considerably easier'.[10]

In this context, data protection legislation in general - and Directive 95/46/EC in particular - is a legal tool aimed at the recognition of fundamental rights of the individual and awareness that their protection could represent an obstacle for market integration unless there is convergence among the Member States. Hence, contrary to the isolated view expressed by some commentators, it is far from being a measure reflecting what has been defined as ‘the fear of the democracies of the European Union that information technology might be used in the future to subjugate people to private-sector dictators’ (MacDonald, 2000, p.55).[11]

Indeed, there is a considerable amount of literature available about the perils of an indiscriminate use of information technologies in today's information society. Just to give few examples, it is well known that technologies have the potential capability of aggregating an enormous amount of data in a short time, manipulating, storing, retaining, and disseminating them as quickly to an indefinite number of third parties that may access them from many different points. The uses of various data mining techniques discussed above, including artificial intelligence and neural networks, and what they can potentially do, exemplify the problem. Then, data may be inaccurate, outdated, out of context, expressed in an unintelligible form, and so on. Consequently, they make it possible to follow an individual’s information trail step by step, manipulate his/her economic decisions, profile and/or categorise people, discriminate them, impede forgetfulness (the possibility to forget as well as being forgotten), enable people to change and/or progress, infringe (if not stele) their identities, create reputations, etc.[12] In short, they have a clear potential to influence dramatically the lives of people and this provides an exceptional power in the hands of those who use them.

Put it in simple terms, that is the reason why data protection is about liberty, intimacy, and dignity thus constituting an important legislative tool to protect those fundamental legal values of a modern democratic order. This is also why data protection, as an essential part of the right to privacy, is generally accepted and construed as a human right - at least in Europe.[13]

It is a law that has the objective to apply to the public and the private sector alike. As both governments and business are in a dominant position vis-à-vis the individual, their use of power - dictated by whatever reason, may it be political or simply by the search for profitability - could easily result in the abuse of such power and/or dominant position, thus penalising the individual in the same manner as described in the examples provided above. By applying to both the state and the private sector, the law addresses the issue whether data protection is or ought to be a person-to-person or a person-to-state matter. This, in many ways, disturbs the North Americans' approach to data protection but is along the lines of the European model of the welfare state and the idea of the social market. In that perception, it reflects the EC view about the relationship between Member States and their citizens, as well as the relationship among the latter. This is where the European and the American views over privacy have a major clash. In the broadest terms, in fact, in the US the private sector remains comparatively free of regulation as it is not considered a danger to individuals and their human rights in the sense that governments are (in terms of expansion, surveillance and deprivation of people’s liberties). This reflects a greater distrust of government by North Americans as compared with a less suspicious view of big or small businesses alike. Similarly, in economic terms, restrictions on the private sector are deemed to be counterproductive because by reducing the free flow of information consumers would lose favourable new products and/or better prices. In summary, the US favours a liberal understanding and approach towards the collection and dissemination of personal information by the business community as long as it does not harm others, a vision according to which the general economic good prevails (Jay and Hamilton, 2003; MacDonald, 2000; Singleton, 2000).

What is important to highlight here is the value placed over data protection by the EC and the reasons for its innovative legislative approach, albeit widely criticised by its detractors. In this regard, the EC acceptance of data protection as both a person-to-person and a person-to-state concern denotes a circumstance that exemplifies the centrality of the individual and his/her right to freedom vis-à-vis third parties notwithstanding who they are, may they be governments, the business sector, or other individuals. It intends to exemplify not only an aspect of individual self-determinism but also the individual's right to exist in, or be accepted by the community where he/she expresses his/her own personality (data protection as a safeguard of social relationships).[14]

Such centrality, of course, has exceptions mainly owing to the respect of prevailing conflicting rights of others, including the public or general good. In fact, the right to data protection is not absolute, insofar as the justified interest of others outweighs the interest of the individual concerned. Accordingly, this happens in those cases where an absolute right prevails over a qualified right such as that to privacy, or two or more qualified rights are in opposition and the judiciary has to take them all into account and weight the one versus the other in the concrete case. So, for example, despite the extent to which this could be criticised, the Directive expressly provides that it does not apply to the processing of data in the course of the so-called 'third pillar', that is a number of state activities such as those falling outside the scope of Community law like Title V (PESC) and VI (JAI) of the Treaty, public safety, defence, State security, and the activities of the State in criminal law matters.[15] Equally, Article 7 (b-f) and Article 8(2) of the Directive are clauses designed for the balancing of interests establishing that personal data may legitimately be processed by certain subjects for certain purposes without the consent of the person concerned.

7. The rule of law

One of the main criticisms of data protection legislation is that it is not adequate for a knowledge-based economy: most of the time the new economy and technological developments may bring advantages and gains to consumers and industries alike that the current design of the law is incapable of exploiting. The so-called 'data explosion' of modern economies inevitably raises the question whether data protection could ever cope with the challenges brought by progress. Ultimately, this is believed to be the reason why the law need to be brought in line and up-to-date with new concepts, processes, and products. It is not a novelty, in fact, that the EC is often said to be facing the paradox to find a balance between the need to protect the fundamental rights of consumers on the one side, and foster the Internal Market in the context of the benefits of the technological era on the other side.[16] Unfortunately, the constant development of the information society and the continuous growth of, and reliance upon the knowledge-based economy make it difficult for legislation to draw alongside new processes. It really seems that as soon as it is enacted the law is already obsolete or, as one commentator has put it, 'it's a race the regulator will never win' (Sousa De Jesus, 2004, p. 27).

In this way, data protection legislation is constantly tested by new technological challenges forcing EC policy to take into account on the one hand, progress and economic growth, and on the other hand, new threats that could seriously affect its citizens. As openly admitted by the Council of Europe, experience has demonstrated that the principles and regulations on data protection cannot regulate every situation in which personal data are collected in different sectors.[17] In business, this phenomenon seems exacerbated by the development of what has been called the 'risk and instant society', epitomised by the development of highly technological risk or knowledge management tools, such as consumer credit reporting and risk scoring systems, designed to make instant decisions in order to provide instant services to customers.

Nevertheless, in each sector - including in the 'risk and instant society' in which consumer credit scoring takes part - and whatever technology is used, personal data must be collected, processed, and communicated to third parties in line and accordance with the principles and the provisions of the positive law, notwithstanding any individual evaluations as to its adequacy to regulate a given situation. After that, if the law proves inadequate to suit such a situation and the latter is one that either is necessary for the larger society or outweighs the interests thereby protected, then there may be ground for amendments in the law or alternative regulatory instruments which comply with the new legislative framework. However, until that moment (if ever), legal certainty and respect for the rule of law require compliance with the existing regime in accordance with its underlying principles. Consequently, any infringement that may occur should be treated as an unlawful interference with a legally protected personality interest.

8. The Law

As noted, the Directive serves the double purpose of both ensuring the free movement of personal data in the internal market and guaranteeing a high level of protection for data subjects. It establishes a minimum level of harmonisation, setting out a high level of normative protection with the result that the Member States cannot go beyond nor fall short of these minimum standards. The scope of the Directive, which applies to any operations performed upon personal data (data processing) is to provide for good data management practices on the part of those entities that determine the purposes and means of the processing of personal data (data controllers- Article 2d). It contemplates a sequence of general rules on the fairness and lawfulness of the processing of personal data, where consideration should be given to the consequences of the processing to the interests of the data subjects and the respect of other existing laws (Article 6a) (Carey, 2004). The principal ones include the following obligations:

- to inform in an intelligible form data subjects about the identity of the data controller(s) and the use, purpose and recipients of personal data (Articles 10 and 11) so that data subjects do not lose control over them;
- to process personal data only upon obtaining the unambiguous freely given specific consent of data subjects after having informed him/her of the processing of the data (Article 2h and 7a) or without consent if the processing is necessary for the performance of a contract (Article 7b), compliance with a legal obligation of the data controller (Article 7c), to protect a vital interest of the data subject (Article 7d), or for the performance of a task carried out in the public interest or in the exercise of a public authority (Article 7e);
- to process personal data only for specified, explicit and legitimate purposes (Article 6b) in order to limit data controllers in further uses of personal data and for the purpose for which they were collected;
- to use personal data that are adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed (Article 6c);
- to process accurate and up-to-date personal data, taking any reasonable step to ensure the rectification or erasure of inaccurate data (Article 6d);
- to keep the personal data in a form that permits identification of data subjects for no longer than necessary (Article 6e) in relation with the purpose for which they were processed and depending on the nature and type of data in consideration;
- to guarantee the security of the data against accidental, unauthorised access, or manipulation;
- to provide notification to the national supervisory authority before carrying out all or certain types of data processing operations (Article 17).

Prima facie, it looks that the Directive contains a specific provision for credit scoring. Article 15 on automated individual decisions, provides that in certain cases, including expressly that of the evaluation of a person's creditworthiness, data subjects have the right not to be subject to a decision based solely on the automatic processing of data.[18] However, Member States are given the possibility to provide that a person may be subjected to an automated decision as long as the decision:

> 'is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract *(...) has been satisfied* or that there are suitable measures to safeguard his *legitimate interests*, such as arrangements allowing him to put his point of view' (emphasis added).[19]

Alternatively, Member States may allow automated decision making if this is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.[20] In the absence of this type of laws, the first limb of the provision applies. Interestingly, the key terms *'satisfied'* and *'legitimate interests'* have not been specified and leave some uncertainty, especially if one considers that the right to informational privacy should be satisfied in the first place. It should be recalled, however, that credit scoring is built on consumer credit reporting. Before the application of Article 15, therefore, the data that are used to generate the score (a new personal datum allowing the automated decision-making) must be processed according to the other provisions of Directive 95/46/EC.

Indeed, whether CRAs activities truly comply with the law is problematic. There are critical concerns about the necessity, adequacy, and relevance of the type of data involved and the foundations, or assumptions, upon which consumer credit reporting is based to determine the predictability of individual human behaviours and/or the real financial capability of borrowers. In particular, many doubts arise as far as the legal compliance of information to be given to data subjects is concerned (Articles 10 and 11 of the Directive). The general objectives of transparency and informational self-determination set by the Directive seem seriously compromised by the amount and intelligibility of information that should be provided to individuals, the type and number of personal data processed by CRAs, the indefinite number of actors involved in a spill-over data dissemination, and the secondary uses of the same data.

As far as all the other requirements set by the Directive are concerned (i.e. the processing purposes, the adequacy and relevance of the data, accuracy, the data retention period), in the end the whole system seems to rely predominantly on the consent of the data subjects. This is so because in the absence of the universal acceptance of the assumptions upon which consumer credit referencing is based (i.e. past behaviour as predictive of future behaviour and the type of data to determine it), CRAs need to rely on the informed consent of data subjects unambiguously agreeing to all the 'rules of the game' set by the credit industry unilaterally. Consent, as conceived by the law, is a key element that permits the processing of personal data by data controllers that would otherwise be forbidden. When consent is validly provided by a data subject, this releases data controllers from the restrictions provided by the law in a fashion that has been described as an 'opt-in' system, i.e. the processing becomes lawful from the moment such consent is unambiguously expressed.

This issue is even more important in a system that is voluntary, as there is not any necessary requirement, either legal or natural, to justify the communication and sharing of personal data for the performance of a contract that, after all, is the core of the business of lending. Lending money in exchange of a profit (the interests on money lending) is perfectly possible and most probably lucrative even without the intervention of CRAs. At the most, data sharing is useful, in the same manner as using personal data for marketing purposes is useful. When consumers interact with business entities, however, the latter do not necessarily have to disseminate the data for marketing reasons; no matter how useful this may be (it is unquestionable that in business terms marketing is a very important activity). Indeed, the processing of data for marketing purposes should be kept separate from the processing of data for the purposes for which they were originally collected. This voluntary aspect about marketing is very well accepted by the business community and current legal practice. Consumer credit data sharing should not be treated differently. Certainly, lenders have a legitimate interest in wanting to know whether credit applicants are, in their own terms, creditworthy. After all, they have a legitimate interest in profitability. At the same time, though, consumers have not only a legitimate interest but indeed a right in the respect of their informational privacy, and the law recognises and protects that.

This view is reinforced by practice, where CRAs and lenders rely on consent for a lawful processing of consumers data. But according to the law, such consent must be informed, unequivocal, specific, and given freely. Crucially, more than one instance of consent should be required because it would otherwise create a problem of absence of specificity. In fact, it would be a violation of the information privacy principles to ask consumers to sign authorisations, unlimited in subject matter, essentially purporting to give permission to data controllers to process any personal data that they unilaterally decide to be relevant and disclose that information for expanding purposes to any person. By contrast, one of the primary concerns of the Directive is to ensure that data subject consent specifically to all uses of the data is processed for. A processing based on consent cannot be regarded to be lawful if sought for general or vague aims or if the data subject has no possibility of knowing the recipients of his/her data.[21] Importantly, the above instances of consent should be separate from the consent which a customer gives for the processing of his/her data for the specific purposes of the credit relationship with the lender at stake. Another fundamental feature is that, as a general rule, each instance of consent should be the free choice of the individual. Arguably, in fact, in data protection terms, consent would be meaningless if people have no option but to consent in order to obtain a benefit or a service that could be nonetheless provided.

It seems the case, however, that in the credit reporting process consumers do not have much choice if they do not want to be refused credit. The consumer’s consent with regard to the searches to be carried out in the CRAs’ databases, for example, seems to be viewed either mandatory or assumed. Lenders say that the lack of such consent would impede them from taking the credit application any further. Moreover, lenders make it a condition in the same instance of consent or in the credit contract that at a later stage they have the right to pass the information concerning such specific credit line to CRAs, which in turn will have the right to disseminate the same to their client members, such condition seeming to be non-negotiable. In the absence of alternative contracts with different lenders offering similar credit terms (i.e. mainstream lenders) which do not contain the objectionable clause it may be reasonably suggested that consumers have no option but to accept to be included in credit reference databases (see Howells, 1995 for an example of terms deemed to be considered unfair in the absence of alternatives).

It is vital to stress once more that the expression of will in order to be regarded as having been given voluntarily, must refer explicitly to the processing of personal data, and not to the consent to conclude the credit contract. This would be already a sufficient reason to maintain that the refusal by a data subject to permit an amount of processing of personal data that is not necessary for the provision of a service that he/she requires should not mean that he/she is failing to consent to that service. A typical example is that of commercial marketing: no one denies that it is an important economic activity that would increase the profitability of an industry, this latter circumstance possibly being reflected also in an economic advantage for consumers. It is well accepted in data protection, however, that data controllers may not obtain the giving of the consent to process the data for such a purpose upon the understanding that the goods or services may not otherwise be purchased or obtained. According to the Directive, and read in conjunction with the proportionality principle, such a practice to obtain consent would lack its freely given element (see, for example, Kuner, 2007, ch. 5j; Jay 2007 ch. 12, 22). Finally, it has to be taken into account that the so-called 'mainstream lenders' are part of a network system, thus leaving no live option to consumers if they do not want to be refused credit. Or in those few European jurisdictions where money lending is not considered usury for rates above a certain threshold set by the law (as opposed to those Member States that punish such a practice in criminal law, leaving little or no space for lawful subprime lenders) consumers are left with the alternative option of recourse or resorting to subprime lenders, overpaying for the service.

This problem is well synthesised by Howells in his analysis of the determination of the fairness of clauses requiring consent for disclosing positive data: 'such a term may be considered unfair if consumers have no option but to accept the term if they desire a particular form of credit and yet be acceptable if other creditors offer them similar credit whilst not requiring such consent (Howells, 1995, p. 353). In the end, therefore, as has been noted for other areas of law, consent might be formally free in the sense that there is not a single or traditional method of forcing individuals into a transaction by commercial organisations, but if the costs of not consenting are considerable in relation to the situation at stake, and there are no live options, then consent can be said not to be materially free (Leader, 2006; Agre, 1997).

There is another important aspect of consent. As construed by the data protection legislation, consent is normally a unilateral act, and therefore it is inherent in its nature that it can be withdrawn by the data subject at any time.[22] The more, thus, consent may be withdrawn if the data processing is not necessary for the service provided or it may be denied for a further processing that is compatible, but still different, from the original purpose of the processing. Once the assessment of the creditworthiness has tested positive and credit has been granted to a consumer, there would be no necessary reason for the communication of his/her data to CRAs, hence there would be no reason to impede the concerned individual's right to revoke his/her consent to the subsequent processing.

However, consent may not be withdrawn by a data subject, at least for a certain lapse of time, if it has been given under contractual arrangements which limit its withdrawal. In legal terms, such an obligation seems once more incorporated in the standard terms of consumer credit agreements, leaving no option to data subjects to exercise the right of withdrawal. All the above difficulties would probably be acceptable if consumer credit reporting were a necessary step of the credit granting process or a processing in the public interest. It is useful to recall that for the processing of data to be considered lawful under these latter circumstances it must be certain that the interest at stake is indeed a legitimate one recognised and protected by law. But the assessment of the creditworthiness of consumers via CRAs is factually not and, at any rate, the consent of the data subject would not even be a necessary requirement of the law.

Instead, as in the case of data processing for marketing purposes, an attentive application of the law should lead to a different scenario where consumers are left the choice to be included or excluded from CRAs databases. At the same time, however, the freedom that must be left to people to decide upon their participation in the system leads to a conflicting reflection: a CRA database comprised only of individuals who voluntarily accept the inclusion of their data in it, who could furthermore withdraw at any time their consent for the processing, would have no reason to exist as it could not even address the rationale and objective of the system itself. In all likelihood, those who eventually decide to be excluded from CRAs databases or withdraw their consent every time a negative piece of information is created would be largely, though not exclusively, precisely those customers that a credit reporting system is designed to identify. Indeed, a database designed to be incomplete would be helpless to address any need of the credit industry in the first place. Paradoxically, therefore, as the system stands it seems that:

(i) the essential option that on the one hand must be offered to consumers by law to accept or decline inclusion in the system, and

(ii) the rationale and scope of consumer credit reporting on the other hand,

are incompatible elements that create a vicious circle. Either the industry violates the law abusing consumers' freedom to provide consent, or it abides to the positive law but feeds a system that is ineffective and has no reason to exist. In brief, the problem with credit referencing, and then scoring, is that consumers are not presented with a real choice, and if the choice were given, this would be incompatible with the logic of the reporting system itself. But the law must be respected.

9. Conclusions

When balancing the conflicting interest of lenders with the rights conferred by the data protection legislation, it could be reasonably argued that the right of informational self-determination of individuals in the modern society cannot necessarily be sacrificed for the interest of lenders of minimising risk in the name of better business. Obviously, the protection of creditors’ rights is important. But the legal tools to achieve this are already in place in the positive law. If a debtor fails to comply with his/her contractual obligations, the law recognises the rights of creditors to recover the debt and it offers the tools to satisfy the creditor’s rights. It is important to stress, however, that credit scoring is about the minimisation of business risk and increased profitability, not the rights of creditors. At the least, it can be considered as an instrument for the economic welfare of society as a whole, but this circumstance is not supported by evidence of a link of cause and effect and, in addition, it lacks empiricism.

The law could punish or forgive a failing debtor, but credit scoring is about predicting failure beforehand. It does not satisfy any right of the creditor. It is a risk-management tool for the profitability of lenders, it is not a right. In fact, there is no legal right to maximise profits, especially if obtained with the sacrifice of other parties’ rights. Credit reporting is an activity which is carried out before a person enters any obligation in the creditor-debtor relationship. Only when a contractual relationship has been established then the creditor has rights, which however are not satisfied by the sharing of the debtor’s data.

It is against this background that one needs to analyse the legal framework of consumer credit scoring in the EC. Likewise, it is against the same background that an interpreter should read existing data protection legislation and ask how do the processing, sharing, and manipulation of a multitude of credit reference data empowered by highly sophisticated technologies comply with it. In so doing, he/she should bear in mind the design, functioning, and uses of modern consumer credit scoring systems, described earlier in this work: systems where data from different sources are easily and quickly aggregated, new data automatically created and disclosed to a potentially unlimited number of third parties for a growing number of expanding purposes, and decisions affecting the lives of people are taken by means of their profiling and differentiation as well as the conferment of reputations.

For consumer credit scoring systems to be legally used, in fact, they must be subject to the prevailing protection offered to individuals set out in the law. The existence of reputation is certainly an inevitable phenomenon that affects every individual living in a community ('no man is an island', as Sartor, 2006, writes quoting poet John Donne) but ever developing sophisticated information technologies exacerbate and push to the extreme the negative consequences that it entails, i.e., the creation of blacklists and dissemination of so-formed 'achieved reputations'.

By contrast, the origins of, and reasons for, European data protection legislation denote the importance of the need for individual self-determination over one's personal data and the dangers that would derive from its absence or violation. Informational privacy is a right and represents a safeguard of social relationships for every individual living in a community. It is about liberty, dignity, and intimacy (just to mention few) and contributes to protect the values of the democratic order, at least as it is perceived according to the European welfare state model. Despite all the criticisms and problems of implementation associated with Directive 95/46/EC, respect for the rule of law requires compliance with the basic principles that it sets out. Thus, consumers should be given the clear choice and freedom to accept or not whether their personal data could be used for credit scoring and its purposes without penalising them in case of refusal. Beforehand, they should be clearly and intelligibly informed as to such a freedom and lack of negative consequences on their application, be it present or the future ones, or the cost of credit. In this respect, the terms and conditions that consumers sign when applying for credit should be scrutinised more closely and non-compliance with the law punished firmly. Perhaps, therefore, the EU may find out that, although it has already caught the original strain of the virus, it already possesses in its existing law the vaccine to cure it and prevent a pandemic effect: all it has to do is making sense of its data protection legislation.

References:

Agre, PE (1997), 'Introduction', in Agre, PE and Rotenberg, M (eds.) Technology and Privacy: The New Landscape (Cambridge: MIT Press), 1-28

Baesens, B et al., (2003), 'Benchmarking state-of-the-art classification algorithms for credit scoring', 54 Journal of the Operational Research Society, 627-635

Bainbridge, D and Pearce, G (2002), 'Tilting at Windmills - Has the New Data Protection Law failed to make a Significant Contribution to Rights of Privacy?', The Journal of Information, Law and Technology(JILT), at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/bainbridge/

Berger, AN and Udell, GF (1995), 'Relationship Lending and Lines of Credit in Small Firm Finance', 68 Journal of Business, 351-381

Bigus, JP (1996), Data mining with neural networks: Solving business problems from application development to decision support (New York: McGraw Hill)

Bloustein, EJ (1964), 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', 39 New York University Law Review, 962-1007

Bork, R (1990), The Tempting of America: The Political Seduction of the Law (New York: Simon & Schuster)

Bradford, M (2004), ‘Full data-sharing could stem over-indebtedness concerns’, 11 Credit Risk International, 10-11

Bridges, S and Disney, R (2001), ‘Modelling Consumer Credit Risk and Default: the Research Agenda’, Research Paper, Experian Centre for Economic Modelling (ExCEM), University of Nottingham

Bygrave, LA (1998), ‘Data Protection Pursuant to the Right to Privacy in Human Rights Treaties’, 6 International Journal of Law and Information Technology, 247-284

Carey, P (2004), Data Protection – A Practical Guide to UK and EU Law (Oxford: Oxford University Press)

Castelfranchi, C and Falcone, R (2003), ‘Socio-cognitive theory of trust’, in J, Pitt (ed.) Open Agent Societies: Normative Specifications in Multi-Agent Systems (London: Wiley)

Chalton, SNL and Gaskill, SJ (2006), Encyclopaedia of Data Protection (London: Sweet & Maxwell)

Conte, R and Paolucci, M (2003), Reputation in Artificial Societies: Social Beliefs for Social Order (Dordrecht: Kluwer)

DeCew, J (1997), In Pursuit of Privacy: Law, Ethics, and the Rise of Technology (Ithaca: Cornell University Press)

Desai, VS, Convay, DG, Crook, JN, and Overstree, GA (1997), ‘Credit scoring models in the credit union improvement using neural networks and genetic algorithms’, 8 IMA J Mathematics Applied in Business and Industry, 323-346

Diamond, DW (1991), ‘Monitoring and Reputation: The Choice between Bank Loans and Directly Placed Debt’, 99(4) Journal of Political Economy, 689-721

Diana, T (2005), ‘Credit Risk Analysis and Credit Scoring – Now and in the Future’, March Business Credit, 1-3

Electronic Privacy Information Center and Privacy International (2002), Privacy and Human Rights 2002 – An International Survey of Privacy Laws and Developments (Washington D.C. and London)

Fakuyama, F (1995), Trust (New York: Free Press)

Falcone, R and Castelfranchi, C (2001), Social Trust: A Cognitive Approach (Dordrecht: Kluwer)

Fensterstock, A (2005), ‘Credit Scoring and the Next Step’, March Business Credit, 46-49

Fractal Analytics (2003), ‘Comparative Analysis of Classification Techniques’, September, A Fractal Whitepaper

Fried, C (1970), An Anatomy of Values (Cambridge: Harvard University Press)

Gambetta, D (1990), Trust (Oxford: Blackwell)

Gavison, R (1980), ‘Privacy and the Limits of the Law, 89 Yale Law Journal, 421-471

Gerstein, R (1978), ‘Intimacy and Privacy’, 89 Ethics, 76-81

Glorfeld, LW and Hardgrave, BC (1996), ‘An improved method for developing neural networks: The case of evaluating commercial loan creditworthiness’, 23(10) Computer Operation Research, 933-944

Gross, K (2008), ‘Expanding the Use of Credit Reports and Credit Scores: The Need for Caution and Empiricism’, in Twigg-Flesner, C, Parry, D, Howells, G and Nordhausen, A The Yearbook of Consumer Law (Aldershot: Ashgate), 327-336

Hand, DJ and Henley, WE (1997), ‘Statistical Classification Methods in Consumer Credit Scoring: a Review’, 160(3) Journal of the Royal Statistical Society, 522-541

Handzic, M, Tjandrawibawa, F, and Jeo, J (2003), ‘How Neural Networks Can Help Loan Officers to Make Better Informed Application Decisions’, June Informing Science, 97-109

Hanson, JD and Kysar, DA (1999), ‘Taking Behavioralism Seriously: Some Evidence of Market Manipulation’, 112(7) Harvard Law Review, 1420-1572

Herzberg, L (1988), ‘On the attitude of trust, 31 Inquiry, 307-322

Howells, G (1995), ‘Data Protection, Confidentiality, Unfair Contract Terms, Consumer Protection and Credit Reference Agencies’, 4 Journal of Business Law, 343-359

Inness, J (1992), Privacy, Intimacy, and Isolation (Oxford: Oxford University Press)

Jappelli, T and Pagano, M (2002), ‘Information Sharing, Lending and Defaults: Cross-Country Evidence’, 26(10) Journal of Banking and Finance, 2017-2045

Jay, R and Hamilton, A (2003), Data Protection – Law and Practice (London: Thomson Sweet & Maxwell)

Jay, R (2007), Data Protection Law and Practice (London: Thomson Sweet and Maxwell)

Jensen, HL (1992), ‘Using Neural Networks for Credit Scoring’, 18(6) Managerial Finance, 15-26

Klein, DB (2001), ‘Credit-Information Reporting: Why Free Speech is Vital to Social Accountability and Consumer Opportunity’, 5(3) The Independent Review, 325-344

Klein, DB (1997), ‘Knowledge, Reputation, and Trust by Voluntary Means’, in Klein, DB (ed.) Reputation: Studies in the Voluntary Elicitation of Good Conduct (Ann Arbor: University of Michigan Press)

Kuner, C (2007), European Data Protection Law (Oxford: Oxford University Press)

Kuner, C (2005), ‘Privacy, Security and Transparency: Challenges for Data Protection Law in a New Europe’, 16(1) European Business Law Review, 1-8

Leader, S (2006), ‘Inflating consent, inflating function, and inserting human rights’ in Dine, J and Fagan, A (eds.) Human Rights and Capitalism (Cheltenham: Edward Elgar, Cheltenham), 28-47

Liu, Y (2002), ‘A framework of data mining application process for credit scoring’, *Arbeitsbericht Nr 01/2002, Institut fur Wirtschaftsinformatik*

Lund, G (2004), ‘Credit bureau data: Maximising the benefits’, May/2004 Credit Management, 44-46

MacDonald, DA (2000), ‘Myths in the Privacy Debate’ in CEI Staff (ed.) The Future of Financial Privacy (Washington: Competitive Enterprise Institute), 54-75

MacKinnon, C (1989), Toward a Feminist Theory of the State (Cambridge: Harvard University Press)

McKnight, DH and Chervany, NL (1996), ‘The Meanings of Trust’, Technical Report MISRC Working Paper Series 96-04, Management Information Systems Research Center, University of Minnesota

Mester, LJ (1997), ‘What’s the Point of Credit Scoring?’, September/October Business Review, Federal Reserve Bank of Philadelphia

Moore, A (1998), ‘Intangible Property: Privacy, Power, and Information Control’, 35 American Philosophical Quarterly, 365-378

Orgler, YE (1978), ‘A Credit Scoring Model for Commercial Loans’ in Cohen, KJ and Gibson, SE (eds.) Management Science in Banking (Boston: Warren, Gorham & Lemont, Boston)

Parent, W (1983), ‘Privacy, Morality and the Law’, 12 Philosophy and Public Affairs, 269-288

Paul, J, Miller, F, and Paul, E (2000), The Right of Privacy (eds.) (Cambridge: Cambridge University Press)

Pennock, J and Chapman, J (1971), Privacy, NOMOS XIII (New York: Atherton Press)

Posner, R (1981), The Economics of Justice (Cambridge: Harvard University Press)

,
Rachels, J (1975), ‘Why Privacy is Important’, 4 Philosophy and Public Affairs, 323-333

Ramsay, I (2005), ‘From Truth in Lending to Responsible Lending’ in Howells, G, Janssen, A and Schulze, R (eds.) Information Rights and Obligations (Aldershot: Ashgate), 1-19

Rodotà, S (1995), Tecnologie e Diritti (Bologna: Il Mulino)

Sandage, SA (2005), Born Losers: A History of Failure in America (Cambridge: Harvard University Press)

Sartor, G (2006), ‘Privacy, Reputation, and Trust: Some Implications for Data Protection’, EUI Law Working Paper No. 2006/04, March 2006, available at http://www2.cirsfid.unibo.it/~sartor/GSCirsfidOnlineMaterials/GSOnLinePublications/GSPUB2006PrivacyReputationTrust.pdf on 08/01/09

Schoeman, F (1984), Philosophical Dimensions of Privacy: An Anthology (Cambridge: Cambridge University Press)

Singleton, S (2000), 'Privacy and Human Rights: Comparing the United States to Europe' in CEI Staff (ed.), The Future of Financial Privacy (Washington DC: Competitive Enterprise Institute) 186-202

Solove, DJ (2004), 'The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure', 53 Duke Law Journal, 967-1062

Sousa De Jesus, A (2004), 'Data Protection in EU Financial Services', ECRI Research Report No. 6, April 2004

Stiglitz, JE and Weiss, (1981), 'Credit Rationing in Markets with Imperfect Information', 71(3) American Economic Review, 393-410

Thomas, LC (2000), 'A Survey of Credit and Behavioural Scoring: Forecasting Financial Risk of Lending to Consumers', 16(2) International Journal of Forecasting, 149-172

Thomson, J (1975), 'The Right to Privacy', 4 Philosophy and Public Affairs, 295-314

Warren, S and Brandeis, L (1890), 'The Right to Privacy', 4 Harvard Law Review, 193-220

Westin, A (1967), Privacy and Freedom (New York: Atheneum)

Yobas, M and Crook, NJ (2000), 'Credit Scoring Using Neural and Evolutionary Techniques, 11 IMA Statistics in Financial Mathematics Applied in Business and Industry, 111-125

ENDNOTES

[1] This definition has been taken from Gross (2005, p.332).

[2] See, for example, McKnight and Chervany (1996); Fakuyama (1995); Herzberg (1988); Falcone and Castelfranchi (2001); Castelfranchi and Falcone (2003); Gambetta (1990); Klein (1997).

[3] See also Conte and Paolucci (2003).

[4] Article 29 Working Party on Data Protection, Working Document on Blacklists, 11118/02/EN/final, Adopted on 3 October 2002.

[5] Ibid.

[6] Directive 95/46/EC, OJ 1995 L 281 p 0031-0050.
Other laws, regulations, or codes of practices may have an impact on consumer credit reporting, although they do regulate it neither directly nor comprehensively. In Great Britain, for example, the 2006 Consumer Credit Act does not address the issue of data collection, processing, and dissemination.

[7] There is a considerable amount of literature that contributes to the moral, social, political and jurisprudential debates on privacy. The literature also helps to distinguish between descriptive from normative accounts of privacy. In these discussions, some emphasise the moral value of and interest in privacy, while others focus on it as a legal right to be protected. For general discussions about the value of privacy and its protection see Pennock and Chapman (1971); Paul et all (2000). For privacy as human dignity see Bloustein (1964). For a narrower view of privacy as self-determination, intimacy, or a meaningful aspect of interpersonal relationships, personal expression, and choice see Parent (1983);

Gerstein (1978); Westin (1967); Inness (1992); Fried (1970); Rachels J (1975); Gavison (1980); Moore (1998); Schoeman (1984); DeCew (1997). Contra, see Thomson (1975); Posner (1981); Bork (1990). For a feminist critique of privacy see MacKinnon (1989).

[8] See Directive 95/46/EC, Recitals 1-11.

[9] Charter of Fundamental Rights of the European Union, C 364 (2000), 0001-0022. See also Commission of the European Communities, Report from the Commission – First report on the implementation of the Data Protection Directive (95/46/EC), Brussels, 15 May 2003, COM (2003) 265 final. But see the exemption obtained by the United Kingdom – according to which the Charter on Fundamental Rights will not be justiciable in British courts or alter British law - after the agreement reached in late June 2007 on the Reform Treaty which replaced and preserved much of the Constitutional Treaty nominally collapsed after the rejection by Dutch and French voters in 2005.

[10] Directive 95/46/EC, Recital 4.

[11] Arguably, this opinion stems from the view over privacy laws enshrined in the US legal system. It follows the criterion that someone should have a reasonable expectation of privacy in a particular activity rather than embracing the European view that an individual should have control over data generated about him/her. See Kuner (2005).

[12] See also, for example, Hanson and Kysar (1999); Solove (2004); Rodotà (1995).

[13] See also, for example, Bygrave (1998); Chalton and Gaskill (2006). Jay and Hamilton (2003) explain that data protection is no longer seen as a 'stand alone' area of law as judges have increasingly taken a holistic view of personal information bringing together converging privacy sources (p. 39-69).
Reference should also be made to the Charter of Fundamental Rights of the European Union.

[14] See, for example, Jay and Hamilton (2003); MacDonald (2000); Singleton (2000).

[15] Directive 95/46/EC, Art. 3(2). Such derogation has been criticised as it could confer too much power to Governments or easily turn them into a 'Big Brother' hardly protecting the privacy of individuals and their liberty. See Singleton (2000).

[16] For criticisms on data protection legislation see Bainbridge and Pearce (2000)

[17] Council of Europe, Committee of Ministers, Explanatory Memorandum to Recommendation No. R (97) 18 of the Committee of Ministers to member states concerning the protection of personal data collected and processed for statistical purposes, Adopted by the Committee of Ministers on 30 September 1997.

[18] Directive 95/46/EC, Art. 15(1).

[19] Ibid., Art. 15(2)(a).

[20] Ibid., Art. 15(2)(b).

[21] Ibid., Art. 7(a).

[22] See also, for example, Carey (2004, p 73); Bainbridge and Pearce (2000).