Big Brother Is Scoring You

Wen Li CHAN[1]* and Hsin-Vonn SEOW[1]

[1]*Nottingham University Business School, University of Nottingham Malaysia Campus.*

**Correspondence: Wen Li Chan, Nottingham University Business School, University of Nottingham Malaysia Campus, Jalan Broga, 43500 Semenyih, Selangor, Malaysia. E-mail:wenli.chan@nottingham.edu.my*

Abstract

The personal data of a credit applicant that is collected by a lender from his application form and from credit reference agencies is used to generate credit risk profiles, that are used to make credit decisions that take place at various stages of an applicant's account, as well as for purposes of marketing other products or services of the lender or affiliated third parties. With the extensive amount of information at the disposal of lenders, data subjects may well be overwhelmed by the pervasiveness of potential incursions into their private lives based on patterns and relationships in mined data that form a person's profile. Focusing on the data protection and privacy framework in the UK, this paper identifies several areas for concern in the form of knowledge asymmetry and the inherent shortcomings of data mining, and links them to gaps in data protection in the areas of privacy notices, consent, and safeguards in automated decision-taking, with a view to establishing several broad recommendations moving forward.

Keywords: Credit scoring; Credit risk; Data mining; Profiling; Data protection; Privacy

1. Introduction

In the credit landscape, lenders have access to a wealth of information about individuals who apply for credit facilities. Personal data is obtained from a credit applicant in an application form. Data held by credit reference agencies (CRAs) often offer useful insights to other aspects of the applicant's financial standing and debts. Data on a customer's spending patterns after credit has been granted offer potentially valuable insights into his lifestyle and preferences.

'Profiles' derived from an analysis of all this data by way of credit scoring models may be used for credit decisions that take place at various stages of the lifetime of an applicant's account with the lender. From the lender's point of view, information from profiles provide useful insights to applicants' potential repayment behaviour, to aid decision-making in whether to grant, deny or renew credit, and in decisions to alter the terms upon which credit was initially granted (Lewis, 1992; Thomas *et al.*, 2002). The mining of such data is also useful to discover opportunities for the cross-selling of other financial products, and also to better target the communication of a product or service according to the probability of satisfactory payment by the customer (Lewis, 1992). In each of these scenarios, the purpose of the data processing, and hence profiling, is with the aim of making the most profitable decision in each case (Lewis, 1992; Siddiqi, 2006).

It is clear that the amount of information that can be derived out of such credit 'profiles' can be extensive, particularly given the speed and ease at which computing technologies are able to store, manipulate and utilize

data provided by a credit applicant (Shermach, 2006). It would not be far from the truth to say that the data collected for credit scoring purposes, combined with credit bureau data, could reveal much about applicants' private lives. Although carried out in the interests of promoting responsible lending and to reduce the lender's risks, it could be unsettling for an individual that upon making an application for credit, interpretations about his behaviours and habits from piecemeal disclores in application forms and public records are being made, at least partly by automated means, and converted into psychographic 'profiles' that could be used against him at any point of time during the life cycle of his credit facilities (Hildebrandt, 2006; Shermach, 2006). Indeed, the UK Information Commissioner's Office (ICO), which enforces the Data Protection Act 1998 (DPA), recognizes this when it states in its Privacy Notices Code of Practice that "combining information from different sources can create a very detailed picture of an individual's affairs" and that the individual "may not expect this and may find it overly intrusive" (ICO, 2010:14).

As an illustration of the potential pervasiveness of profiling, the Federal Reserve Board in the United States recently confirmed the evidence of practices where credit card holders had their credit limits reduced and interest rates increased because their spending patterns showed that they had begun to shop at discount stores, even in the absence of delinquency in any account (Rule, 2008; Board of Governors of the Federal Reserve System, 2010). While such practices were then discontinued upon receiving unfavourable public attention, it was reported that Congress would be loath to introduce restrictions in this regard without considering the role played by detailed transaction-specific information in fraud detection and prevention systems. Is profiling therefore a 'necessary evil', and how effective are the safeguards that are currently in place?

This paper reviews, with a focus on credit scoring practices in the United Kingdom, the extent to which the current legal regimes of data protection and privacy affords adequate protection in the interests of the credit applicant where credit profiles are concerned. The scope of this paper does not cover issues associated with credit reporting and data held and disseminated by CRAs, the legal framework surrounding which would be the subject of a separate, albeit related, area for consideration (Ferretti, 2008: 40).

The paper's analysis begins by examining the composition of an individuals' credit 'profile' and an overview of the main concerns surrounding the current legal framework. Some broad areas of concern are identified relating to the current practices in profiling and its associated data protection and privacy frameworks, followed by an assessment of the legal and practical implications. The final section concludes and discusses recommendations in moving forward.

2. Profiling the profile

Profiling may be said to be a form of sophisticated pattern recognition (Hildebrandt, 2006) that can be a valuable tool to distil useful knowledge out of a large volume of information (and noise) that is available to businesses, for the purpose of making decisions that lead to the most profitable courses of action. Profiling is widely applied across a broad spectrum of business areas where information is collected and analysed for decisions to be made affecting a person's financial, political, employment or healthcare situations (Hildebrandt, 2006; Weitzner *et al.*, 2008; FIDIS, 2009). In the financial sector, profiling is done for fraud prevention, anti-money-laundering, and in credit reporting and credit scoring (FIDIS, 2009).

Credit scoring models used by lenders, which determine the probability of repayments of debts by credit applicants, assign a score to an individual based on the information processed from the data provided by the applicant and CRAs. A credit applicant's personal information, such as age, marital status, job, income level, living arrangements, real estate data, and dependents (Lewis, 1992; Ferretti, 2006; Siddiqi, 2006), is obtained by the lender from the applicant's application form, and is combined with information from credit reference files kept by CRAs to create credit scorecards that will form the basis for a decision on whether or not to grant credit (FIDIS, 2009; Information Commissioner's Office, 2009).

Data that is kept on an individual's credit reference file with a CRA include public record information from the electoral roll, from bankruptcy/insolvency records, data on court proceedings such as court county court and high court judgments, information on a person's credit account with his other lenders (if the individual's consent has been sought for such disclosure to the CRA when credit was applied for), arrangements to pay, records of credit reference searches made within a certain timeframe, any financial associations with joint accounts or joint applications for credit, and live, settled, closed and defaulted accounts within a certain timeframe (Information Commissioner's Office, 2009). With the breadth and depth of information involved, the extent to which a credit applicant's right to privacy is respected is worthy of investigation.

Before assessing the legal implications of profiles, the anatomy of a profile should be examined. Profiles are usually created by way of a process referred to as knowledge discovery in databases (KDD), which involves the data collection, data preparation and storage, data mining, interpretation and decision making (Hildebrandt, 2006; FIDIS, 2009).

The word "profiling" is defined in the Oxford English Dictionary as "the recording and analysis of a person's psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people". In more technical terms, profiling can be described as an exercise of using data mining to identify certain patterns in an effort to classify individuals into particular sets of expected characteristics. The importance of profiling is not in the data; rather, it is in the knowledge one obtains from the data (Hildebrandt, 2006). This particular knowledge is inferred from data through the utilisation of particular techniques, and subsequently e used in making decisions that impact lives.

According to FIDIS (2009), the profiling process is usually associated with data mining, which is defined as a technique used for large databases to discover patterns or hidden information in very large databases. Data mining one of the five steps in Knowledge Discovery in Databases, a nontrivial process used to identify valid, novel, potentially useful, and ultimately understandable patterns in data (Fayyad *et al*. ,1996). From a technical standpoint, there are five successive steps: data collection, where the relevant data is selected to form the target dataset or database for analysis; data preparation, where the data collected goes through pre-processing to ensure the removal of noise and complexity reduction; data mining, where the analysis of the data with the usage of algorithms or heuristics that fit the data, the model developed and goals it is meant to achieve; interpretation, where the knowledge in the form of the mined profiles are evaluated by analysts to determine their usefulness; and the determination of actions, a stage that encompasses the identification of a user as a member of a mined profile, institutional decisions and subsequent actions upon profile application.

In the financial sector, banks and insurance companies normally carry out profiling where different interest groups or stakeholders like customers, are involved (FIDIS, 2009). In credit scoring, which is optimised for the

management of risks of the financial institution, profiling can play a role in the prevention of systemic risks from happening. This concept was common before the post-2007 crisis in the financial sector, for instance in the Basel II regulations that provide international standards for banking regulators when evaluating the risk management of banks.

3. A score or a miss?

Data used in creating a profile includes information that is provided to the lender (data controller[1]) directly from the credit applicant or customer (data subject[2]), during the credit application process. Issues arise on several levels that in essence revolve around the problem of knowledge asymmetry.

3.1 Knowledge asymmetry

The data collected from customers from their application forms may not always be accurate. However, as no mandatory procedures for verification (of correctness or truth) take place prior to the inputting of such data into the credit scoring system[3], for understandable reasons that it would be impractical for accuracy checks to be made of personal data provided by someone else (ICO, The Guide to Data Protection), the inaccurate risk profile that is generated is nevertheless used to make decisions on giving or rejecting credit, revision of interest rates or putting an account under scrutiny (FIDIS, 2009).

Pursuant to Section 7 of the DPA, a data subject has a right to access and request for amendments to personal data[4] that is being held by a data controller, by way of a 'subject access request'. Thus, an individual who is refused credit may write to the lender for an explanation of the reasoning for the decision (ICO, 2009; ICO, The Guide to Data Protection). If any data held by the lender or CRA is found to be inaccurate, an individual has the right under Section 14 of the DPA to apply[5] to request for such data to be rectified, blocked, erased or destroyed. The court may extend such an order to ask the data controller to notify any third parties to whom the information has been disclosed; for instance, a lender may be ordered to inform the CRAs who retain the individual's information of the amendment (ICO, The Guide to Data Protection).

---

[1] 'Data controller' is the term used in the Data Protection Act 1998 (s. 1) to refer to a person who (alone or jointly with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

[2] 'Data subject' is the term used in the Data Protection Act 1998 (s. 1) to refer to an individual who is the subject of personal data.

[3] The Guide to Credit Scoring only goes as far as to state that data should be captured, entered and coded correctly; validation of application details may take place but is not compulsory; see Guide to Credit Scoring (2000), paragraphs 3.2, 4.3, 5.1.

[4] In credit scoring, a profile is linked to an identifiable person (as opposed to an anonymous person), thus bringing it under the purview of data protection legislation, which applies to 'personal data', i.e. any information relating to an identified or identifiable natural person.

[5] If the issue cannot be resolved by informal means, the data subject may apply to the Information Commissioner or to the courts. Depending on the merits of the case, the Information Commissioner may ask the lender to take the relevant steps to comply with the DPA if it feels compliance has not taken place (DPA; ICO, The Guide to Data Protection). The Information Commissioner does not have power to award any compensation, and redress in this manner will have to be sought in court (ICO, The Guide to Data Protection).

It is noted that the exercise of the data subject's rights described above would be in reaction to a situation where data processing has already taken place and the applicant is informed of a refusal of credit, and would thus come too late, as it will not afford preventive protection against incorrect treatment and espouses a process that is contradictory to the presumption of innocence (FIDIS, 2009). Furthermore, any rectification of incorrect data may involve a release of more personal data (i.e. the correct data), resulting in the data subject experiencing a further loss of informational privacy (FIDIS, 2009).

To compound the situation discussed above, the lender may cite the protection afforded by intellectual property rights or trade secrets to restrict data subjects' right to access their profiles (ICO, The Guide to Data Protection), or decide not to reveal information on the type of scoring used if it is felt that such disclosure could be linked to financial crime and may result in compromising their security procedures (Guide to Credit Scoring, 2000; The Lending Code, 2011).

In short, a person who applies for credit starts off the process in a position where his application is likely to be assessed by the lender based on potentially inaccurate information, and is thus placed in a guilty-until-proven-innocent situation. In proving his 'innocence', there is a possibility that his right to access the information on him kept by the lender would be restricted curtailed on the grounds of intellectual property rights or for security reasons, in which case he may end up with limited or no means of redress. If he is granted subject access, he incurs a further notional loss of informational privacy if he decides to provide information to correct the data in the profile.

In effect, it could be said that the present legal regime of data protection vis-à-vis credit applicants and lenders is such that it keeps the credit applicant in the dark, producing an asymmetry of knowledge greatly in favour of the lender (De Hert and Wright, 2009; Hildebrandt, 2006; Rule, 2008). The procedural safeguards of ensuring transparency to data subjects and accountability of data controllers is therefore compromised (see De Hert and Gutwirth, 2006; Weitzner, 2008).

Interestingly, the informational imbalance also affects the lender – the situations discussed above generally take place when an applicant has been refused credit. Persons whose applications for credit have been successful would be rather more unlikely to make a subject access request. In such a situation, any error in data would not be uncovered, which raises the question of whether within this data protection regime, lenders could then be unknowingly making non-optimal decisions based on inaccurate data.

3.2 Data mining – a double-edged sword

As discussed above, the process of credit scoring utilises data mining techniques to arrive at credit scorecards, that are incorporated as part of a profile on the applicant that is then used in a decision to grant or deny credit, or to identify data subjects who are likely to be interested in and would be good customers to cross-sell financial products to. From a data mining standpoint, the general principle is that the more data there is available for analysis, the more precise the resulting profile will be (De Hert and Wright, 2009), and, barring any legal barrier, as many variables as possible that may have associations with the risk of default would be included in the credit scorer's model (Chan and Seow, 2013).

It should be borne in mind that the process of data mining does more than merely presenting existing data in new ways; as its value is in discovering previously unknown patterns and relationships among the data (Cook and Cook, 2003). However, data mining can be a double-edged sword. While such exploitation of data has potentially great commercial value to businesses in creating and maintaining their competitive advantage, data mining processes are just as likely to generate patterns or trends that are meaningless, or worse, do not represent a correct picture of the data subject's financial situation (Cook and Cook, 2003).

As the profiles still go on to be the included in the decision-making process in respect of a data subject's creditworthiness, such possibilities can be alarming for both lender and customer. On the part of the lender, it would defeat the very purpose of credit scoring and profiling which was intended to help the lender make the best possible decision in each case. The customer suffers even more detriment, in that in addition to running the risk of being 'judged' based on an inaccurate profile, in seeking redress, he will find himself already in a disadvantaged position, as described in the preceding section on the problem of knowledge asymmetry.

4. Data protection gaps

What recourse do data subjects have in the wake of these bleak revelations? In the UK, the credit industry clearly has informational advantage over applicants (Rule, 2008). It is a recognized fact that the practice of 'positive reporting', referring to the virtually unlimited access by lenders to consumers' accounts with lenders, the data subject is at the mercy of an information flow that they cannot control, between retailers and financial institutions, CRAs, and lenders (Rule, 2008). This is however not a universal state of affairs, even within the European Union. In France, only data in delinquent accounts are kept in a central register, and the applicant has the discretion whether to bring other credit relationships to the attention of the prospective new credit grantors (Rule, 2008; Ferretti, 2008).

As far as credit profiles are concerned, individuals are entitled to expect equal access to credit (see Chan and Seow, 2013), but there is no legal right to be entitled to credit (Information Commissioner's Office, 2009). However, individuals do have a right to privacy of their information, as a manifestation of individual choice, personal autonomy, and the self-determination of individuals in their social and relational affairs (De Hert and Gutwirth, 2006). This is consistent with the right to privacy set out in Article 8(1) of the European Convention on Human Rights which provides a right to respect for one's "private and family life, his home and his correspondence"[6]. Respect for privacy and data protection are regulated in several European Union directives; principally the Data Protection Directive[7], which is incorporated into UK law by way of the DPA.

A 'privacy notice'[8] is a way of satisfying the legal requirements in the DPA that require data controllers to process (i.e. collect, use, disclose, retain or dispose[9]) personal data fairly and lawfully[10] (ICO, 2010). The DPA requires

[6] The European Convention on Human Rights is incorporated into UK law through the Human Rights Act 1998.
[7] 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.
[8] Privacy notices have also been referred to as "fair processing notices", the term being a reference to the provisions of the DPA stating that personal data must be processed "fairly" (ICO, 2010).
[9] DPA, Section 1
[10] DPA, Schedule 1, Part I, Paragraph 1; Schedules 2 and 3.

privacy notices to inform a person of the identity of the data controller, the purpose or purposes for which the data is intended to be processed, and any further information necessary, in the specific circumstances, to enable the processing in respect of the individual to be fair[11]. "Fairness" in this context is not specifically defined in the DPA, but is taken to refer to the use of information in a way that people would reasonably expect and in a way that is fair, and ensuring that data subjects know how their information will be used, as well as considering the effect the processing will have on the individual (ICO, 2010). The Information Commissioner's Office recommends that at the bare minimum, privacy notices should inform the identity of the data controller, what the data controller will do with the collected personal data, and who it will be shared with (ICO, 2010). Regard is also to be had to the method by which the personal data is obtained, including whether the data subject has been deceived or misled as to the purposes for which the data is to be processed[12].

4.1 Privacy notices and the reality of consent

Issues of consent arise in situations where the lender wishes to pass on a customer's personal data to for purposes other than the credit application concerned, or to third parties who may be affiliated with the lender or who may have been contracted to carry out marketing and promotional activities for the lender's products and services. Consent is not so much an issue where it relates to the processing of personal data for purposes of the transaction that the individual has requested for (ICO, 2010), provided the use of the information is transparent and the processing has been conducted fairly.

The EU Data Protection Directive[13] emphasizes the importance of obtaining the unambiguous consent of data subjects before any data processing takes place (Ferretti, 2008). In obtaining consent, an 'opt-in' system is preferred, whereby in the absence of any positive statement that a person consents to dissemination of his personal data, no consent is to be interpreted (Ferretti, 2008; Rule, 2008). The opposite, so-called 'opt-out' system is where a person is assumed to have consented to dissemination of his personal data unless he indicates to the contrary (Ferretti, 2008; Rule, 2008).

The gaps in personal data protection that give rise to information asymmetry are manifold. Firstly, as far as the DPA is concerned, it is left to data controllers (lenders) to determine if they wish to obtain consent through opt-in, or opt-out, scenarios; the ICO's Privacy Notices Code of Practice expressly states that it is "acceptable to use both opt-ins and opt-outs", with the only caveat that the notice is not phrased in a way that will confuse people (ICO, 2010:16). Indeed, the said Code also states that "in many cases it is enough to be transparent" and that a person's positive agreement will most likely be needed "where sensitive information is being collected, or where previously collected information is to be used in a significantly different way" (ICO, 2010:11). "Sensitive" information is not defined, as is what is to be considered use in a "significantly different way", and presumably this would depend on the facts of the individual case.

Given the already disadvantaged position of the data subject, as discussed in the preceding section, it is submitted that this burden be reversed, with a focus on allowing the data subject determine the boundaries

[11] DPA, Schedule 1, Part II, Paragraph 2(3).
[12] DPA, Schedule 1, Part II, Paragraph 1(1).
[13] EU Directive 95/46/EC, see Articles 30, 33.

within which his personal information should be disclosed, as opposed to focusing on what is the more efficient manner for organisations to operate behind the scenes. Implementation-wise, this may call for changes in the way lenders cross-market their products, but it is submitted that an approach to privacy and data protection that is based on the notions of transparency, control (by the data subject of his privacy) and responsibility (of the data controller in handling personal data) is adopted rather than one that is opaque and one-sided (Rule, 2008; De Hert and Wright, 2009). Such recommendations have already surfaced in the larger area of profiling in ambient technologies (Hildebrandt, 2006; De Hert and Wright, 2009).

The second problem that is contributing to the imbalance of information is that the DPA does not compel the disclosure by the lender to the applicant of the specifics of how his personal data will be used other than for the present credit application, or the identity of the third parties to whom the information is intended to be passed on. For the specific context of lenders, the Lending Code provides that lenders must have a customer's "specific permission" to pass his name and address to "any company, including other companies in the [lender's group of companies], for marketing purposes"[14], but does not compel the identities of those companies to be revealed to the applicant.

Turning to the ICO's Privacy Notices Code of Practice for guidance, the recommendation of the ICO is that any requests for permission to share customer information with third parties should be "backed up with more detailed information, for example the names of the companies involved, *for those that want it*" [emphasis added] (ICO, 2010:14). The sharing of detailed information on the third parties who may receive an applicant's data is thus not only non-mandatory (the ICO's code of practice does not have the force of law), it places the onus on the data subject to actively request for such disclosure.

It is submitted that this absence of specificity in the information provided to data subjects is contrary to the notion that in order for data processing to be transparent, the data subject should be notified in advance of the purposes for which his personal data will be use, by making information readily available. The reverse situation, which is reflected in the current practice, does not usefully benefit a data subject, and tends to focus more on procedural, rather than substantive, compliance with data protection legislation (see Robinson *et al.* (2009) for similar views in a critique of the EU Data Protection Directive).

One could argue that it may not be practical to disclose entire lists of affiliated organisations up-front in an application context. It may be that lenders will need to anticipate more than one instance of consent to be sought from the data subject, for every instance that personal data is processed or passed on to a different entity for processing; as is recommended in the context of CRAs by Ferretti (2008). It would not be unfair to state that data processing cannot be said to be based on lawful consent if it is sought for general or vague purposes (Ferretti, 2008).

4.2 A potential decline of credit scoring?

In grappling with the issues highlighted in the preceding section on the predicament surrounding the use of data mining in the profiling process, it would be useful to examine the provision of the DPA conferring data subjects a

[14] The Lending Code, paragraph 23.

right to not be subject to decision-making on a solely automated basis in circumstances that significantly affect the data subject, such as his creditworthiness[15].

The DPA stipulates that the data subject has a right to notify the data controller not to take an automated decision affecting him, and that in the absence of such a notice the data controller should inform a data subject when a decision has been taken based on automated means without human intervention. The individual may request to be reconsidered if a decision was taken on automated means. Automated decision-taking is allowed if it is taken in preparation for, or in relation to, a contract with the data subject to give the individual something they have asked for, or where steps have been taken to safeguard the legitimate interests of the data subject, such as allowing them to appeal the decision[16].

The Guide to Credit Scoring (2000) implies that credit scoring would fall under the category of decisions involving automated decision-taking under the DPA, as credit grantors would be using personal data for considerations related to the entry into, or performance of, a contract for provision of credit with the applicant; and that the fact that the applicant is allowed to appeal a decision on granting credit, steps would have been taken to safeguard legitimate interests of credit applicants[17]. The Guide also notes that lenders will generally use credit scorecards as part of an automated decision-taking process (recognizing that human input would still play a part in the eventual credit decision)[18] and indicates that if credit scoring has been used and a data subject has put the data controller on notice that a decision is not to be taken on automated means, a manual underwriting process may be introduced[19].

The preceding section highlighted inherent flaws in data mining that have a potential of backfiring on both customers and lenders. In light of this, is the provision of an avenue for appeal in respect of a credit granting decision sufficient to deem the data subject's interests "safeguarded"? Given the inherent exploratory nature of data mining, there may be no such thing as a "safeguard" against incorrect patterns and relationships being generated during the process. It would be paradoxical to suggest increased human intervention into the identification of patterns, as the development of credit scoring techniques is based on the underlying notion that humans are unable to evaluate loan applications in an optimum way due to bounded rationality and the propensity for judgmental processes to enter the decision-making process (see Ferretti, 2008: 21).

As further food for thought, will awareness of data protection rights, coupled with the predicaments surrounding the use of data mining in profiling, result in more and more data subjects requesting lenders not to use automated processes in their decisions to grant or deny credit, thus leading to a decline in the use of credit scoring?

[15] DPA, Section 12(1).
[16] DPA, Section 12(7).
[17] See Guide to Credit Scoring (2000), paragraph 5.7
[18] *Ibid.*, paragraph 5.8
[19] *Ibid.*, paragraph 5.9

5. Conclusions and further research

It is clear that the regulatory framework in terms of privacy and data protection that has evolved around the credit risk profiling has been excessively focused on secrecy and up-front control of information by data controllers, resulting in policies and practices that suppress information flow and that may hinder the resolution of the very problems they sought to address (Rule, 2008; Weitzner *et al.*, 2008). The present data protection framework in the UK is not adequate in preserving the rights of individuals the face of potential incursions into personal space that come with the process of profiling. The data subject is often left in the dark as to where his personal data may end up once he has signed off his application form, and although lenders will attempt to inform him how they will use his information, he is often not in a position to negotiate. Neither does he have any real choice - with few incentives to be transparent and every reason to retain secrecy to preserve competitive advantages, the *status quo* fosters a situation where potentially all lenders in the market will remain opaque.

While the processes currently in place appear to serve lenders' purposes well and are important in maintaining the efficiency of lenders' decision support systems, concerns are raised over the limited extent to which the data subject can meaningfully exercise rights to ensure that his personal data is used only for the purposes he is requesting for. It is recommended that an opt-in system be adopted in order for meaningful consent to be obtained where personal data is further processed to profile the customer for account maintenance and marketing purposes, and that details of third parties to whom information is intended to be passed on to for further processing be made available on a proactive basis.

The process of profiling one's credit behaviour includes a process of data mining, intended to discover new, previously unknown patterns, which are then used in taking a decision on whether credit would be granted, or if terms on which credit was granted would be altered. When the present data protection setbacks are viewed together with the inherent exploratory nature of data mining that could work against both lenders and customers, interesting questions arise in terms of the long-term sustainability of the empirical methods currently used.

It would be challenging to attempt to change the present frameworks of data protection and privacy, though a beacon of hope may lie in increasing awareness of the inequities perpetuated by the present system, in order that best practices may develop that equal out the information imbalance between lenders and consumers.

Moving forward, it would also be useful for further research to consider how human intervention could usefully supplement the automated decision-taking present in a credit scoring process in a way that would mitigate the shortcomings of data mining as a decision-making tool that potentially affects the financial health of individuals.

References

Board of Governors of the Federal Reserve System (2010), *Report to the Congress on Reductions of Consumer Credit Limits Based on Certain Information as to Experience or Transactions of the Consumer,* May 2010.

Chan, W. L. and Seow, H. V. (2013) Legally Scored, *Journal of Financial Regulation and Compliance*, Vol. 21, Iss. 1, pp. 39-50.

Cook, J. S. and Cook, L. L. (2003), *Social Ethical and Legal Issues of Data Mining,* in Wang, J. (2003) (ed.), *Data Mining: Opportunities and Challenges*, Idea Group Publishing, Hershey, pp. 395-420.

Data Protection Act 1998, available at: http://www.legislation.gov.uk/ukpga/1998/29, (accessed June 21, 2013).

De Hert, P. and Gutwirth, S. (2006), *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power*, in Claes, E., Duff, A. and Gutwirth, S. (eds.) *Privacy and the Criminal Law*, Interstentia, Antwerp/Oxford, pp. 61-97.

De Hert, P. and Wright, D. (2009), Legal safeguards for privacy and data protection in ambient intelligence, *Personal and Ubiquitous Computing*, Vol. 13, pp. 435-444.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals wiith regard to the processing of personal data and on the free movement of such data, No. L 281/31.

European Court of Human Rights, *Official text of the European Convention on Human Rights*, available on: http://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=#n1359128122487_pointer (accessed July 28, 2013).

Fayyad, U.M., Piatetsky-Shapiro, G. and Smyth, P. (1996) From Data Mining to Knowledge Discovery: An Overview, *AI Magazine*, Fall 1996, pp. 37-54.

Guide to Credit Scoring (2000), available at: http://www.bba.org.uk/policy/article/guide-to-credit-scoring/self-regulation, (accessed June 21, 2013).

Ferretti, F. (2007), Consumer credit information systems: A critical review of the literature. Too little attention paid by Lawyers?, *European Journal of Law and Economics*, Vol. 23, No. 71, pp. 71-88.

Ferretti, F. (2006), Re-thinking the regulatory environment of credit reporting – Could legislation stem privacy and discrimination concerns? *Journal of Financial Regulation and Compliance*, Vol. 14, No. 3, pp. 254-272.

Ferretti, F. (2008), *The Law and Consumer Credit Information in the European Community – The Regulation of Credit Information Systems*, Routledge Cavendish, Abingdon/New York.

Future of Identity in the Information Society (FIDIS) (2009), *Profiling in Financial Institutions*, D 7.16, Final report version 1.0, June 29, 2009, available at: http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp7-del7.16.Profiling_in_Financial_Institutions.pdf (accessed June 25, 2013).

Hildebrandt, M. (2006), Profiling: From Data to Knowledge, *Datenschutz und Datensicherheit*, Vol. 30, No. 9, pp. 548-552.

Information Commissioner's Office (ICO) (2009), *Credit Explained*, February 2009, available at: http://www.ico.org.uk/for_the_public/topic_specific_guides/~/media/documents/library/Data_Protection/Practical_application/credit_explained_leaflet_2005.ashx (accessed July 28, 2013).

Information Commissioner's Office (ICO) (year unavailable), *The Guide to Data Protection*, available at: http://www.ico.org.uk/for_organisations/data_protection/the_guide (accessed on June 21, 2013).

Information Commissioner's Office (ICO) (2010), *Privacy Notices Code of Practice*, December 2010, available at: http://www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_notices (accessed June 21, 2013).

The Lending Code (2012), March 2011, Revised May 1, 2012, available at: http://www.lendingstandardsboard.org.uk/docs/lendingcode.pdf (accessed June 25, 2013).

Lewis, E.M. (1992), *An Introduction to Credit Scoring*, Fair, Isaac & Co. Inc., San Rafael, CA.

Robinson, N., Graux, H., Botterman, M. and Valeri, L. (2009), *Review of the European Data Protection Directive* (prepared for the Information Commissioner's Office), RAND Europe , May 2009.

Rule, J. B. (2008), *Conclusion chapter,* in Rule, J. B. and Greenleaf, G. (Eds.) (2008), *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham.

Siddiqi, N. (2006), *Credit Risk Scorecards – Developing and Implementing Intelligent Credit Scoring*, Wiley, Hoboken, NJ.

Shermach, K. (2006), Data Mining: Where Legality and Ethics Rarely Meet*, Ecommerce Times*, August 25, 2006, available at: http://www.ecommercetimes.com/story/52616.html (accessed July 24, 2013).

Thomas, L.C., Edelman, D.B. and Cook, J.N. (2002), *Credit Scoring and Its Applications*, Society for Industrial and Applied Mathematics, Philadelphia, PA.

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J. and Sussman, G. J. (2008), Information Accountability*, Communications of the ACM*, Vol. 50, No. 6, pp. 82-87.