RESPONSIBLE A.I. CREDIT SCORING

Katja Langenbucher
Frankfurt/Goethe University
Paris/SciencesPo
currently visiting at Fordham Law School

Introduction

A core element of a lender's decision when handing out a loan is the assessment of the borrower's creditworthiness. Some of this work is done by the lender himself, for example by performing internal checks and by applying rating models to information he may have at his disposal. Other parts of this task are outsourced to intermediaries, such as data brokers or credit rating agencies. The latter deliver credit scores based on their proprietary rating methodology.

Historically, corporate lenders based their loan decision on a more or less intuitive mix of quantitive and qualitative information. They might have looked at income, net worth, pay-back morale, and availability of collateral. But many will also have considered gender, religion, race or social networks. Outfits such as FAIR, ISAAC AND COMPANY were among the first to aim beyond mere hunches on which information might be relevant for a lender. Instead, they tried to deliver quantitative risk assessments.[1] Earlier work by mathematicians had paved the way for this. These had combined measurable data points with information about the repayment of past loans.[2] In this way, they established statistical correlations between specific pieces of information and ease (or difficulty) of repayment. Relying on such correlations, not only would some data points emerge as more relevant than others. In addition, it was possible to attribute more weight to important information, whereas other variables contributed to a lesser degree to the overall score. Credit scoring agencies, until this day, compete in finding the best model to establish relevant variables and the appropriate weight to be assigned to those in the overall assessment.

A credit score's usefulness for a corporate lender depends on its ability to predict the borrower's performance. Progress in technology available for this task has been disrupting the credit scoring business in a number of ways. The amount of potentially relevant information has soared. Massive amounts of data are stored and the costs for sorting them and for searching for specific variables have been decreasing. "Artificial intelligence" (more accurately: machine learning) has contributed to finding numerous and often unanticipated correlations and has delivered ever more finely tuned predictions. Today we are seeing traditional credit rating agencies improving their methodology as well as entirely new players entering the field. They do so as rating agencies and as (often online) lenders, both using novel types of data and models. What these players look for goes beyond traditional quantitative data. In addition to (or sometimes instead of) income, net worth or collateral, they may collect information on "education, area of study" and "job history"[3], the state of residence[4] or the borrower's performance at online platforms such as amazon

[1] This is where today's U.S. credit rating score "FICO" stems from. On Europe see Sachverständigenrat für Verbraucherfragen, *Verbrauchergerechtes Scoring*, Berlin 2018, p. 22-23.
[2] David Durand, *Risk Elements in Consumer Installment Financing*, New York NBER 1941.
[3] See: https://www.upstart.com.
[4] See: https://www.circlebacklending.net/index.php.

or ebay.[5] More daringly, they check "handset details, SMS logs, GPS data" or "contact lists"[6] (and much more[7]).

A.I. credit scoring has been hailed as inclusive, giving groups of borrowers access to credit which had long been held back because their profile did not match traditional scoring models. Just like FAIR, ISAAC AND COMPANY allowed more measurable risk assessments instead of intuition and bias, and opened up credit markets to those which displayed the sought-after quantitative characteristics, A.I. credit scoring will often have that effect.[8] At the same time, the availability of what has been called "alternative data" on a global scale as well as the considerable intransparency of how such data are being used in credit scoring models have raised a number of concerns.

Data privacy is chief among them. The relevance of much "old-school" quantitative data underlying credit scoring won't come as a surprise to potential borrowers. Most people are probably aware that data such as their income, their net worth or the collateral they can post will influence their credit score. This will be different as to the often unexpected correlations between alternative data such as social network affiliations, browser history, preferred means of payment or fitness tracking data and creditworthiness. Even less are most retail borrowers aware of what has been called "profiling". Profilers establish correlations between specific data points and belonging to a certain group. Using keywords such as "payday loan", "drunk" or "sick" in social media communication or in google searches may, for instance, correlate with belonging to a group which has difficulty in repaying loans.[9] To provide another example: information which correlates with impulsive behaviour puts a borrower in the more risky "bucket"[10] whereas information which, based on a correlation, suggests that he is good at delaying gratification puts him in the more successful group.[11] Lenders will be looking out for such data whereas potential borrowers may be hesitant about providing it - if they are being asked for their consent at all.

Discrimination is another worry. Legislation such as the U.S. Equal Credit Opportunity Act or a number of European Anti-Discrimination Directives prohibit discriminating on the basis of certain protected categories when making a loan decision. One concern is that a combination of innumerable data points and the correlations suggested by machine learning will produce discriminatory results which are not immediately apparent and much less provable in a litigation context. More worries arise from the type of data involved. Just like mathematicians established correlations between information gathered about bank customers and their success in repaying loans, machine learning starts with historical data on borrowers and their performance.[12] Any (current or historical) discriminatory measures reflected in such data will enter into the algorithm as the starting point on which it is trained. In that sense, artificial intelligence has been called "biased" because it pegs current to past choices.

---

[5] See: https://help.bitbond.com/article/9-borrow-bitcoins-in-3-steps.
[6] See the online lending company branch's advertisement available at: https://branch.co/how-it-works.
[7] Preliminary interviews conducted by me pointed to the frequency of charging a smartphone, to owning a pet or to having a garage as relevant variables.
[8] For the sake of simplicity, the question how the risk/return ratio of this new group of borrowers may translate into very high interest rates is ignored.
[9] See as an example: https://www.totallymoney.com/social-credit/
[10] On a statistical methodology called "bucket evaluation" see: XXXXXXXShabtai et alXXXXXX
[11] See https://www.fico.com/blogs/credit-scoring-which-personality-traits-predict-credit-risk
[12] GABRIELE BRITZ, EINZELFALLGERECHTIGKEIT VERSUS GENERALISIERUNG, VERFASSUNGSRECHTLICHE GRENZEN STATISTISCHER DISKRIMINIERUNG, p. 76 (Mohr Siebeck 2008).

A further concern has to do with the temptingly scientific allure of A.I. At first blush, algorithmic credit-scoring offers the chance to replace human errors, intuition and biases, with what comes across as an objective, mathematics-based computation. For a corporate lender, having "an algorithm" do the credit scoring carries the potential to comply automatically, as it were, with highest standards of care, surpassing whatever humans might be capable of. However, upon closer examination the promise of neutral objectivity might not carry that far. Algorithms have been called "opinions embedded in mathematics",[13] highlighting human input in their set-up. (Human) decisions are made on their point of departure, on the data they take in and on their "definition of success",[14] *i.e.* the goal towards which their correlations aim. Data fed into a machine-learning structure may suffer from a form of historical selection bias, it might not be correct, not exhaustive or not entirely up-to-date, to name but a few shortcomings of supposedly objective machine learning devices.

This paper suggests first steps towards what I will call "responsible" A.I. credit scoring, pulling together legal tools with a very different pedigree. The natural first step is to offer a tentative definition of "responsible" scoring. Against the backdrop of the most pressing concerns outlined above, I use the term "responsible" as meaning: in compliance with data protection and anti-discrimination laws. Exploring the legal framework provided by these areas of the law is done from a comparative law perspective. I outline general principles of U.S. and EU law, a discussion of doctrinal details is beyond the current scope. Data protection law will be illustrated using the European GDPR's and the U.S. FAIR CREDIT REPORTING ACT'S rules, focusing on collection, processing, profiling and consent. I explore anti-discrimination laws on the basis of the U.S. EQUAL CREDIT OPPORTUNITIES ACT and a number of EU Directives on equal treatment. Faced with algorithmic credit scoring, both jurisdictions encounter similar problems. Given that the corporate lender is mainly concerned with good credit risk, it will often be difficult to make a case for intentional discrimination on the basis of prohibited categories. Instead, concepts such as "disparate impact" (under U.S. law) or "indirect discrimination" (under EU law) come into play. These allow to address decisions based on rules which are facially neutral, but, statistically, produce discriminatory outcomes. While at first glance this seems a handy solution for achieving responsible A.I. scoring, I show significant challenges brought about when applying these concepts to machine-learning algorithms.

Having established a definitory legal framework for responsible A.I. scoring, I explore whether we can understand corporate duties of care as a legal tool providing efficient incentives to work towards that goal. I start from the assumption that there is a general duty for corporations to follow the law, hence for officers (and to a lesser degree for directors) to look out for that.[15] At first glance, this points towards strong incentives. The lender might expose himself to litigation by borrowers who were discriminated against or not adequately informed about storage, processing or profiling of their data. For the same reasons, regulatory authorities might step in, sanction via fines or withdraw a license required for the lender's business. Duties of care might require actions such as updating of historical data, limiting the extent of outsourcing scoring to third parties, calling for transparency towards potential borrowers or for a benchmarking of algorithmic correlations against

---

[13] CATHY O'NEILL, WEAPONS OF MATH DESTRUCTION, p. 21 (Broadway Books New York).
[14] CATHY O'NEILL, WMD, p. 21.
[15] U.S. scholars typically address this issue under the heading of "compliance". Some speak of a "duty of obedience", see Alan R. Palmiter, *Duty of Obedience: The Forgotten Duty*, 55 NEW YORK LAW SCHOOL LAW REVIEW 2010, 457-478; on the board's "Caremark" duties under U.S. law see XXXXXX; on the much less developed doctrine on officer's duties: VIRGINIA HARPER HO XXXXX; German law uses the term "duty of legality", see KATJA LANGENBUCHER IN: BANKGESCHÄFTE ZWISCHEN MARKT, REGULIERUNG UND INSOLVENZ, FESTSCHRIFT FÜR JÜRGEN LWOWSKI 333-347 (Beck 2014).

anti-discrimination standards. However, I suggest that closer inspection reveals significant doubts about the efficiency of these tools. Discussing the legal framework, it will become apparent that the application of both, data protection and anti-discrimination law to A.I. credit scoring is riddled with especially vague terms and concepts. This may change over time. For now, I submit that this fact alone will give considerable leeway on how to structure loan decisions to a corporate lender's management. This is even more so in the face of corporate law's business judgement rule, allowing for broad discretion as long as an informed decision is made in good faith. A.I.'s scientific charm will often provide good arguments for showing that an informed decision was made.

Obviously, any lender's business model depends on good predictions about the potential borrower's ability to repay. If he involves machine learning algorithms in his decision-making process, their design and implementation will have to be "state-of-the-art" to allow for profit and to satisfy his shareholders. Inappropriate design carries the risk of false positive as well as false negative rating results, leading to a host of unwelcome consequences. The lender may cluster risk with a group of borrowers or inadvertently miss out on groups of borrowers with an attractive risk/reward profile. The rise of FinTech lenders shows that there has indeed been considerable market potential for novel scoring models, some of which will even have benefitted formerly disadvantaged borrowers. I argue that it this shareholder-value driven approach which will probably shape how corporate duties of care will play out in the near future, rather than data protection or anti-discrimination laws.

The skeptical conclusions I draw as to corporate duties being a promising legal tool for achieving responsible A.I. credit scoring suggest a glance at more traditional topics of regulatory theory. A good mix of public and private law rules as well as meaningful enforcement options of both kinds is generally considered a promising avenue for legislators. It builds on empowering public agencies and on providing incentives for private actors. This seems to hold for algorithmic credit-scoring as well. Analyzing the role of public authorities, I discuss powers to enforce data protection in the EU and the U.S.[16] The U.S. Federal Trade Commission (FTC) and the U.S. Consumer Financial Protection Bureau (CFPB)[17] illustrate how public authorities have been entrusted with rule-making and enforcement powers as to discriminatory lending practices. Turning to private enforcement, I explore under which circumstances EU and U.S. borrowers, which have been discriminated against "by an algorithm", may file a civil liability law suit for actual and (under some jurisdictions) for punitive damages.[18] Still considering private enforcement, the potential for

---

[16] Art. 51 GENERAL DATA PROTECTION REGULATION (GDPR); FTC XXXX FAIR CREDIT REPORTING ACT.

[17] Under the Dodd-Frank Act, the CFPB has rule making and enforcement authority for the Equal Credit Opportunities Act (ECOA), the FTC has authority to enforce ECOA and Regulation B which details its application. In addition, the FTC has authority to enforce any CFPB rules to entities within the FTC's jurisdiction, which includes most providers of financial services which are not banks, see: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-enforcement-activities-under-equal-credit-opportunity-act-regulation-b/p811504_cfpb_ecoa_report_2018.pdf

[18] Art. 8 para. 2 of DIRECTIVE 2004/113/EC requires compensation of actual damages for violations of the Directive's rules on gender-based discrimination; art. 15 of DIRECTIVE 2000/43/EC and art. 14 of DIRECTIVE 2004/113/EC require efficient, proportionate and deterrent sanctions for violations of Member State's laws transposing the Directive, without stipulating that this has to include civil liability, details at: MÜNCHENER KOMMENTAR ZUM BGB (8th edition, Beck 2018), § 21 AGG, THÜSING, note 2. 15 U.S. CODE § 1691E(A) and 12 C.F.R. § 1002.16(B)(1) allow for actual damages, 15 U.S. CODE § 1691E(B) and 12 C.F.R. § 1002.16(B)(1) for punitive damages for violations of

civil liability law suits on the basis of data protection violations under EU and under U.S. law is discussed.[19] Lastly, I examine a flip-side of private enforcement in credit-scoring constellations. Against the backdrop of the growing importance of ESG-factors[20] in corporate governance, we may see an unusual actor contributing to private enforcement, namely the corporate lender's management. It may - exceptionally - push for non-discriminatory lending practices or for limiting certain usages of data, beyond what is clearly pre-formatted by the law. Often, this will involve a trade-off between accurate predictions of creditworthiness and fairness considerations. In the framework of corporate law, such situations translate as a conflict between shareholder and stakeholder value. I suggest that for jurisdictions stressing the former, it will often be difficult to see director's and officer's including fairness considerations at the expense of precise predictions of creditworthiness. Banking regulation will often point in that same direction, requiring safe and sound lenders and, probably, pricing algorithmic predictability over standards of responsible lending.

1. Defining responsibility: The framework of anti-discrimination and data protection law

1.1. Taking accountability seriously?

1.2. Taking anti- discrimination seriously?

2. Corporate duties and incentives

2.1. Corporate compliance and responsible A.I. credit scoring

2.2. Shareholder value and responsible A.I. credit scoring

3. Public and private enforcement and incentives

3.1. The public power to enforce

3.2. The private power to sue

3.3. The corporate power to do good

ECOA. Punitive damages are only available from nongovernmental creditors and limited to $10,000.

[19] Art. 82 para. 1 GDPR establishes a private right to compensation for material and non-material damages from the data controller or processor. The U.S. FAIR CREDIT REPORTING ACT allows for actual or statutory damages, and for punitive damages if the violation was willful XXXXXX. U.S. tort law accepts causes of action for invasion of privacy. The CALIFORNIA PRIVACY ACT, ASSEMBLY BILL NO 375, CHAPTER 55, provides for civil action for very specific cases, namely the unauthorized access and exfiltration, theft or disclosure as a result of a business' violation of the duty to implement and maintain reasonable security procedures and practices.

[20] The abbreviation stands for "environmental, social, governance".