Risky Business: Legal Implications of Emerging Technologies Affecting Consumers of Financial Services

Zofia Bednarz <z.bednarz@unsw.edu.au>

Kayleen Manwaring <kayleen.manwaring@unsw.edu.au>
SYDNEY, Australia

Abstract

Artificial Intelligence- (AI) driven Big Data analytics are becoming a core capability for financial institutions, giving rise to promises of profits and increased efficiency both for new FinTech firms and incumbent institutions. This, however, may come at a cost to consumers. This chapter analyses the challenges to legal and regulatory framework applicable to provision of financial services to consumers brought about by the use of AI and Big Data tools by financial services firms. We discuss harms to consumers potentially arising in terms of discrimination, privacy breaches, digital manipulation and financial exclusion, and argue policymakers and regulators must deliver a fit-for-purpose legal and regulatory framework, allowing both financial firms and consumers to reap benefits of the technological revolution.

Keywords:
Artificial Intelligence, Big Data, Financial Services, Consumer Protection, Consumer Harms

1. Introduction

Artificial Intelligence (AI)- and Big Data-related technologies have been recently causing major disruptions to the financial services industry. These technologies create important new opportunities for financial services

providers, in terms of costs reduction and increased efficiency.[1] The naturally data-rich industry is a perfect environment for AI and Big Data tools, which are leveraged to create value, offer innovative products and introduce new processes through AI-enabled analytics, risk management, customer acquisition, customer service, as well as automation and process re-engineering.[2] AI and Big Data analytics are becoming a core capability for financial institutions, with the technology playing 'an increasingly central role in creating value for banks',[3] insurers[4] and financial investment firms,[5] as well as their customers. The focus of this chapter is the use of AI and Big Data tools for automated decision-making in relation to offering of financial services to consumers and challenges it poses for legal and regulatory frameworks protecting consumers of financial services.

Recent studies are consistently showing increasing adoption of AI technology by financial services firms, indicating 85 % of firms are already using the technology,[6] and in particular, machine learning (ML) models.[7] The industry is making significant investments in AI technologies,[8] expecting consequent important benefits for firms. FinTech organisations are leading technological transformation of the industry.[9]

These promises of improvements may, however, come at a cost to consumers. Many customers will likely benefit from more accessible, cheaper and personalised services. Nevertheless, the technologies' use and automated decision-making may affect some consumers negatively, leading to harms related to discrimination, exclusion, invasions of privacy, unfair prices and digital consumer manipulation. Some of these issues are known, 'old' problems, which may become exacerbated through the tech-

1 Tom CW Lin, 'Artificial Intelligence, Finance, and the Law' (2019) 88 Fordham Law Review 531, 532–33.
2 Cambridge Centre for Alternative Finance and World Economic Forum (CCAF), 'Transforming Paradigms: A Global AI in Financial Services Survey' (January 2020) 30–33.
3 Sven Blumberg and others, 'Beyond Digital Transformations: Modernizing Core Technology for the AI Bank of The Future' (McKinsey & Company Financial Services, 28 April 2021).
4 Ramnath Balasubramanian, Ari Libarikian and Doug McElhaney, 'Insurance 2030: The Impact of AI on the Future of Insurance' (McKinsey & Company Insurance Practice, March 2021).
5 Deloitte, 'Client-facing technologies for investment banks' (December 2020).
6 CCAF (n 2) 25.
7 Deloitte Centre for Financial Services, 'AI leaders in financial services' (Deloitte Insights, 13 August 2019).
8 CCAF (n 2) 18.
9 ibid 26.

nology; some are new, arising directly out of this sociotechnical transformation. The use of AI and Big Data analytics may thus present a number of important challenges for law and regulation of retail financial services provided to consumers.

The issue is time sensitive. This sociotechnical change is already occurring, and it is crucial to analyse how existing legal rules govern this new reality, and if law reform is needed. The rules need to achieve a balance between protecting the market, as well as consumers, from harms, while at the same time creating a space in which innovation thrives. Timely examination of the problem against these criteria will allow us to assess whether the current legal and regulatory framework is fit for purpose, in order to both incentivise beneficial innovation and discourage harmful business models, that may otherwise become too entrenched to be easily dislodged later.[10]

This chapter proceeds as follows. Section 2 starts with a brief overview of AI and Big Data technologies, analyses how they are currently used in financial services, and outlines their potentially concerning characteristics. Section 3 focusses on challenges posed by these sociotechnical developments to legal and regulatory frameworks, including possible harms to consumers arising out of algorithmic bias, excessive data collection, digital manipulation and personalisation of financial services. Section 4 concludes.

2. *The Technologies: Characteristics and Use in Financial Services*

2.1. *Emerging Technologies Used by Financial Services Firms*

The sociotechnical change brought about by AI and Big Data technologies in the financial services industry is nothing short of revolutionary.[11] To

10 This conundrum or incentive for timely analysis of regulatory regimes in the face of sociotechnical change is also known as the 'Collingridge dilemma'. For a detailed discussion of the effects of the Collingridge dilemma, see Lyria Bennett Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target', (2013) 5 *Law, Innovation and Technology* 1, 8 and Kayleen Manwaring 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (2017) 22 *Deakin Law Review* 51, 58. Collingridge himself described it as the 'dilemma of social control': David Collingridge, *The Social Control of Technology* (Pinter, 1980) 11.

11 See eg CCAF (n 2) 11; OECD, 'The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector' (Report, 2020) 6–7; Linklaters, 'Artificial Intelligence

properly understand the legal and social consequences, we need to understand what these technologies are and what makes them so disruptive.[12]

Artificial Intelligence and Machine Learning

The term 'artificial intelligence', coined in the mid-1950s,[13] can be defined in a number of ways, both as a sociotechnical concept[14] and as a technology. As a technology, AI encompasses a range of tools and techniques.[15] One of the most common forms of AI of particular interest in the context of financial services is machine learning (ML).[16] ML models can be used in decision-making processes. These models improve their outcomes through learning, ie 'modify[ing] or adapt[ing] their actions',[17] eg using methods which detect patterns in data, which can be used to predict future data, or in probabilistic decision-making.[18] ML models tend to be empirically constructed, so their outcomes are based on the identification and application of correlations in the data, rather than causal reasoning.[19]

---

in Financial Services: Managing Machines in an Evolving Legal Landscape' (Report, September 2019) 4–6.

12 Chris Reed, 'Taking Sides on Technology Neutrality' (Pt 2007) (2007) 4(3) *SCRIPTed* 263, 282; Bert-Jaap Koops, 'Ten Dimensions of Technology Regulation: Finding Your Bearings in the Research Space of an Emerging Discipline' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing 2010) 312.

13 Gil Press, 'A Very Short History Of Artificial Intelligence (AI)' *Forbes* (30 December 2016) <https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/?sh=45bbb6e96fba> accessed 26 May 2021.

14 Michael Guihot and Lyria Bennett Moses, *Artificial Intelligence, Robots and the Law* (LexisNexis, 2020) Ch 1; Toby Walsh, *It's Alive! Artificial Intelligence from the Logic Piano to Killer Robots* (La Trobe UP, 2017) 17; House of Lords Select Committee on Artificial Intelligence, *AI in the UK: Ready, Willing and Able?* (Report of Session 2017–19, HL Paper 100, 16 April 2018) 13–14. Also See eg High-Level Expert Group on Artificial Intelligence, 'A Definition of AI: Main Capabilities and Disciplines' (European Commission, 8 April 2019) 1.

15 Toby Walsh and others, 'The Effective and Ethical Development of Artificial Intelligence: An Opportunity to Improve Our Wellbeing' (Report for the Australian Council of Learned Academies, July 2019).

16 CCAF (n 2) 16 –17.

17 Guihot and Bennett Moses (n 14) 23.

18 Kevin P Murphy, *Machine Learning: A Probabilistic Perspective* (MIT Press, 2012) 1.

19 Clarke, Roger, 'Why the world wants controls over Artificial Intelligence' (2019) 35 *Computer Law and Security Review* 423, 428 and Table 2. See also Kalev Leetaru, 'A Reminder that Machine Learning is About Correlations not Causation' *Forbes* (15 January 2019) <https://www.forbes.com/sites/kalevleetaru/2019/01/15/a

The advancements in AI technology bring about a paradigm shift. ML offers tools allowing for data analysis which are unprecedented in terms of their potential for managing large quantities of data and uncovering new correlations and trends difficult or impossible for humans to discover. Furthermore, the models now, as opposed to traditional, statistical ML, work with unstructured data, having capability to process high volumes and variety of data to produce a wide range of inferences, in particular about individuals.

Big Data

The AI models described are able to process 'data with high volume, velocity and/or variety', ie Big Data.[20] The volume of Big Data is significant, usually in excess of terabytes, and is continuously expanding.[21] 'Velocity' describes dynamic data generation, creation and modification requiring high processing speeds.[22] 'Variety' of data 'refers to the fact that data will not all lie within a single database architecture'[23] and includes 'large volumes of structured and unstructured data [held] in different formats from which insights may be drawn'.[24] For example, it is possible to link different forms of data such as images, text, audio and video files, and numbers.[25]

2.2. Use of AI and Big Data in Retail Financial Services

The properties of the technologies described promise important beneficial capabilities for the industry. The technology uptake within the industry is growing, with new FinTech market entrants quite literally enabled by the

---

-reminder-that-machine-learning-is-about-correlations-not-causation/?sh=5f2b93d66161> accessed 26 May 2021.

20 Guihot and Bennett Moses (n 14) 9, citing Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* (Sage Publication Ltd, 2014) 68.

21 Terabyte is 2^{40} bytes, see OECD (n 11) 10; Rob Kitchin and Gavin McArdle, 'What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets' (2010) Jan-Jun *Big Data and Society* 1, 6.

22 Guihot and Bennett Moses (n 14) 76.

23 ibid 9.

24 ibid.

25 Kitchin (n 20) 77.

technological advancements, and more traditional incumbents, including banks and insurers, quickly catching up.[26]

Due to 'entrenched corporate secrecy practices and a consequential lack of transparency',[27] some of the data practices and harms mentioned in this chapter are as yet unconfirmed in a financial services context. Also, some of the examples are likely to be much less complex than the reality. The corporate secrecy around AI models and data used by financial firms makes it even more challenging for policymakers and regulators to adequately address emerging issues, including potential consumer harms.

Surveys indicate the great majority (85 %) of financial services firms, including banks, investment firms and insurers, use some forms of AI.[28] Financial services, as a data-rich industry, benefit from a wide variety of applications of the technology. Our focus in this chapter is the automated decision-making affecting consumers. It is already considered a standard practice to use Big Data analytics for consumer credit scoring and lending.[29] Emerging evidence also suggests insurers are increasingly engaging in using ML models for underwriting of contracts.[30]

2.3. (Concerning) Characteristics of the Technologies

AI (in particular ML tools) used in Big Data analytics often presents certain characteristics that can be concerning, especially in the context of decision-making processes affecting consumers of financial services. The most relevant issues for our discussion are the opacity of ML models and the potentially inaccurate inferences they produce.

Opacity

The *opacity* (or lack of *transparency*) of many AI and Big Data processes has attracted significant attention. This attention arises particularly in contexts

26 CCAF (n 2) 11.

27 Kayleen Manwaring, 'Will emerging information technologies outpace consumer protection law? The case of digital consumer manipulation' (2018) 26 *Competition and Consumer Law Journal* 141, 180.

28 CCAF (n 2) 25.

29 Blumberg and others (n 3).

30 European Insurance and Occupational Pensions Authority (EIOPA), 'Big Data Analytics in Motor and Health Insurance: A Thematic Review' (Report, 2019) 29–41.

where those processes are used to make decisions resulting in social consequences, such as a decision to grant a loan or insurance. Three types of opacity seen in AI models can be distinguished:[31]

1. an opacity resulting from deliberate corporate secrecy, for reasons such as protecting trade secrets, limiting 'gaming', and avoiding scrutiny and/or regulation of dubious activities;[32]
2. 'technical illiteracy', as most people lack specialist skills required to understand algorithmic design; and
3. opacity due to complexity arising out of:
   (a) multi-component systems; and
   (b) interplay between large datasets and the way the model processes data: complex ML models are notable for the difficulty or even impossibility to understand why a decision was made, or outcome arrived at, even by the original programmer.[33]

(In)accuracy of Inferred Information

ML models have been shown to be capable of inferring things such as a person's sexual orientation from their face photos,[34] or a person's suicidal tendencies from their posts on Twitter.[35] However, a question arises as to accuracy of such predictions. Models operate on correlations between input data and target variables, rather than confirming a causal relationship between them.[36] Consequently, where certain features of a person or their behaviour *correlate* statistically with a ML model's desired outcome, this

31 Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 *Big Data & Society* 1, 3–5.

32 See Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).

33 Eg the Deep Patient ML system was able to come to accurate predictions of schizophrenia in patients, but the developers have admitted they do not understand how it arrives at its predictions. Will Knight, 'The Dark Secret at the Heart of AI' (2017) 120 *MIT Technology Review* 54, 57.

34 Yilun Wang and Michal Kosinski, 'Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images' *OSF* (Research Project, updated 26 May 2020) <https://osf.io/zn79k/>.

35 Bridianne O'Dea and others, 'Detecting Suicidality on Twitter' (2015) 2 *Internet Interventions* 183.

36 Anya E. R. Prince and Daniel Schwarcz, 'Proxy Discrimination in the Age of Artificial Intelligence and Big Data' (2020) 105 *Iowa Law Review* 1257, 1263–64.

does not mean the outcome is correct for a specific individual. Accuracy is also heavily dependent on training data provided.[37]

3. Challenges to Financial Law and Regulation

3.1. Overview of Potential Consumer Harms

AI and Big Data technologies used in automated decision-making in the context of retail financial services may lead to consumer harm. Several reasons for this can be identified. First, harm may partly stem from characteristics of the technology discussed, such as opacity and unreliable inferences. Second, new technologies are opening doors to new possibilities in terms of financial products being offered, especially personalised products, which may affect consumers in negative ways. Third, use of technologies and the promised benefits incentivises wide-reaching collection of consumers' data by financial firms, which again may (potentially) have negative consequences for consumers. We discuss specific instances of consumer harm below.

Various areas of law and regulation can potentially address some harms. In many cases current rules, when applied to factual scenarios arising in the context of the use of AI and Big Data analytics, should provide a high level of consumer protection. Areas of potential relevance include:

- financial services law, applying to consumer contracts such as banking contracts, insurance, investment contracts, and especially rules requiring consumer-centric approaches to design, advertising and selling of financial products;
- consumer protection rules, especially rules:
  - introducing fairness standards for treatment of consumers, either generally, or specifically in the financial services context (including concepts such as 'good faith' and 'utmost good faith', 'fair dealing', 'fairness', etc);
  - protecting consumers from unfair commercial practices, misleading conduct, and related concepts;
  - related to consumer contracts in general, including formation, information duties, withdrawal or termination, online contracting;

37 Guihot and Bennett Moses (n 14) 31-41.

- privacy and data protection rules, including rules aimed at providing consumers with information and control over automated processing of their data;
- anti-discrimination laws, relevant to provision of financial services to consumers.

Sometimes, however, current law and regulation may be inadequate in addressing some potential harms. There are two reasons for this. First, it may be because use of new technologies exacerbates issues arising previously or independently from technology use. For instance, if financial services firms have already been engaged in misconduct harming consumers,[38] either by breaking the law or taking advantage of legal loopholes, there are reasons to believe they will continue doing so, especially where technology makes such conduct easier to hide, cheaper, or more efficient. The examples discussed below, in particular regarding algorithmic bias and discrimination, and excessive data collection, provide useful illustrations.

Second, use of this technology by the financial services industry can also bring about new challenges for consumer protection legal frameworks. For example, certain uses of technology can enable firms to manipulate consumers more efficiently and in new ways. It can also provide means to personalise financial services to a point not possible before. Although this may benefit some consumers on price or terms, others may find themselves totally excluded from accessing financial services such as insurance or bank loans.

3.2. Algorithmic Bias and Discrimination

A concern often raised in the context of AI tools being used for decision-making is the possibility of algorithmic bias and resulting discrimination.[39] Discrimination in provision of financial services is not strictly related to the use of AI models. It is actually an 'old' problem,[40] but it can potenti-

38 Systemic misconduct of financial services firms towards consumers has been evidenced, eg, in Australia, see Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, 'Final Report' (1 February 2019).

39 Centre for Data Ethics and Innovation (CDEI), 'Review into Bias in Algorithmic Decision-Making' (Report, November 2020) 21; Eirini Ntoutsi and others, 'Bias in Data-Driven Artificial Intelligence Systems: An Introductory Survey' [2020] *WIREs Data Mining and Knowledge Discovery* 1, 2.

40 See eg practices such as 'redlining': Robert Barlett and others, 'Consumer-Lending Discrimination in the FinTech Era' (2019) National Bureau of Economic

ally be *exacerbated* through use of new technologies.[41] With the increasing volume of data held by financial services firms, rapid technological advancements and promised benefits, more and more consumers may become affected.[42]

Algorithmic bias can result from perpetuating human biases embedded in datasets used for training and testing of models.[43] For example, historically women were underrepresented in banks' clients bases. Men would traditionally be the income earners, consequently using bank services such as loans. A ML model trained on such historic data could therefore learn that more loans, with lower default risk, were granted to men, and then reproduce this in its outcomes.

Use of AI models may also lead to creating new biases. Even where a 'protected attribute' under discrimination law has been removed from an automated decision-making algorithm, where the attribute correlates with a particular risk on historical data, AI-enabled tools may nevertheless find proxies for this protected attribute, and outcomes will be based on these proxies.[44] These may be more difficult to discover than decisions based directly on the protected attribute. For example, if data processed by an AI model discovered a correlation that people with a commonly protected attribute, such as a disability, were more likely to default on a loan, the model may base its decisions on the *proxies* for disability found in the dataset. These could be very diverse information items, such as

Research Working Paper 25943, 5 <https://www.nber.org/papers/w25943>, and 'cherry-picking' and 'lemon-dropping': Marshall Allen, 'Health Insurers Are Vacuuming Up Details About You: And It Could Raise Your Rates', *NPR* (17 July 2018) <https://www.npr.org/sections/health-shots/2018/07/17/629441555/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates> accessed 26 May 2021.

41 Australian Human Rights Commission (AHRC), 'Using Artificial Intelligence to Make Decisions: Addressing the Problem of Algorithmic Bias' (Technical Paper, 2020) 26, 31, 40; Prince and Schwarcz (n 36) 1267–68; CDEI (n 39) 7; Frederik J. Zuiderveen Borgesius, 'Strengthening Legal Protection Against Discrimination by Algorithms and Artificial Intelligence' (2020) 24(10) *The International Journal of Human Rights* 1572, 1577; Ntoutsi and others (n 39) 9.

42 CDEI (n 39) 24.

43 AHRC (n 411) Scenarios 2 and 3.

44 ibid 32; Prince and Schwarcz (n 36) 1273.

membership in certain Facebook groups,[45] grocery shopping history,[46] or Google search history.

The risk of algorithmic bias is exacerbated by lack of reliable datasets for training and testing of models. Ironically, this derives in part from operation of data protection rules requiring anonymisation or de-identification of data to protect individual identity.[47] This often results in sensitive or protected attributes, such as gender-, health-, or ethnicity-related data being removed, which means bias may become unmeasurable.[48]

However, two considerations need to be made. First, some form of discrimination, and especially indirect discrimination,[49] will almost always exist in any decision-making procedure,[50] including automated decision-making. Second, some types of discrimination are not always unlawful, due to exemptions for industries such as insurance.

3.3. Excessive Data Collection

There is growing evidence that various organisations, including financial services firms, are obtaining consumers' data from external sources.[51] Such

45 Moana Mononoke and Fred Trotter, 'Strict Inclusion Closed Group Reverse Lookup (SICGRL) Attack', *Missing Facebook Patient Consent* (Report, 16 February 2019) <https://missingconsent.org/downloads/SicGRL_initial_report.pdf>.

46 See eg observations made in Australian Competition and Consumer Commission, 'Customer Loyalty Schemes' (Final Report, December 2019) 45ff.

47 Christine M O'Keefe and others, 'The De-Identification Decision-Making Framework' (CSIRO Data61 Report, 18 September 2017) 18–20.

48 This is a very real-life problem, as the example of Onfido, a company providing remote biometric identity verification technology for banks, demonstrates: Information Commissioner's Office UK, 'Regulatory Sandbox Final Report: Onfido' (A summary of Onfido's participation in the ICO's Regulatory Sandbox Beta, September 2020).

49 Which is when a seemingly neutral rule leads to discriminatory outcomes, see eg European Court of Human Rights, 'Guide on Article 14 of the Convention (Prohibition of Discrimination) and on Article 1 of Protocol No. 12 (General Prohibition of Discrimination)' (Report, updated 31 December 2020) 11–12.

50 And especially in processes such as underwriting of insurance, Anti-Discrimination Working Group of the Actuaries Institute, 'The Australian Anti-Discrimination Acts: Information and Practical Suggestions for Actuaries' (Paper Presented to the Actuaries Institute 20/20 All-Actuaries Virtual Summit, 3-28 August 2020) 28.

51 See eg Mohammed Aaser and Doug McElhaney, 'Harnessing the Power of External Data', *McKinsey Technology* (3 February 2021) <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/harnessing-the-power-of-external-data> accessed 26 May 2021.

external sources may include, for example, consumers' social media, Internet browsing history, website cookies, retail loyalty schemes, credit cards, smartphone applications, wearable devices, connected cars, smart home devices, voice assistants such as Alexa – the list is potentially endless. Financial firms may directly engage in collection of such data, which includes practices such as sharing of data between various entities belonging to the same company group or aggregating and repurposing information collected previously. They may also purchase consumers' data from data brokers.[52]

The financial services industry has always been concerned with data analytics and statistics, and it has quickly adopted the new technologies. AI models need huge amounts of data to work, as they become increasingly accurate with more training and testing data available. The reverse is also true: AI models provide means to analyse massive amounts of data and create value for corporations.

Such large-scale data collection presents important challenges for privacy and data protection regimes. Various questions arise, such as:

- how consumers' data should be collected;
- to what extent consumers should be able to control what happens to their data;
- whether sharing of personal data can be a condition of access to services; and
- how re-identification of data should be treated.

These issues, already of concern in online advertising,[53] are becoming increasingly relevant in the context of financial services.

Data collection from external sources also raises ethical questions. AI tools make it possible to analyse data without an easily identified link to customer's financial value, such as peoples' lifestyles, hobbies, and behaviours.[54] They may infer, and thus reveal, facts that individuals would prefer to keep private, for example their sexual orientation,[55] mental health

52 Wolfie Christl, 'Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze,
Trade, and Use Personal Data on Billions' (Report by Cracked Labs, Vienna, June 2017).

53 See eg Forbrukerrådet, 'Out of Control: How Consumers Are Exploited by the Online Advertising Industry' (Report, 14 January 2020).

54 Allen (n 40).

55 See Wang and Kosinski (n 34).

issues,[56] or pregnancy.[57] Finally, abundant data collection potentially exposes the data, including inferences, to cyber security breaches.[58]

3.4. Digital Consumer Manipulation

There is a concern that increasing use of AI and Big Data tools will support a significantly increased capacity not only to discover consumer preferences, but also to use data combined with insights from behavioural research to *exploit* consumer vulnerabilities, emotions and individual cognitive biases for commercial benefit. This type of 'digital consumer manipulation'[59] may be used to manipulate consumers to buy particular products or services, hand over additional data, pay higher prices or recommend particular brands to other consumers.

In a financial services context, digital consumer manipulation may take the form of 'margin optimisation', a 'process where firms adapt the margins they aim to earn on individual consumers'.[60] Reviews of EU, UK and US insurance firms' practices demonstrated how, when setting prices, firms may look at a consumer's willingness to pay based on their personal characteristics gained from the insights that external data provides.[61] The use of data analytics means that the firms, instead of taking into account the cost a consumer generates for the firm, examine the consumer's price sensitivity and propensity to switch to a different product. This may be inferred by an AI model from, eg, the analysis of consumers' behaviour on a website or app controlled by the financial firm, the time an individual spends reading terms and conditions, or websites visited before applying

56 See O'Dea and others (n 35).

57 Brigid Richmond, 'A Day in the Life of Data: Removing the opacity surrounding the data collection, sharing and use environment in Australia' (Consumer Policy Research Centre Report, 2019) 34 describes how US retailer Target inferred a customer's pregnancy based on shopping history and sent them pregnancy- and baby-related advertising and products.

58 Kayleen Manwaring and Pamela Hanrahan, 'BEARing responsibility for cyber security in Australian financial institutions: The rising tide of directors' personal liability' (2019) 30 *Journal of Banking and Finance Law and Practice* 20, 25.

59 Manwaring, 'Will emerging information technologies outpace consumer protection law?' (n 27). See also Ryan Calo, 'Digital Market Manipulation' (2014) 82 *George Washington Law Review* 995.

60 Financial Conduct Authority UK, 'General Insurance Pricing Practices: Interim Report' (Market Study MS18/1.2, October 2019) 21.

61 ibid, EIOPA (n 30) 12, 39.

for (or enquiring about) a financial product. This type of conduct by financial firms is particularly concerning for regulators, as it may amount to unfair pricing or unfair commercial practices in some jurisdictions.[62]

3.5. Personalisation of Financial Services

Personalisation of financial services is hailed as one of the main benefits, both to consumers and financial firms, that advancements in data analytics can provide, as consumers will be offered products tailored to their needs.[63] However, for 'lower value' customers, it may create additional difficulty in accessing financial services.

Consumer insurance contracts provide a useful example. Greater granularity and availability of data, paired with means to analyse it, translates into a possibility of individualised risk assessment of prospective insureds. In voluntary lines of insurance, this in turn may lead to a situation in which insurance firms will only offer insurance to consumers who present very low risk and exclude those who may potentially generate higher costs.[64] However, these excluded customers may be in most need of insurance. Similar scenarios could occur in context of other financial services, such as loans, as consumers who need the loan most, will be least likely to have it granted.

Clearly, a delicate balance must be struck with rules relative to responsible lending or, more generally, provision of fit-for-purpose financial services for consumers. The problem, however, lies in the fact that using AI and Big Data tools may bring about such granular assessment of individuals, that affordability of financial services offered to them, and ultimately their access to financing, investment, and insurance, may be inappropriately limited. What makes this potentially worse is when the automated decision-making process is opaque and possibly discriminatory or based on inaccurate inferences produced by an AI model.

62 ibid.
63 CCAF (n 2) 32.
64 EIOPA (n 30) 30; Financial Conduct Authority UK, 'Sector Views' (Report, 2020) 35.

4. Conclusions

Sociotechnical change does not arise in a regulatory vacuum, so much of it will be regulated under current rules. Legislative overreaction to sociotechnical change runs the risk of restricting beneficial innovation. Nevertheless, some rules in the new context may be under- or over- inclusive, uncertain, or sometimes the change is so truly new that it may amount to an unregulated 'new harm'.[65] Therefore any legal and regulatory framework should allow and promote courts, legislators and other rulemakers to be both swift and flexible in their responses to sociotechnical change, particularly in development and application of legal rules,[66] and the provision of accessible opportunities for consumer redress. Rules that aim to prevent consumer harm in a traditional setting should be interpreted, as much as possible, to achieve that rationale in a new sociotechnical reality.

Some of the harms discussed may not be intentional. For example, algorithmic bias and resulting discrimination may be difficult to discover due to ML opacity and be unintended by well-meaning financial services firms using AI and Big Data tools. This lack of intention may or may not have legal consequences, depending on the context and relevant legal system and applicable rules. For example, the law may impose specific consequences when harm is inflicted knowingly, or with an intention to profit from, and a disregard for the interests of, affected individuals. However, intention in some cases may be irrelevant. Therefore, financial services firms must be particularly diligent in implementing these technologies to avoid situations in which consumer harms may arise.

Use of emerging technologies brings about a risk of various harms to consumers. These harms are especially concerning in the context of retail financial services, where discrimination and digital manipulation may result in financial exclusion, disproportionately affecting already disadvantaged and vulnerable consumers. As AI and Big Data tools bring significant gains to financial firms, expectations of their conduct and the fairness of decision-making processes they implement increase.

The digital transformation of financial services, including the use of advanced AI and Big Data tools is here to stay. Policymakers, regulators and courts, in addition to industry bodies and associations, need to be

65 Lyria Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (2007) 2 *University of Illinois Journal of Law, Technology & Policy* 239, 269.

66 Manwaring, 'Will emerging information technologies outpace consumer protection law?' (n 27).

ready to deliver a legal and regulatory framework that is fit for purpose, and allows both financial firms and consumers to reap the benefits of the technological revolution.