

EBA/DP/2016/01

04 May 2016

Discussion Paper

on innovative uses of consumer data by financial institutions

Table of contents

Table of contents	2
Practical information	3
Executive summary	4
Background	5
Scope	9
Legislative frameworks applicable to data protection	11
Description of the phenomenon	14
Sources of data	15
Purpose of data	16
Potential benefits	19
Benefits to consumers	19
Cost reductions	19
Improved product quality	20
Benefits to financial institutions	20
Reduction of costs	21
New sources of revenue	21
Risks	23
Risks to consumers	23
Information asymmetries	23
Misuse of the data	24
Data security	25
Risks to financial institutions	27
Reputational risks	27
New entrants in the market	27
Data security	28
Risks to the integrity of the financial sector	29

Practical information

EBA welcomes comments on this Discussion Paper on innovative uses of consumer data and in particular on the specific questions set out in this paper.

Comments can be sent by clicking on the 'send your comments' button on the consultation page of the EBA website. Please note that the deadline for the submission of comments is 4 August 2016. Comments submitted after this deadline, or submitted via other means may not be processed.

Comments are most helpful if they:

- a. respond to the question stated;
- b. indicate the specific question or point to which a comment relates;
- c. are supported by a clear rationale; and
- d. provide evidence to support the views expressed/ rationale proposed.

It is important to note that although you may not be able to respond to each and every question, the EBA would encourage partial responses from stakeholders on those questions that they believe are most relevant to them.

All contributions received will be published following the close of the consultation, unless you request otherwise by ticking the relevant box in the consultation form. If you request that your response is treated as confidential, it will not be published in the EBA website, or shared with any third parties.

Please note that a request to access a confidential response may be submitted in accordance with the EBA rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA Board of Appeal and the European Ombudsman.

Executive summary

The founding regulation of the European Banking Authority mandates the EBA “to monitor new and existing financial activities” and “to adopt guidelines and recommendations with a view to promoting the safety and soundness of markets and convergence in regulatory practice”.

In order to fulfil its mandate, the EBA continuously monitors innovations in financial markets, with a view to ensuring that market actors engaging in such innovations can do so with confidence. Consumers in particular need to have confidence before innovation can succeed and be sustained, by innovators and markets operating according to rules and procedures that are transparent, fair, and free from manipulation, conflicts of interest, or other shortcomings.

One of the innovations that the EBA has been monitoring more recently is the innovative uses of consumer data by financial institutions. Financial institutions have always used the data that consumers provide in various ways. However, in recent years some financial institutions have started using such data in innovative ways and have done so across the EBA’s regulatory remit comprising mortgages, personal loans, payment accounts, payment services, and electronic money. Also, new entrants in the market, such as fintech or large digital companies, have been seen to use consumer data in a way that may change the way the market will evolve in the coming years.

Payment data, among other types of consumer data, is of particular interest to the EBA because consumers engage in payment transactions often, and do so each time they pay for the purchase of products and services through their payment accounts or payment cards. Unlike other, one-off types of data provided by consumers, payments data therefore provides financial institutions with a continuous insight into consumers’ purchasing habits and preferences.

This Discussion Paper identifies the risks and potential benefits of innovative uses of data to consumers, financial institutions, and financial integrity more widely. For the purposes of this assessment, the use of consumer data encompass the collection, processing and storage of data, including aggregation tools and other data processing technologies. Potential benefits identified by the EBA include cost reductions, improved product quality, and new sources of revenue for financial institutions, whereas the risks identified consisted of information asymmetries, the misuse of data, data security, as well as reputational risks for financial institutions.

Although general provisions apply to financial institutions on secrecy and conduct and on data protection that impose restrictions to the use of consumer data, only few requirements presently exist in EU legislation specific to the financial sector that address the use of consumer data by financial institutions. The EBA hopes that the responses to this Discussion Paper will allow it to make a better informed decision on which, if any, regulatory and/or supervisory actions are needed to ensure that the regulatory framework mitigates the risks while also allowing market participants to harness the benefits from the innovation.

Background

1. When the European Banking Authority (EBA) was established in 2011, its founding regulation conferred on the authority the mandate “to monitor new and existing financial activities” and “to adopt guidelines and recommendations with a view to promoting the safety and soundness of markets and convergence in regulatory practice”.¹ The mandate was a reflection of the fact that many of the financial innovations that had emerged in the previous decade were greeted as beneficial initially but later turned out to have significant detrimental effects, on consumers, investors, the financial system, and society overall. One of the many lessons learned from the financial crisis that ensued was that benefits arise, not from innovations as such but from innovations that are sustainable, that is: that do not result in undesirable outcomes or other negative externalities.²
2. In order to fulfil its mandate, the EBA continuously monitors innovations in financial markets, with a view to ensuring that market actors engaging in such innovations can do so with confidence. Consumers in particular need to have confidence before innovation can succeed and be sustained. There are limits to the ability of consumers to protect themselves in their dealings with financial institutions. So, when engaging in innovations, they need assurance that the innovator and markets operate according to rules and procedures that are transparent, fair, and free from manipulation, conflicts of interest, or other shortcomings.
3. Financial innovation has a broad meaning and encompasses not only innovative products and services but also processes, functions, conduct, and distribution channels through which financial institutions bring their products and services to the market. It is therefore generally not helpful to attempt to treat financial innovation as a singular phenomenon, for which an equally singular regulatory approach would then suggest itself. Rather, various approaches will evolve that are attuned to the nature and incidence of particular innovations. As such, the EBA’s approach to financial innovation examines innovations on a case-by-case basis, in the context of a standardised methodological framework.
4. At the EBA, that methodological framework comprises a sequence of analytical steps, including:
 - a. identify the potential benefits of digital technologies, to consumers, to financial institutions, to the financial system, to society more widely;
 - b. identify and assess the risks, not only those arising for consumers but also for financial institutions, market confidence; and, depending on the nature of the

¹ See Article 9(2) of Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority) at

<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010R1093&from=EN>.

² OECD (2009), *Regulatory Issues Related To Financial Innovation*, p. 2.

- innovation, to financial integrity such as anti-money laundering and the prevention of financial crime, and financial stability;
- c. prioritise the risks, in order to identify which ones can be left to market participants to address, and which ones do indeed require a regulatory response;
 - d. develop a regulatory response that is technology neutral and strikes an appropriate balance between the competing demands of mitigating risks and harnessing the benefits;
 - e. assess the extent to which some risks are potentially already addressed in existing EU legislation; and
 - f. analyse whether the particular innovation requires a standardised approach across the EU or whether it can be left to Member States and national authorities. While it is true that many innovations are internet-based, therefore travel easily across borders, and that a prima facie case for a harmonised approach therefore exists, a proper assessment should be carried out notwithstanding.
5. A key step is for the EBA to assess the benefits and risks of the financial innovations it monitors, with a view to determine which, if any, actions may be needed to ensure that the regulatory framework mitigates the risks while also allowing market participants to harness the benefits from the innovation. The identification of risks is important because, while exposure to risk is inherent in innovative (and indeed any economic) activity, it is the identification, sound management, and mitigation of such exposures that offers benefits to individuals, enterprises and the economy as a whole. Put differently, the benefits will be able to materialize only to the extent that risks are shifted to actors that have the knowledge and ability to bear them.
6. One of the innovations that the EBA has been observing, and which is the subject matter of this Discussion Paper, is the innovative uses of consumer data by financial institutions. Financial institutions, like market players in other sectors of the economy, have always used the data that consumers provide to them in various ways, either directly or indirectly.
7. However, in recent years some financial institutions have started using such data in innovative ways. For example, some financial institutions combine consumer data that they hold internally with data obtained from external sources, such as public or private companies (e.g. data vendors) and social media. In the process, consumer data is in itself used as an asset in the provision of financial services. For example, some banks are offering shopping discounts to consumers, based on their buying behavior, although consumers may not realise how personal the data being shared between financial institutions and any third parties is.³

³ Which? Magazine, September 2015, p. 18-21.

Studies report increased investment in consumer data analytics, i.e. extensive collection and further processing of personal information, across the board.⁴

8. Furthermore, financial institutions have been seen to be responding to the increased importance of data more generally, by changing their internal governance, for instance: 16% of financial institutions responding to a recent survey carried out within the industry reported to have already appointed a “Chief Data Officer”, against 14% for telecommunication companies, 11% for healthcare and 10% for consumer goods companies. Also, 79% of financial services executives believe that the ability to extract value from data is an important factor in their future success.⁵
9. Social networks, search engines and large retailers aside, financial institutions arguably possess the largest amount of data about their consumers. Banks, in particular, hold a large amount of data, including structured data (such as credit card payments, money withdrawals, and account balance check via smartphones); semi-structured data (such as emails, and browsing history); and non-structured data (such as through their call centres, or exchanges between consumers and advisers)⁶. And if some analyses are to be believed, the amount of data will grow further still in the years ahead, with the development of connected objects that banks will integrate in their mobile services.⁷
10. More specifically, banks own a very valuable type of consumer data: payment data, i.e. data that results from consumers engaging in commercial transactions and paying for the purchase of products and services through their payment account. Today, a large amount of payments is done through electronic processes (e.g. credit and debit transfers, card payments) and gives financial institutions an extensive insight into their consumers’ purchasing habits and preferences.⁸
11. The payment services sector in the EU is also in the process of a major transformation that will arguably further increase the use of consumer data. The Payment Services Directive 2

⁴ See, for instance, “Big Data Alchemy: How can Banks Maximize the Value of their Customer Data?”, Cap Gemini, https://www.capgemini-consulting.com/resource-file-access/resource/pdf/bigdatainbanking_2705_v5_0.pdf.; and “Big Data, Big Banks and Unleashing Big Opportunities”, NG Data, <https://www.aba.com/Tools/Offers/Documents/NGDATA%203.pdf>.

⁵ Data retrieved from ‘Stewarding data: Why financial services firms need a chief data officer’, Capgemini Consulting and Efma, May 2015, at: https://www.capgemini-consulting.com/resource-file-access/resource/pdf/cdo_12-15_v7_0.pdf

⁶ References to structured, semi-structured and unstructured data can be found in “Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics”, ENISA, December 2015, p. 42, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-data-protection/at_download/fullReport.

⁷ See: “Quand DATA MINING rime avec big data et open source”, Point Banque magazine, 1 July 2015; also at <http://www.data.net.ma/index.php/2015/08/04/quand-data-mining-rime-avec-big-data-et-open-source/>.

⁸ See, for instance, data on the total number of transactions based on cashless payments (2010), in “Innovations in retail payments”, Committee on Payment and Settlement Systems, Bank for International Settlements, May 2012, p. 59, <http://www.bis.org/cpmi/publ/d102.pdf>.

(PSD2)⁹, which entered into force on 13 January 2016 and will apply from 13 January 2018 onwards, will regulate two new types of payment services: payment initiation services (PIS), and account information services (AIS) – and will subject their providers to licensing and other supervisory requirements.

12. AIS services in particular involve the use of consumer data. These services already exist today but are expected to proliferate even further once they are subject to the requirements in the PSD2, through financial technology (fintech) companies that specialise in data gathering and processing, or regulated financial institutions.
13. The EBA is issuing this Discussion Paper in order to find out from market participants whether the innovative uses of consumer data that it has identified are comprehensive, reflect current practices, and whether the risks and potential benefits are fairly reflected. The EBA will assess the responses to this Discussion Paper, with a view to refine its assessment and make a better informed decision on which, if any, steps it should take.
14. The Discussion Paper starts by outlining the scope of the work, and the existing legislative frameworks applicable to data protection, before presenting the description of the phenomenon as observed by the EBA. It then presents a preliminary assessment of the potential benefits and risks associated with the use of consumer data by financial institutions, for consumers, financial institutions and the integrity of the financial sector. Benefits and risks are presented in a way that does not exclude that some features of innovation may be benefits as well as risks. Readers are invited to confirm or challenge the views expressed by the EBA, and specific questions are presented at the end of each chapter.

⁹ Directive (EU) 2015/2366, of the European Parliament and the Council, of 25 November 2015, on payment services in the internal market), <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN>.

Scope

15. This Discussion Paper is focused on the phenomenon of financial institutions using consumer data, obtained directly and/or indirectly from consumers, and/or from external sources, in an innovative way. Innovative uses of data include financial institutions using consumer data in the provision of “traditional” financial services, such as granting credit¹⁰; or in the provision of new types of services, such as offering tailored products to consumers. This data may also be shared with third parties.
16. For the purposes of this DP, consumer data can be structured, semi-structured or unstructured and include:
- a. ID details, such as first and last name, citizenship, nationality, place of birth, date of birth, age, gender, marital status, number of children and/or dependants;
 - b. Contact details, such as home address, telephone number, e-mail address, geolocation;
 - c. Browsing history, IP address, log data, call activity, and messaging data;
 - d. Property ownership details, such as type of housing, ownership status of housing;
 - e. Education and professional details, such as education degree, occupational status (self-employed or dependent), sector of employment, employer, job title, revenue or monthly net income, commencement of employment;
 - f. Other types of semi-structured sensitive personal information¹¹;
 - g. Hobbies; sports; other personal interests;
 - h. Multimedia, such as, audio, video and images data;
 - i. Social network information (including data on a person’s social connections and information provided in status updates).
17. More specifically, consumer data of a financial nature can include:

¹⁰ For instance, financial institutions may use new types of data, such as social networks data, for creditworthiness assessment. While creditworthiness assessment is a legal requirement for financial institutions, the fact that new types of data may be used by financial institutions to comply with this obligation is relevant and is included in the scope of this Discussion Paper.

¹¹ To this regard it is important to note that article 8(1) of the Data Protection Directive states that “Member States shall prohibit the processing of personal data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, of genetic data or of data concerning health or sex life”. See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.

- a. Data on the consumer's financial involvement, such as number of accounts held with the financial institution; account balance(s); account limits; information on other products purchased from the same financial group; data from financial advice;
 - b. Data on the consumer's credit profile, such as information about consumers' solvency and credibility; existent loans; court judgments; credit file search history; overdrafts; interest paid; payment performance; and defaults;
 - c. Data on consumer's habits as regards banking services, such as payment data (including patterns, purposes and history); certain account movements; number of credit transfers executed to a person/firm; number and identification of authorised direct debits collectors;
 - d. Data related to customer services, such as complaints details, customer queries details; information collected through internal satisfaction surveys; and
 - e. Data on the communication between the consumer and the financial institution, such as communication data, communication channel, clicks on topics on the financial institution's website.
18. For the purposes of this Discussion Paper, "financial institutions" refers to financial institutions that fall within the remit of the EBA, as stated in its founding Regulation, which are credit institutions, creditors, credit intermediaries, financial conglomerates, payment institutions and e-money institutions.
19. The 'use' of consumer data, in turn, encompasses the following:
- a. the collection of data;
 - b. any processing of data, including through aggregation tools and other data processing technologies; and
 - c. the storage of data.
20. This includes the processing of data *initially* collected by financial institutions to fulfil legal obligations, such as reporting obligations under Anti-Money Laundering regulations or tax regulations.

Legislative frameworks applicable to data protection

21. Only few requirements presently exist in sectoral EU financial legislation or regulation that specifically address the use of consumer data by financial institutions.¹² Nevertheless, there are general provisions applicable to financial institutions on secrecy and conduct. Banking secrecy rules, for example, impose restrictions to the use of consumer data by financial institutions.¹³
22. Additionally, financial institutions are also bound by an existing body of EU law in the areas of consumer protection, personal data protection, electronic commerce and advertising/sales promotions that companies already have to comply with. Most of this is horizontally applicable. This includes, inter alia, the Data Protection Directive 95/46/EC, soon to be replaced by the General Data Protection Regulation, the Directive on Electronic Communications and Privacy, the Unfair Commercial Practices Directive, the E-Commerce Directive, the Directive on Unfair Contract Terms, and the Directive on Distance Marketing of Financial Services.
23. Sector-specific financial services-specific legislation, such as the Payment Services Directive, the Consumer Credit Directive, the Mortgage Credit Directive, and the Payment Accounts Directive, also touch upon the collection and processing of consumer data for marketing and sales purposes.
24. This Discussion Paper acknowledges that the types of tools used by financial institutions to process data might be impacted by these requirements and the limits imposed by the above-mentioned European and/or national legislation or regulation. In general, it can be argued that, for instance:
 - a. Where consumers have given their informed consent to their personal data being used by financial institutions for a specific purpose (i.e. they have opted in), their individual data may be processed for that purpose, but must not be used for additional, incompatible purposes;

¹² See article 94(2) of PSD2: “Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user”. In PSD2 see also article 66 (2) (b) and (g), for payment initiation services; and article 67 (2) (b) and (e) for account information services.

¹³ See, for instance, article 62 of the Capital Requirements Directive IV; and article 172(1)(e)(iii) of the Capital Requirements Regulation.

- b. If consumer data is anonymised in a way that prevents re-identification of consumers, data is no longer personal and thus consent is not relevant;¹⁴
 - c. Consumers have the right to access, modify or delete their personal data stored by financial institutions.
25. While the topic of innovative uses of consumer data by financial institutions may be primarily seen as a personal data protection topic, there are many interlinkages between financial supervision, consumer protection and data protection, which explain why the EBA has an interest in the phenomenon, such as:
- a. the fact that society attaches particular importance to, and is sensitive about, the use of data by financial institutions, and therefore financial institutions, particularly banks, are held to higher standards than other (non-financial) organisations, especially with regard to data protection and privacy. Societal expectations regarding the use of consumer data towards financial institutions may be higher than towards other firms because the risks and loss to consumers can be significantly higher;
 - b. the fact that the services provided by financial institutions are regarded by some consumers as public services/utility functions, where the transaction data is a by-product that society would not want to see being used lightly for purposes other than the ones it was disclosed for (e.g. data provided by consumers to banks when opening a bank account);
 - c. from a prudential and conduct supervision perspective, trust in individual financial institutions and/or in the financial sector as a whole can be significantly undermined by incidents related to data protection and privacy involving financial institutions;
 - d. the potential increase of innovative use of consumer data may have medium and long term consequences, such as the transformation of financial institutions' business models and the accentuation of competition among them and with new entrants such as fintech, large international digital companies or telecommunication operators.
26. Against this background, the Discussion Paper focuses on the instances of innovative uses of consumer data by financial institutions and does not, for now, include a legal assessment of

¹⁴ According to the European Union Agency for Network and Information (ENISA), "anonymization refers to the process of modifying personal data in such a way that individuals cannot be reidentified and no information about them can be learned". See: "Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics", December 2015, p. 27, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-data-protection/at_download/fullReport.

See also: Opinion 05/2014 on Anonymisation Techniques by the Article 29 Data Protection Working Party, April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

the extent of their compliance with any legislative and/or regulatory requirements related to, for example, data protection.

27. Finally, the analysis of the responses to this DP will feed into some aspects of the work the EBA will carry out jointly with the European Securities and Markets Authority (ESMA) and the European Insurance and Pensions Authority (EIOPA) later in 2016 on the related topic of 'Big Data'.¹⁵

¹⁵ 2016 Work Programme of the Joint Committee of the European Supervisory Authorities, October 2015, p.2, <https://www.eba.europa.eu/documents/10180/15736/JC+2015+055+Joint+Committee+Work+Programme+2016.pdf>.

Description of the phenomenon

28. The multiple and innovative uses of consumer data and its inherent value are topics that tend to be discussed primarily in the context of the increasing digitalization of the economy. The European Commission recognizes that “generating value at the different stages of the data value chain will be at the centre of the future knowledge economy”¹⁶.
29. The World Economic Forum expressed the same views in 2011 in a report called “Personal Data: The Emergence of a New Asset Class” whereby digital data created by and about people is generating a new wave of opportunity for economic and societal value creation.¹⁷ The ability to leverage data developed or owned by an enterprise, and to build solutions around that data for interested internal and external parties allows for an unprecedented monetization of data.¹⁸
30. According to the US Federal Trade Commission, companies have used big data to provide alternative ways to score populations that were previously deemed unscorable.¹⁹ This has become possible, for example, by innovative computing technology that is capable of drawing inferences from seemingly unrelated sets of data. The US National Consumer Law Center comes to similar conclusions in respect of the particular use case of access to credit by stating that “it is unsurprising that in this era of big data, information culled from Internet searches, social media, and mobile apps would be put to use towards [...] the goal of finding a way of getting affordable access to credit” to the population.
31. Big data analytics “promises to make better predictive algorithms that in turn can make better products available to the unbanked and underbanked”. However, the Center also recognizes that more data does not necessarily mean better data because “expanding the number of data points also introduces the risk that inaccuracies will play a greater role in determining creditworthiness”²⁰. Similarly, the Financial Services User Group (FSUG), recently “found no evidence that increased credit data availability has helped prevent over

¹⁶ See European Commission’s Digital Agenda for Europe: “Making big data work for Europe”, <https://ec.europa.eu/digital-agenda/en/making-big-data-work-europe>.

¹⁷ http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

¹⁸ “What’s your data worth?, Accenture, 2013, https://www.accenture.com/t20150523T054055_w_us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_1/Accenture-Whats-Your-Data-Worth.pdf#zoom=50.

¹⁹ “Big Data - A Tool for Inclusion or Exclusion? Understanding the Issues”, FTC Report, January 2016, p.6, <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>.

²⁰ “Big data: a big disappointment for scoring consumer credit risk”, US National Consumer Law Center, March 2014, p.14, <https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>.

indebtedness” and that “individuals may be prepared to sacrifice privacy in order to obtain credit, but may not appreciate the consequences of doing so.”²¹

32. Financial institutions may collect consumer data themselves or make use of the services of third parties, e.g. companies that compile information from databases with the intent to prepare combined datasets for data processing and then sell the information to third parties.
33. Financial institutions may also use consumer data to expand their client network, by making use of internal and external data sets to develop marketing campaigns so as to approach new consumers. Additionally, some financial institutions have been seen to use consumer data in order to increase their sales by cross-referencing data sources in order to build data bases of consumer behaviour (e.g. opening a savings account). This enables financial institutions to fine-tune their commercial offerings by selling products or services to consumers according to their expected behaviour. Moreover, financial institutions have used consumer data to help with the early identification of consumers’ default, act accordingly beforehand, and, hence, avoid costs.²²
34. Financial institutions may also be sharing consumer data with third parties, when they outsource the analysis of data to third parties or, under certain conditions, if they sell consumer data to third parties, so that these third parties can benefit from the use of the data. Financial institutions include various provisions on data protection and data usage in the contracts that govern the relationship with consumers. These provisions often state that consumer data will be shared by financial institutions with trading partners for internal marketing purposes.²³ Third parties with whom the data is shared may also be able to target consumers, or allow others to target consumers, with tailored offers based on criteria including spending, location and lifestyle.²⁴
35. In what follows below, two aspects about this innovation are highlighted: i) the possible sources of consumer data; and ii) the purpose of consumer data.

Sources of data

36. Consumer data used by financial institutions can be obtained both from internal and external sources. Data obtained from internal sources includes data provided by consumers to their financial institutions. This can be done either:

²¹“Assessing the impact of credit data on preventing over-indebtedness, contributing to prudential regulation and facilitating access to affordable and quality credit”, FSUG, December 2015, http://ec.europa.eu/finance/finservices-retail/docs/fsug/papers/1512-credit-data_en.pdf.

²² For these and other examples, see “Big data alchemy: How can banks maximize the value of their consumer data?”, Capgemini Consulting, 2014,

https://www.capgemini-consulting.com/resource-file-access/resource/pdf/bigdatainbanking_2705_v5_0.pdf

²³ In these circumstances, consumer consent is often acquired via general agreement with the Terms and Conditions offered by financial institutions.

²⁴ See “Risk of rewards?”, Which? Magazine, September 2015.

- a. Directly, i.e. data provided by consumers on a voluntary basis, when requested to do so; and data that consumers are required to disclose to financial institutions when entering into a contractual relationship (e.g. data needed to open an account and to comply with legal and regulatory obligations); or
 - b. Indirectly, i.e., data obtained by financial institutions in the development of the contractual relationship with consumers, payment data²⁵ and browsing history²⁶.
37. In addition to internal data sources, financial institutions may also obtain consumer data from external sources. This is data that financial institutions would collect outside of their own network, namely from other public or private companies and social media. External sources may include:
- a. Other public or reliable sources, the most frequent being credit reference agencies or credit information services providers. Other examples of these sources are population register centres, national statistics offices, land registries and electoral registries;
 - b. Private companies, such as data aggregators, that obtain data from sources accessible to the public and companies that provide data for marketing purposes, including entities making use of social media information (e.g. Facebook) as a means of enhancing and aggregating personal and financial data²⁷;
 - c. Entities within the same group and financial conglomerates, e.g. data that a bank may obtain from an insurance company that belongs to the same financial conglomerate.
38. Data obtained from external sources, such as social media, tends to have been made public by consumers on a voluntary basis but not given specifically to financial institutions. While probably being aware that this publicly available data may be used by (any) third parties, consumers may not be aware that, for instance, under EU data protection law, the fact that information has been published does not deprive it of the status of personal data and the ensuing protection.

Purpose of data

²⁵ Strictly speaking, payment data is also acquired from external sources, as the payment-chain consists of a variety of organizations that initiate and process the payment and, thus, transfer the data that is required to process these payments to banks and other payment institutions.

²⁶ By, for instance, making use of 'cookies technology' provided by software companies, through which financial institutions would be able to track consumers' online movements.

²⁷ For example, Facebook has been reported as having patented a technology in the US that could be used by lenders to assess the credit risk of borrowers by using the borrower's social network data.

See <http://money.cnn.com/2015/08/04/technology/facebook-loan-patent/>, August 2015.

39. The EBA has observed numerous examples in the way financial institutions use consumer data such as payment transaction data, including:

- a. Financial institutions using consumer data from innovative sources, e.g. social media, for creditworthiness assessment, assessment of insurance risk, and predicting consumers' default.
- b. Consumers subscribing to a rewards programme on the financial institution website, on a voluntary basis, and selecting the offers they are interested in or that they want to receive. Financial institutions analyse such data and provide targeted offers to consumers according to the offers previously selected on the website program.
- c. Financial institutions offering personalised cash-back deals on debit card purchases (usually equivalent to a percentage discount when the consumer makes certain purchases), or other kinds of bank account loyalty schemes that give consumers discounts and rewards from a number of retailers based on their spending behaviour.
- d. Financial institutions relaying offers and advertisements from other companies based on the consumer's prior payment data and spending behaviour.
- e. Financial institutions profiling and segmenting consumer base. Financial institutions may send personalised offers to consumers instead of general offers through e-mailing non-personalised lists. In order to do this, financial institutions use software that processes large amounts of data collected from financial institutions' consumers, namely consumers' payment flows²⁸.
- f. Financial institutions using payment data to proactively approach consumers with offers of products, services and advice, e.g. customised mortgages and savings advice.
- g. Financial institutions commercially sharing consumer data with third parties either by selling individual consumers' profiles, according to the terms and conditions of the contract entered into with consumers, or aggregated reports.
- h. Financial institutions using consumer data in the provision of various kinds of automated services, including automated advice²⁹ or financial management tools.

²⁸ For instance, a financial institution would be able to conclude whether or not a client has had a baby by spotting a child benefit credited to his/her account. Based on this assumption, the financial institution would offer this client targeted products such as child savings account.

²⁹ Automated advice materialises when a financial institution provides advice or recommendations to consumers without, or with very little, human intervention and relies instead on computer-based algorithms and/or decision trees. See <https://www.eba.europa.eu/documents/10180/1299866/JC+2015+080+Discussion+Paper+on+automation+in+financial+advice.pdf>.

40. Data may be processed by financial institutions in several different forms. For instance, data can be used in an individual or aggregated form; anonymised or non-anonymised. IT technologies exist that are specialized in the complex and mass processing of consumer data. This analysis may be performed internally by financial institutions or outsourced to third parties³⁰.
41. Also, some financial institutions are known to resort to data anonymization approaches. However, this does not mean that an individual cannot be (re)identified. Indeed, if crossed with other sets of external data, data given directly/indirectly by consumers and then “anonymised”, may allow for the (re)identification of a given consumer. In certain situations a person can even be re-identified through aggregated data. If re-identification is possible, then that data shall be considered as personal data and shall be processed with the adequate safeguards.

Questions:

1. In what capacity (i.e. consumer, financial institution, technology providers, etc.) have you had experience with innovative uses of consumer data?
2. Based on your knowledge, what types of consumer data do financial institutions use most?
3. Based on your knowledge, what sources of consumer data do financial institutions rely on most?
4. Based on your knowledge, for what purposes do financial institutions use consumer data most?
5. How do you picture the evolution of the use of consumer data by financial institutions in the upcoming years? How do you think this will affect the market?

³⁰ Regarding outsourcing, it is important to note that, in 2006, the Committee of European Banking Supervisors (CEBS) published guidelines on outsourcing of credit institutions' business activities, so as to promote an appropriate level of convergence in supervisory approaches to outsourcing. See <https://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf>.

Potential benefits

42. This chapter categorises potential benefits for consumers, in terms of costs, product quality and quality of service; as well as to financial institutions, in terms of costs, and new sources of revenue.

Benefits to consumers

Cost reductions

B1: Consumers benefit from financial institutions' improved cost-effectiveness

43. Using consumer data could enhance the cost effectiveness of marketing activities of financial institutions, allowing them to save money in advertising, for instance, and increase their sales and their reactivity to any developments in the market. This increased cost-effectiveness may be passed on to consumers in terms of lower prices.

B2: Consumers save money because they are offered targeted discounts by their financial institutions

44. Financial institutions may use consumer personal and financial data to understand their preferences and payment habits and offer consumers targeted products and services with specific trading partners (e.g. automatic discounts at restaurants or shops that are frequently visited by a specific consumer). This may enable consumers to save money whenever they purchase products or services included in the offers, either because products and services are cheaper or because they are tailored to consumers' needs and thus there is no need to complement the purchase with other products or services.
45. Consumers are seen as being interested in receiving points, rewards, and suggestions of purchases when they purchase a given product or service³¹. Some consumers would apparently be willing to reveal a wider range of their personal data if this meant better service from banks³².

B3: Consumers pay less as a result of more accurate creditworthiness assessment

46. Financial institutions may use consumer data in order to better perform creditworthiness assessments before providing credit to consumers. This can be done by combining data they were given by consumers with other sources of data (e.g. social media) in order to increase

³¹ FT Money Show, "Do you know how much your personal data is worth?", 4 November 2015, at <https://www.acast.com/ft-money-show/doyouknowhowmuchyourpersonaldataisworth->.

³² "Understanding Financial Consumers in the Digital Era: A Survey and Perspective on Emerging Financial Consumer Trends", CGI, 2014, p.12, at http://www.cgi.com/sites/default/files/pdf/br_fs_consumersurveyreport_final_july_2014.pdf.

credit score accuracy for improved risk control and offer more competitive pricing to consumers.

47. By applying more accurate credit scoring methodologies, based on more sophisticated analysis of consumer data, financial institutions may be able to increase the accuracy of risk profile and hence pricing of a specific risk. For instance, financial institutions may be able to offer lower interest rates on mortgages to consumers with a lower risk profile than less accurate traditional credit scoring models are able to produce.

Improved product quality

B4: Consumers are offered products and services that are personalized and adapted to their needs

48. More sophisticated analysis of consumer data can enable financial institutions to have real-time insight into consumer behaviour and anticipate consumers' needs or interests by offering products that are more adapted to them. For example, products could be adapted such that they allow insights in consumers' lifestyles, life-events, behaviours, or preferences (e.g. a financial institution proactively sending an email advertising a children's savings account to a recent parent).

B5: Consumers receive better advice based on analysis of their data

49. More extensive analysis of consumer data (e.g. payment data) can enable financial institutions to gain better knowledge of consumers' overall financial situation, needs and objectives and, thus, to provide better advice to consumers, tailored to their specific needs.

B6: Consumers gain better insight into, and control over, their financial situation

50. Analysis of consumer data may enable financial institutions to provide services that give consumers better insight into their financial situation and spending behaviour, should they possess the desire to want to take control of their financial situation. Such services could help consumers to save money, budget their expenses and control their borrowing level.

B8: Consumers are better protected against fraud

51. Increased use of consumer data could help financial institutions to improve their fraud detection so that fraud is detected more often and/or earlier. For instance, if financial institutions know where a specific consumer lives and works, where he/she normally makes his/her payments, and the amounts that he/she usually spends, they will be more likely to be able to spot an unusual transaction because of where it is initiated, the product/service that is purchased, or the price that is paid. This could protect consumers against financial losses and the inconvenience and practical problems that are associated with incidents of fraud.

Benefits to financial institutions

Reduction of costs

B10: Financial institutions benefit from improved cost-effectiveness

52. Using consumer data could enhance the cost-effectiveness of marketing activities of financial institutions, because it enables them to avoid the costs of unwanted and/or inappropriate spending in marketing, for instance. By offering products that match consumer's needs, financial institutions may save money in advertising and increase their sales and their reactivity to any developments in the market.

B11: Financial institutions reduce costs related to consumers' default

53. Financial institutions may use consumer data in order to create models that predict the probability of default for each consumer. Based on consumer behaviour analysis, drawn from multiple sources of data, financial institutions would be able to identify default risks early in the process and control default by developing actions to prevent it and its consequent losses and costs.

B12: Financial institutions are able to detect fraud at an early stage

54. Through the analysis of consumer data, financial institutions may be able to early identify fraud related, for instance, to payments, and thus decrease the costs and losses they would incur because of this.

New sources of revenue

B13: Financial institutions generate new revenues because of better product and service development

55. Increased use of consumer data can enable financial institutions to improve their product and service development (e.g. tailor-made products, personalized offers, better advice), and generate new revenue as a result.
56. Real-time insight into consumer behaviour (e.g. through analysis of payment data or geolocation) may enable financial institutions to anticipate consumer behaviour and problems. This could help them to pro-actively service their consumers when their current portfolio of products no longer matches their needs (e.g. insurance coverage) or financial capabilities (e.g. increasing risk of arrears). This may, in turn, increase financial institutions' sales, because consumers would feel more prone to purchasing products and services that are tailored to their needs and habits.

B14: Financial institutions generate new revenues by being able to relay to consumers tailored advertisements from third parties

57. Financial institutions may use consumer data to relay their trading partners' advertisements to consumers. By doing so, they add a new source of revenue to their business model (e.g.

payments from trading partners for the relaying of advertisements; percentage share of the trading partners' earnings when the advertised product is sold to the consumer).

B15: Financial institutions generate new revenues by sharing consumer data with third parties

58. Financial institutions may share consumer data with third parties on the condition that consumers have agreed to this. Data may be shared in an aggregated form (usually, anonymised); also financial institutions can share consumer profiles they have created on the basis of the data they have collected and processed.

B16: Financial institutions use external sources of consumer data as a market research tool to expand their services.

59. Financial institutions can use external sources of data (e.g. credit reference agencies), either in isolation or jointly with internal data, to actively identify new customers.

Questions:

6. Do you consider the potential benefits described in this chapter to be complete and accurate? If not, what other benefits do you consider should be included?
7. Are you aware of any barriers that prevent financial institutions from using consumer data in a beneficial way? If so, what are these barriers?

Risks

60. This chapter describes the risks that have been identified as potentially accruing to, consumers, financial institutions, and financial integrity. This does not mean that these risks have materialized yet. The risks to consumers are presented under the following categories: i) information asymmetries; ii) misuse of data; and iii) data security. The risks arising to financial institutions are categorised as those related to i) reputation; ii) new entrants in the market; and iii) security of data.
61. This chapter also discusses risks to the integrity of the financial sector, because it is important to consider whether there would be risks to the entire financial sector should innovative uses of consumer data become a trend among financial institutions.

Risks to consumers

Information asymmetries

R1: Consumers experience detriment if they are unaware of the way financial institutions make use of their personal data

62. Consumers may not always be properly informed of the usage of their personal data. This may be the case when, for instance, the use of their data is not properly described or updated in contractual documentation provided to them by financial institutions.
63. On the other hand, consumers may not understand information that is provided to them regarding the use of their data. For example, very comprehensive information may be made available in the contracts between consumers and financial institutions, but it tends to be too complex and/or too detailed for consumers to understand.
64. Unlike financial institutions, consumers may not always have an in-depth knowledge about the legal framework applicable to the usage of their personal and financial data. This information asymmetry may be especially relevant in cross-border transactions, where the applicability of legal requirements is not always clear.
65. Additionally, financial institutions may have in place automatic rules based on the information given by consumers that result in the usage of consumer data in a way that may be non-transparent and somewhat arbitrary, notably because consumers may not be aware of the factors that led to the decision (e.g. non-approval of credit application because of automatic credit scoring based on consumer data).
66. As a result of the above, consumers may experience detriment in the form of breaches to their privacy.

R2: Consumers are “locked-in” by their current provider because their data is not assessable to other financial institutions

67. Financial institutions may collect and process a significant amount of data throughout the contractual relationship with consumers, which means that they may be able to offer to consumers products and services that cannot be matched by other financial institutions (that do not have access to the same types of data). If financial institutions do not allow for the portability of consumer data, consumers may be hindered from choosing a different provider for the provision of financial services.

Misuse of the data

R3: Consumers experience detriment if financial institutions misuse their personal data

68. Consumer personal and financial data may be used by a financial institution for purposes that were not in any way disclosed to consumers. The misuse of consumer data may be a result of deliberate or accidental actions by the financial institution or an individual employee.

69. Also, financial institutions may interpret legal requirements for data collection, for anti-money-laundering purposes for instance, such that they collect more data than is legally required and then reuse it for other purposes.

70. The misuse of data can manifest itself in consumer data being sold by financial institutions to third parties (such as marketing companies) without the consumers’ consent. Financial institutions may also be processing consumer data without explicit authorization from the consumer. This may result in detriment for consumers, through financial institutions being remunerated for selling consumer data and consumers not benefiting from this; consumers being targeted by third parties with whom they never have, and do not wish to be, commercially engaged; or various types of identity fraud.

71. Finally, the misuse of consumer data can also result in detrimental marketing approaches by financial institutions, in the form of spamming of electronic or conventional mail. This is more relevant in the context of the increasing digitalization of communications between financial institutions and consumers, where the costs of communicating via email are low.

R4: Consumers experience detriment as a result of wrong decisions by financial institutions on the basis of wrong information

72. Financial institutions may use consumer personal and financial data, irrespective of where such data was obtained, to make decisions that may result in detrimental treatment of consumers. This unfair treatment can manifest itself in the following ways:

- a. consumers are turned away by financial institutions, for example, as a result of a financial institution rejecting a consumer based on a profile that categorises the consumer as being prone to credit default because of outdated or inaccurate information;

- b. consumers are declined from purchasing certain products or services, for example, because of a consumer not being offered a mortgage because the specific personal data from social networks incorrectly led the financial institution to believe that the consumer was less creditworthy a borrower;
 - c. consumers are offered or declined certain contractual conditions when asking for a specific product or service, for example a consumer not being granted a long-term loan because the financial institution has wrongfully concluded from external data that the consumer may be a gambler;
73. This risk is more likely to arise if the provider establishes discriminating criteria based on sensitive consumer data, such as those related to health. When consumers are profiled through the use of personal information they might be targeted for specific products and/or services that are not in their best interest (e.g. unsuitable insurances for risk-averse consumers); or they may be excluded from the offer of services that would be interesting to them, because financial institutions see them as uninteresting or too risky.

R5: Consumers have restricted or no access to financial products or services because they do not allow for their information to be used by financial institutions

74. If consumers do not wish to disclose their data for purposes different than those required by law and do not allow their financial institutions to use it for any kind of commercial purposes, they might be excluded from relevant offers.
75. This risk is more relevant if the use of consumer data becomes the main marketing tool of financial institutions. Consumers that do not allow their data to be used for commercial purposes would then have restricted access or even be excluded from some financial services.
76. Also, there may be the case that consumers will be perceived as having a higher risk, thus paying more for the same services when compared to other comparable consumers, because they refuse to disclose any data with which financial institutions would be able accurately to profile them.

Data security

R6: Consumers suffer detriment if consumer data stored by financial institutions is obtained fraudulently by third parties

77. Consumer data stored by financial institutions may be accessed by third parties in an illegitimate way if, for instance, such data is hacked (e.g. credit card details stolen and subsequently used by third payments to purchase goods/services in the name of the consumer). There may also be the case that financial institutions have anonymized consumer data, but third parties with fraudulent intents are able to reconstitute such data and misuse

them to the detriment of consumers. This risk is more likely to occur when financial institutions have weak IT-security measures in place.

Risks to financial institutions

Reputational risks

R7: Financial institutions are exposed to reputational risk if they make questionable use of consumer data

78. Financial institutions might use data in a way that results in questionable decisions about consumers if, for instance, they do not take into account relevant details contained in the data they possess; do not possess enough data to make a decision; or interpret data in a wrong way, because the tool used to process it is flawed. In any of these situations, financial institutions can face reputational risk if they then offer particular products to a consumer that are not tailored to his/her specific needs.
79. Additional reputational risk may arise if a financial institution makes a decision that is correct from a business point of view (e.g. the rejection of a loan application), but is made using data that the consumer would not expect to be used by financial institutions (e.g. data from social networks). Even if the consumer has authorised for the data to be used and/or if the data is publicly available, this kind of decision may be seen by the consumer as questionable and subject to repudiation.
80. This risk can be made worse if financial institutions make decisions based solely on the processing and interpretation of data ('automatic decision'), and/or if financial institutions do not offer their consumers the possibility to challenge the decision made.

New entrants in the market

R8: Financial institutions that are not in a position to process consumer data cannot compete with new entrants in the market that specialise in using consumer data

81. Even if financial institutions collect and have access to much consumer data, they may not use it for commercial purposes. This can occur if financial institutions do not have the IT tools and/or the technological expertise to process data; or if they are not willing to change their business model into one that takes advantage of the potential of consumer data, because, e.g. it is too costly.
82. Furthermore, it may be difficult for financial institutions to efficiently use this data, because consumer data is often collected and stored via multiple channels within financial institutions (e.g. branches, online banking; telephone banking); for multiple purposes (e.g. KYC requirements; AML; commercial offers); and using multiple technologies (e.g. biometrics; geolocation). This is because different methods for accessing the data may be needed, which may not be interoperable. It may also occur that many of these methods are inflexible, expensive to operate, and could be a source of failure in bank risk models that could result in taking incorrect managerial decisions

83. If new entrants in the market are specialised in collecting and using consumer data through innovative technologies and/or have access to a very large amount of personal data, financial institutions that do not make an efficient use of data may be unable to compete, and, thus, may forego revenues. Moreover, financial institutions may decide to restrict themselves in their use of consumer data, so as to try to meet the high expectations society may have towards them, and thus avoid reputational risk.

Data security

R9: Financial institutions are exposed to legal risks if their IT systems are compromised

84. Data security risks may materialize if the IT system owned and/or maintained by financial institutions is hacked or in some way fraudulently accessed by third parties, and if consumer data is made available as a result. This may be especially relevant when, for instance, the database is not stored locally within the financial institution, but outsourced to cloud services that only operate online and are, thus, subject to cyber-attacks. Also, the database may be compromised due to internal factors, such as a flawed data processing system that leads to an unwanted leak of data to third parties.
85. The internal or external impairment of the IT system may result in an obligation to provide redress for consumers who have suffered detriment, such as unauthorised payment transactions initiated by third parties using the data, or consumer data sold to third parties without consumers' consent. Compensation pay-outs, litigation costs and fines may be incurred by financial institutions in this case.

Risks to the integrity of the financial sector

R10: Integrity of the financial sector is undermined if trust in financial institutions decreases because of lack of data security

86. In the event that consumer data is stolen, hacked and/or leaked, trust in financial institutions may be undermined, with spill-over effects to the financial sector overall, in respect of the sector's ability to securely store and process data. This distrust may even spread to other services offered to consumers and result in reduced market confidence.

R11: Integrity of the financial sector is undermined if financial institutions become overly dependent on the use of consumer data as a source of revenue

87. Financial institutions may change the way they conduct their business by excessively basing it on consumer data. This may result in an excessive exposure to any future tightening of legislative or regulatory requirements applicable to the use of data. It may also happen that consumers no longer want to engage with financial institutions having such a profile.

88. Also, if financial institutions become overly dependent on the use of consumer data, they may disregard other profitable business strategies or market opportunities because there is no previous or available data to support the decision of pursuing that specific strategy or market opportunity.

Questions:

8. Do you consider the potential risks described in this chapter to be complete and accurate? If not, what other risks do you consider should be included?
9. Have you observed any of these risks materialising? If so, please provide examples.