Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield

Fact-finding and assessment of safeguards provided by U.S. law

Final Report

Justice and Consumers

Automated decision-making
on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield

Fact-finding and assessment of safeguards provided by U.S. law

Final Report

Authors TNO: Gabriela Bodea, Kristina Karanikolova, LL.M
U.S. Legal experts: Associate Prof. Deirdre K. Mulligan, Jael Makagon (JD, MPP).

Directorate-General for Justice and Consumers
Directorate C : Fundamental Rights and Rule of Law
Unit C.4 International Data Flows and Protection

Acknowledgements

The authors should like to thank all experts who participated in the interviews, among whom: Ms Pam Dixon, Ms Rita Heimes, Ms Müge Fazlioglu, Mr Adam Tanner, Mr Martin Abrams, Mr Jeff Chester, Mr Jeff Larson.

We are grateful to Ms Chi Chi Wu, Mr Robert Gellman and Prof David Vladeck, as well as to the reviewers from the European Commission for their valuable feedback on the report.

Finally, we thank the TNO team for their support: Marissa Hoekstra, Jeanet Gieskens, Wilmy Schipper-van Dijk, and Rick Schalkers.

DISCLAIMER
The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use, which may be made of the information contained therein.

ISBN [to be inserted] doi: [to be inserted]

Table of contents

List of acronyms

ADM	Automatic decision-making
ADA	Americans with Disabilities Act
CDS	Clinical decision support
CJEU	Court of Justice of the European Union
CRA	Consumer reporting agency
DOC	US Department of Commerce
DPA	Data Protection Authority
DPD	Data Protection Directive
EC	European Commission
ECOA	Equal Credit Opportunity Act
ERCP	Economic Growth, Regulatory Relief, and Consumer Protection Act
FCRA	Fair Credit Reporting Act
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
PCLOB	Privacy and Civil Liberties Oversight Board
PHI	Protected health information
PS	Privacy Shield
SCC	Standard Contractual Clauses
TOR	Terms of reference
WP29	Article 29 Data Protection Working Party

List of Figures

List of Boxes

1 Introduction

1.1 Objective

The *Study on automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the E.U.-U.S. Privacy Shield: Factfinding and assessment of safeguards provided by U.S*. was requested by the European Commission, the Directorate-General for Justice and Consumers. The general objective of the study was to provide information which would allow the Commission to decide whether the safeguards for situations of automated decision-making are adequate in the context of transfers of data on the basis of the Privacy Shield.

More specifically, the study was intended to support the Commission's assessment regarding:

(i) the extent to which Privacy Shield-certified companies in the U.S. take decisions affecting the individual based on automated processing of personal data transferred from companies in the EU under the Privacy Shield; and

(ii) the safeguards for individuals that U.S. federal law provides for this kind of situations and the conditions for these safeguards to apply.

The terms of reference (TOR) of the request for services are described below and present the background of the requested study.

1.2 Background as per TOR

EU data protection law contains protections for individuals in cases of automated decision-making. Article 22 of the General Data Protection Regulation (GDPR) provides that a data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This principle is subject to exceptions, notably if such decision is necessary for entering into, or the performance of, a contract between the data subject and a data controller, or if the decision is based on the data subject's explicit consent. In these cases, the data controller is obliged to implement appropriate safeguards to protect the data subject's rights and freedoms and legitimate interests, at least the right to obtain human

intervention on the part of the controller, the right to express his or her point of view and the right to contest the decision.

The EU-U.S. Privacy Shield ("Privacy Shield") is a framework for transfers of personal data between the EU and the U.S. which the Commission has found to provide adequate protection under EU data protection law. In the absence of overarching privacy legislation in the U.S., the Privacy Shield is based on a self-certification system by which U.S. companies commit to adhere to a set of privacy principles. While certification is voluntary, companies that have been certified are obliged to comply with the principles, which become enforceable under U.S. law. The privacy principles contained in the Privacy Shield reflect the main principles of EU data protection law, such as data integrity, purpose limitation, limited data retention, protections in case of onward transfers, information to the data subject, the right to access and rectification, the right to object, and individual redress rights. However, no principle that would provide similar protections to Article 22 GDPR is contained in the Privacy Shield.

As far as automated decision-making is concerned, the Commission concludes in recital 25 of its decision on the adequacy of the Privacy Shield ("the adequacy decision") that in areas where companies most likely resort to the automated processing of personal data to take decisions affecting the individual (e.g. credit lending, mortgage offers, employment), U.S. law, notably the Equal Credit Opportunity Act, the Fair Credit Reporting Act or the Fair Housing Act, offers certain protections against adverse decisions. These acts typically provide that individuals have the right to be informed of the specific reasons underlying the decision, to dispute incomplete or inaccurate information, and to seek redress. At the same time, the adequacy decision is based on the assumption that the number of cases where automated decisions are taken by a Privacy Shield-certified company itself is rather limited. The reason is that, in the context of a transfer of personal data that have been collected in the EU, the commercial relationship with the individual (customer) will in most cases be with the EU controller, who would typically be the one to take a decision based on automated processing and would then have to abide by EU rules.

1.3 Additional background information

The assumptions described in the previous paragraph were generally supported by the findings of the first annual Joint Review of the Privacy Shield. The review was conducted on 18 and 19 September 2017 in Washington, DC.

In its report[1] published after the review, the Article 29 Data Protection Working Party (henceforth WP29) mentioned that the review did not indicate that data of EU data subjects transferred to the U.S. by companies self-certified under the Privacy Shield would have been processed by automated decision-making systems.
The WP29's report also commented on the information provided on the Fair Credit Report Act, confirming the existence of specific rules under U.S. law. However, the WP29 noted the limited scope of the existing rules which would leave certain areas of application of automated decision-making (henceforth ADM) less well-covered. The WP29 also pointed to the limited relevance of the Fair Credit Reporting Act (FCRA) presented during the review together with examples of related enforcement cases. The reason for this opinion was the fact that, at the time, no credit reporting agency was participating in the Privacy Shield. (It should be noted that since the first annual review, several credit reporting agencies have self-certified under the Privacy Shield, most notably Experian, one of the three big credit reporting companies in the US, and FICO). It also raised questions whether the scope of the FCRA would also extend to behavioral advertising. (Note: the issue of whether behavioral advertising should be considered as a form of ADM, which could have legal effects or significantly affect the individual, is currently being addressed by the UK Information Commissioner's Office (ICO) as part of the ongoing Facebook-Cambridge Analytica investigation. See also section 9.2)

The WP29 further commented in their report on the feedback received from Privacy Shield self-certified companies about their use of automated decision-making. Given the limited and general character of the feedback, the WP29 could not draw definitive conclusions about all participating companies.

In its recommendations to the European Commission, the WP29 suggested exploring "the extent of the practical relevance of automated decision making processes by Privacy Shield certified companies" and, if necessary, "the possibility to provide for specific rules concerning automated decision making to provide sufficient safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis".

[1] Article 29 Data Protection Working Party (28 November 2017) EU – U.S. Privacy Shield – First annual Joint Review, Brussels, https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

The Report[2] from the European Commission to the European Parliament and the Council on the first annual review of the functioning of the Privacy Shield also concluded that additional factual evidence was needed to assess "the relevance of automated decision-making for transfers carried out on the basis of the Privacy Shield". This conclusion was echoed by the European Parliament in its 2018 resolution[3] on the Privacy Shield.

This study attempted to gather such evidence, to the extent that it was available, and assess the safeguards provided by the relevant U.S. federal law.

1.4 Methodology

The method of research included primary and secondary sources, as well as interviews with experts representing various stakeholder groups and potential domains of ADM application. Additional interviews have been conducted as part of the legal analysis to ensure that both industry and regulator views are included for each area analysed. The sources consulted were selected in order to collect factual evidence and further assess the relevance of automated decision-making for transfers of personal data carried out on the basis of the Privacy Shield during the period 2017-2018.

1.5 Potential challenges

In conducting the study, we took into account a number of potential challenges and risks, including but not restricted to the:

- limited availability of experts to take part in the interviews conducted by the project;
- limited relevance of the answers provided by experts;
- limited availability of cases of automated decision-making relevant to this study.

Other challenges encountered during the performance of the study included reservations expressed by the experts to take part in the interviews on-the-record,

[2] European Commission (18 October 2017) Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield of 18 October 2017, COM (2017) 611 final. Brussels

[3] European Parliament (5 July 2018) - Resolution on the adequacy of the protection afforded by the EU-US Privacy Shield, Provisional edition P8_TA-PROV(2018)0315, Strasbourg, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2018-0315

the relative novelty of automated decision-making as a business application, and more generally, the opacity characterizing the data industry.

1.6 Structure of the report

The report consists of eleven chapters and six annexes. Chapter 1 introduces the study: its background, objectives, and methodology. Chapters 2 and 3 present the results of the fact-finding part of the study into the extent to which Privacy Shield-certified companies in the U.S. take decisions affecting the individual, based on the automated processing of personal data transferred from companies in the EU under the Privacy Shield. The chapters includes evidence from ADM-related complaints, insights from expert interviews and ADM market evidence. Chapter 4 introduces the legal analysis part of the study, comparing the different E.U. and U.S. approaches to privacy, data protection and automated decision-making. Chapters 5 through 10 assess the protections for ADM offered by relevant U.S. federal law with regard to consumer credit, employment, housing, health information, advertising, insurance. In addition to the sectoral law explored in these chapters, chapter 7 examines the Federal Trade Commission Act. Finally, Chapter 11 presents the conclusions of the legal analysis, which, together with the conclusions of the fact-finding exercise in Chapter 3, should allow the European Commission to decide whether the safeguards for situations of automated decision-making are adequate in the context of transfers of data on the basis of the Privacy Shield.

1.7 Definitions

Central to this study were the concepts of automated decision-making and profiling, neither of which are defined in the adequacy decision[4].

To ensure consistency of analysis and use of the two concepts throughout the study, the following definitions were used.

1.7.1 GDPR

Regarding profiling, the GDPR[5] definition was taken into account:

[4] European Commission (July 2016). Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C/2016/4176. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG

[5] GDPR, http://eur-lex.europa.eu/eli/reg/2016/679/oj

> Article 4 (4) of the GDPR defines profiling as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.

Regarding automated individual decision-making, we took into account the definition provided by Article 22 of the GDPR,

> Article 22 of the GDPR refers to “a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

Recital (71) of the GDPR further specifies scope, conditions and exceptions as well as the rights of the data subject with regard to automated decision-making, and provides examples of possible areas of application:

> “The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her”, adding that such processing would include ‘profiling’.

As mentioned above, the same recital of the GDPR provides some examples of automated decision, including profiling, producing legal effects concerning an individual or similarly significantly affects him or her, namely the “automatic refusal of an online credit application or e-recruiting practices without any human intervention.“

Recital (71) also specifies the cases in which decision-making based on such processing, including profiling, should be allowed, namely:

> “ where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent.”

Suitable safeguards would have to apply in the case of the exceptions mentioned above and they would have to include:

> “specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.”

1.7.2 Article 29 Working Party Guidance

Article 29 Working Party[6] (WP29) provides further guidance as to the interpretation of automated individual decision-making and profiling.

Automated individual decision-making is explained by WP29 as:

> "the ability to make decisions by technological means without human involvement (…) based on any type of data, for example:
> - data provided directly by the individuals concerned (such as responses to a questionnaire);
> - data observed about the individuals (such as location data collected via an application);
> - derived or inferred data such as a profile of the individual that has already been created (e.g. a
> credit score)."

WP29 further clarifies that Article 22 GDPR only covers ADM that has serious impactful effects on data subjects ("legal or similarly significant effects"). According to the WP29, a legal effect requires that someone's legal rights (e.g. freedom to associate with others, vote in an election or take legal action) are affected. It may also affect a person's legal status or rights under a contract.

For data processing to significantly affect someone, the decision must have the potential to:

> "-significantly affect the circumstances, behaviour or choices of the individuals concerned;
> - have prolonged or permanent impact on the data subject; or
> - at its most extreme, lead to the exclusion or discrimination."

WP29 also explains that ADM can in some cases overlap with profiling or result from it. However, ADM and profiling can also be performed independently of each other.

[6] Article 29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_on_profiling_wp251rev01_enpdf.pdf

(i.e. “Automated decisions can be made with or without profiling; profiling can take place without making automated decisions.”)

Regarding profiling, the guidance interprets the GDPR definition as including three elements:

- an automated form of processing (not necessarily ‘solely’ automated processing)
- carried out on personal data; and
- with the objective of evaluating personal aspects about a natural person.

Adding that the evaluation of personal aspects of natural persons:

- may involve a series of statistical deductions, “often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar”.

WP29 further contrasts the GDPR definition of profiling with that provided by the Council of Europe Recommendation[7] CM/Rec (2010)132 which excludes processing that does include inference and considers profiling only that based on correlations identified and “applied to an individual to identify characteristics of present or future behaviour.”

Current practices and emerging trends in profiling would indicate that both types of profiling are currently being pursued for commercial applications, by different means and with different results. The two types of profiling for commercial applications distinguish between 1) the gathering of comprehensive information about individuals to create profiles “that could be used in many ways for different purposes”[8], and 2) profiling “with the objective of evaluating personal aspects about a natural person”. In the second category, a further differentiation is made between probabilistic and deterministic profiling (i.e. based on correlation or, indeed, causation).

Detailed commentary on the WP29 guidance is provided in the chapter Legal analysis – Introduction.

1.7.3 The adequacy decision

The adequacy decision, although not defining what constitutes profiling, refers to it in the context of the automated decision-making whilst stressing the need to monitor the use of automated processing:

[7] Council of Europe. (23 November 2010) The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 and explanatory memorandum.
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cdd00
[8] ibid.

> (25) "In areas where companies most likely resort to the automated processing of personal data to take decisions affecting the individual (e.g. credit lending, mortgage offers, employment), U.S. law offers specific protections against adverse decisions (23). These acts typically provide that individuals have the right to be informed of the specific reasons underlying the decision (e.g. the rejection of a credit), to dispute incomplete or inaccurate information (as well as reliance on unlawful factors), and to seek redress. These rules offer protections in the likely rather limited number of cases where automated decisions would be taken by the Privacy Shield organisation itself (24). Nevertheless, given the increasing use of automated processing (including profiling) as a basis for taking decisions affecting individuals in the modern digital economy, this is an area that needs to be closely monitored. In order to facilitate this monitoring, it has been agreed with the U.S. authorities that a dialogue on automated decision-making, including an exchange on the similarities and differences in the EU and U.S. approach in this regard, will be part of the first annual review as well as subsequent reviews as appropriate."

further clarifying that , in most cases of data transfers, the data subject's contractual relationship will be with a controller for whom the EU data protection rules apply:

> "In the context of a transfer of personal data that have been collected in the EU, the contractual relationship with the individual (customer) will in most cases be with — and therefore any decision based on automated processing will typically be taken by — the EU controller which has to abide by the EU data protection rules. This includes scenarios where the processing is carried out by a Privacy Shield organisation acting as an agent on behalf of the EU controller".

2 ADM & the Privacy Shield - Evidence-based analysis

2.1 Introduction

As part of the effort to monitor the use of automated decision-making (including profiling) and as described in the TOR, the first purpose of this study was:

> "to enable the Commission to understand whether U.S. companies that are certified under the Privacy Shield take decisions based solely on automated processing, including profiling, which have a legal effect on an individual or similarly significantly affect him or her, and if so, whether such decisions are taken on the basis of personal data that has been collected in the EU and transferred to the U.S. (or whether such decisions rather occur in EU-customer facing situations that are covered by EU data protection law)."

To address this first task, the study used a series of complementary approaches to assess the likelihood of data of EU data subjects being transferred to the U.S. by Privacy Shield (PS) self-certified companies for further processing in the context of commercial ADM during the period 2017-2018. The resulting three main sections of this chapter document the four approaches.

- In the first section, we present the insights gained from examining complaints about ADM activities of PS programme participants.
- In the second section, we present insights gained from a series of interviews with legal and technical experts.
- In the third section, we examine the likelihood of ADM availability and use from a supply- and demand-side perspective, focusing on the two main elements of ADM, namely: data (including profiles) and (analytics and decisioning) software.

2.2 Insights from ADM-related complaints received by PS independent dispute resolution bodies

This section presents the results of the first approach to assessing the likelihood of data of EU data subjects being transferred to the U.S. by Privacy Shield participants for further processing in the context of commercial ADM, between 2017-2018. Specifically, it presents the insights gained from examining complaints about ADM activities of PS self-certified companies .

2.2.1 Introduction

All organizations that participate in the Privacy Shield are subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body. Through the Recourse, Enforcement and Liability Principle, the adequacy decision requires all Privacy Shield self-certified organizations "to provid[e] for effective and readily available independent recourse mechanisms by which each individual's complaints and disputes can be investigated and expeditiously resolved at no cost to the individual." Various types of independent recourse mechanisms are allowed, located either in the U.S. or in the E.U., including:

Box 1 Privacy Shield survey (IAPP-EY 2017)

According to the IAPP-EY 2017 Annual Privacy Governance Report[1], more than half of the participants in the survey reported transferring data from the EU to the USA and almost half of them used the Privacy Shied Framework as a data transfer mechanism, an increase of 13% compared to the previous year, 2016. The report indicates that transfer rates of data are higher for larger organizations: "82% of organizations with revenue exceeding $25 billion and 75% of those with more than 25,000 employees" as well as for EU-headquartered respondents (79%).

The survey also enquired into specific difficulties in following legal obligations of the GDPR. Amongst the difficulties, restrictions on profiling were rated 4.8 on a scale from 0 (not at all difficult) to 10 (extremely difficult). Automated decision-making was not addressed separately in the survey.

- voluntary commitments to cooperate with the EU DPAs, and
- independent Alternative Dispute Resolution (ADR).

Individuals are free to choose to "bring a complaint directly to an organisation, to an independent dispute resolution body designated by the organisation, to national DPAs or to the FTC". If complaints remain unresolved by any of these recourse or enforcement mechanisms, individuals can also invoke binding arbitration under the Privacy Shield Arbitration Panel, as a recourse mechanism of 'last resort'.

Any complaints related to ADM, if lodged and reported, would provide a first category of direct evidence for this study. In order to assess whether companies self-certified under the Privacy Shield received complaints about their use of data transferred from the EU to the U.S. for ADM purposes in the period 2017-2018, we examined available reports published in the above-named categories, with varying results.

2.2.2 Selection of sources

The following sources were evaluated and discarded for lack of available information:

1. Information about the complaints brought by EU data subjects directly to the organizations could not be reviewed. Because of the sheer number of self-certified organizations and the fragmentation of reporting, no meaningful information could be derived.

2. Information about complaints received and handled by the U.S. Department of Commerce about Privacy Shield-participating organisations' non-compliance with the Principles was not available at the time of our research and will most likely be made available as part of the report for the second annual review on the functioning of the EU-U.S. Privacy Shield.

3. The complaints handled by the FTC between 2017-2018 did not include cases where the data had been transferred from the EU to the U.S. for ADM by Privacy Shield self-certified companies. Additionally, the 2017 edition of the annual Consumer Sentinel Network Data Book[9] did not include information on international complaints.

4. Information on binding arbitration by the 'Privacy Shield Panel' was not yet available.

5. Finally, there was no indication about EU data subjects having sought judicial redress in U.S. courts for matters relevant for this study.

The remaining two avenues for recourse were evaluated as providing more information and subsequently examined into more detail. They included:

[9] Published by the FTC since 1997, the annual Sentinel report includes information on consumers' complaints about fraud, identity theft, and other consumer protection topics. The 2017 edition did not include a section on international complaints.
https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf

6. The Independent dispute resolution bodies, other than the EU DPAs, designated by the Privacy Shield self-certified organizations. These bodies are required by the adequacy decision to publish an annual report providing aggregate statistics regarding their services.

and

7. The national Data Protection Authorities (DPAs).

2.2.3 Analysis of selected sources

The analysis was conducted in August 2018[10]. By that date, 3,447[11] active organizations were listed as self-certified under the Privacy Shield framework. 327 additional organizations were listed as inactive.

It should be noted that the actual number of entities covered by the Privacy Shield exceeded 3,447, as each organization can choose to list several of their entities (for example, their fully owned subsidiaries).

The data covered can be either HR or non-HR, or both.

According to the adequacy decision, complaints sent by eligible individuals to participating organizations must be answered within 45 days. In the absence of a timely or satisfactory response, eligible individuals can contact the independent recourse mechanisms chosen by the organizations.

In many cases, organizations select different recourse mechanisms to handle non-HR-related requests from HR-related requests (for the latter only DPAs can be selected).

At the time of the analysis, and in addition to the EU DPAs, there were 11[12] (groups) of independent dispute resolution bodies providing services to the PS self-certified companies. It should be noted that each PS-listed organization may choose one or several resolution providers to handle their complaints.

[10] By September 2018, the number of participating entities had increased to over 3,760. https://www.privacyshield.gov/list

[11] ibid.

[12] The 11 (groups) of Privacy Shield independent dispute resolution bodies in August 2018 were: Insights Association Privacy Shield Program (N.B. their complaints are actually handled by ICDR/AAA Privacy Shield Program); PrivacyTrust Privacy Shield Program; Whistic; BBB EU Privacy Shield Program; DMA Privacy Shield Program; EU Data Protection Authorities (DPAs); ICDR/AAA Privacy Shield Program; JAMS Privacy Shield Program; TRUSTe (now TrustArc); VeraSafe; Privacy Shield Program; Privacy Dispute Resolution Services (PDRS).

2.2.4 Conclusion

A detailed analysis of the PS complaints has been included in Annex 4. The main takeaways are summarized below.

Main conclusion: The information provided by the annual reports of the PS independent dispute resolution bodies and the EU DPAs is inconclusive for our study.

- With one exception (i.e. JAMS), the reports for the period 2017 – 2018 were not (yet) available by August 2018.

- During the reporting period 2016-2017, TRUSTe was the only body to have reported on complaints regarding profiling, more specifically, on 14 cases of ”Unauthorized profile with personal information[13].

- No ADM-related complaints were reported in the documents available at the time of the analysis.

At the same time, it should be taken into account that:

- There is no standard complaints reporting format. As a result, the reporting styles of the independent dispute resolution bodies vary widely and are, in general, very compact. TRUSTe and DMA are the only exceptions, providing detailed analyses on the number and nature of the complaints, the nationality of those who had lodged complaints, reasons for dismissing the complaints, methods employed to deal with the complaints, follow-up actions, etc.
- the EU DPAs provide little to no information about PS-related complaints (neither non-HR nor HR). A selection of annual reports were consulted, namely those of the UK, Ireland, the Netherlands, France, Belgium and Romania. The Belgian (2017) report wass the only one to include statistics on complaints about international data transfers, with references to binding corporate rules, contractual arrangements and “other” (the category “other” could be referring to PS, but not necessarily). The Romanian (2016) report mentions complaints about international search engines (Google) and social media (Facebook) but not specifically about data transfers to the U.S., nor about ADM. Lastly, all EU DPA reports studied mention PS & ADM, but only as a matter deserving close monitoring in the future.

[13] No additional information is provided.

2.3 Insights from expert interviews

In the absence of conclusive evidence from complaints about the potential use of personal data of E.U. data subjects transferred to the U.S. for commercial ADM applications between 2017 and 2018, an additional method of obtaining factual evidence was employed. The second method consisted of a series of expert interviews.

2.3.1 Selection of experts

Fifty U.S. experts were approached and ten accepted our invitation to participate in the interviews. The experts were selected so that they would represent the opinions of all relevant stakeholders: civil society, academics, journalists, industry representatives. The interviews were conducted throughout the month of August 2018. The interviews were conducted remotely and were semi-structured. The interview protocol has been included in this document as Annex 5.
A preliminary desk research helped to formulate the questionnaire used to guide the semi-structured interviews. The insights from the interviews were used to inform the rest of the study. A summary of the interviews has been included in the following section. Only the views of the interviewees who agreed to making their views public were included in the summary. The list of interviewees has been included in Annex 6.

2.3.2 Summary of interviews

1. On the matter of current and near-future use of profiling & automated decision-making (ADM)

Interviewees had divergent views on the extent to which ADM has been adopted as part of commercial applications in the U.S.. They also suggested that any analysis should aim to distinguish between “pure” profiling (i.e. gathering information about an individual) and ADM which might include profiling.

Regarding profiling, the majority of the interviewees agreed that this is a mature and widely-used technique. According to some, there is a transition towards more (types of) automation of profiling, such as new techniques employed to gather data, more types of data used to create an individual profile, new ways of segmenting and categorizing profiles, and new means of targeting individuals on the basis of profiles. Finding out the extent of use and the impact of profiling, however, can be challenging.

Profiling and the uses thereof in advertising are better understood than those in other domains (such as in the financial and health sectors or for employment purposes). The actual impact of automatically targeting individuals for political advertising, in view of the Facebook – Cambridge Analytica case, is still being evaluated in the U.S.

Regarding ADM, the interviewees found it difficult to estimate how widely used it is, although the majority considered that there are very few categories of ADM applications in the U.S. likely to affect E.U. data subjects.

2. Assessment and Examples of profiling & ADM

The interviewees mentioned a number of examples where ADM based on profiling would carry significant privacy risks. Most of these areas concern ADM that would be carried out by public entities or on the basis of personal data of data subjects in the U.S. (e.g. the use of biometrics for border control, criminal risk scoring, data from jail and court systems and transfers of data from and into public (government) databases) and are therefore not relevant for the purpose of this study that focuses only on commercial applications. Relevant examples that were mentioned included:

- the use of medical and health data and profiles that could be used to discriminate against individuals in the process of seeking insurance or employment;
- (political) targeting – cases like Facebook-Cambridge Analytica and unidentified cases of companies that base their business model on (personal) data;
- the use of financial and credit data for automated loan applications;
- the use of personal data (e.g. age, gender, ethnicity) in education and employment-related ADM, which might be biased against certain categories of individuals.

2.1. On the matter of data subject awareness:

Most of the interviewees could not express an opinion on the level of awareness of Europeans regarding the use of their data by U.S. companies in general, and in the context of ADM in particular.

2.2. On the matter of ADM technology employed and the data business ecosystem

According to most interviewees, rapid technological developments, especially in the area of machine learning, the availability of more data and digitization are acting as drivers for the use of profiling and ADM. Several interviewees opined that in the U.S.,

decision automation, as opposed to human decision-making, is generally viewed as less biased and a way to improve effectiveness, as well as a cost-saving measure.

2.5. On the matter of use of data of E.U. data subjects in the US

According to most interviewees, finding concrete proof and grasping the scale of the use of data transferred from the E.U. to the U.S. for ADM purposes remain challenging.
According to the majority of the interviewees, there are very few categories of ADM applications in the U.S. likely to affect E.U. data subjects. According to the interviewees, examples are likely to be limited to applying for a loan, enrolment in higher education, and taking travel insurance.

According to the interviewees, profiling and targeting by U.S. companies on the basis of data transferred from the E.U. are more likely to occur than ADM. Several interviewees mentioned the Facebook-Cambridge Analytica case, and one interviewee referred to the specific case in which political advertisements were targeted at users in Germany or individuals who had travelled to Germany. The targeting was based on factors such as demographics, personal interests, lookalike audiences[14] (i.e. Facebook users selected on the basis of specific characteristics defined by advertisers) and some of their data might have been transferred to the U.S. for further processing. However, the interviewee indicated that no definitive proof was available and that in the wake of the revelations about the case, Facebook changed their data sharing practices, improved their conduct, offering more transparency of targeting and profiling practices.

3. New initiatives in the US

State-level legislative initiatives in Vermont (where a new law was passed to regulate the activities of data brokers) and California (where a new online privacy bill was passed) were mentioned by the interviewees. (See Section 3.3).

[14] See for example the description of Facebook lookalike audiences https://www.facebook.com/business/help/164749007013531

4. On the matter of alternative protection mechanisms

The interviewees were divided on the topic of alternative data protection mechanisms. Whilst some considered that both codes of conduct and self-regulation could be useful, others doubted their effectiveness in practice and urged for stricter enforcement. Transparency initiatives, whether addressing algorithms or business practices, were mentioned by the interviewees as positive developments, worth supporting. The interviewees also mentioned the growing body of academic research into ethics and algorithmic transparency. As regards industry-led initiatives, some of the interviewees referred to a fair amount of controversy regarding their aims and approaches and commented on limits posed on the participation of stakeholders representing the interests of consumers. The interviewees mentioned, for example, the Open AI initiative, whilst also underscoring the need for any such initiative to include not only the industry but also representatives of academia and the civil society.

5. On the matter of the Privacy Shield (PS) and ADM:

Some of the interviewees pointed to the need for more guidance in interpreting the scope of "legal effect" in relation to automated decision-making and thus what constitutes a substantive decision.
Other areas requiring additional guidance or attention, according to the interviewees, were:
- the role of the online browser as an automated decision-making tool;
- the fairness of human decisions made on the basis of automatically generated profiles, especially where the profiles are based on inferred, rather than first-party data;
- various issues of technological bias (i.e. "when the risk is high and the consequences are significant, there is more incentive to use automated tools, if available" ; "automated decisioning tools can be seen as more scientific and could be used to overrule better human expert opinion")
- explainability of models and logic on which algorithms are based ("it might be difficult to explain to the average user how accelerometer data from their mobile phones can be used to assess their fitness and determine what kind of health insurance he can get").

2.3.3 Conclusions

The interviewees found it difficult to assess the impact of current ADM applications in general, and on data transferred from the E.U. in particular. Despite the viability and increasing availability over the past year of commercial ADM solutions, the opinion of most of the interviewees was that actual evidence of this particular type of use is difficult to find. Most interviewees also shared the opinion that, currently, there are very few categories of ADM applications in the U.S. likely to affect data transferred from the EU. The few examples mentioned were: applying for a loan, enrolment in higher education, and taking a travel insurance.

The large majority of the interviewees reiterated that, while technically possible and efforts being invested into developing the technology further, ADM is still at an emerging stage. Only a small minority considered ADM to be relatively widely used, not only in the public sector, but also for commercial applications. Potential current and future areas of commercial applications, most commonly mentioned as also relevant for data transferred from the EU, included the financial and health sectors (e.g. for assessing eligibility and risk associated with new life and health insurances, personal credit and loans), in marketing and advertising (e.g. for serving customized advertisements) and for human resource purposes (e.g. background checks of prospective employees, assessment and selection of job applicants, etc.). Both groups, however, stressed the need to monitor the development of ADM and develop standards for algorithmic transparency, explainability and accountability.

According to the interviewees, automated profiling and targeting by U.S. companies on the basis of personal data transferred from the E.U. are more likely to occur than ADM. One of the main reason mentioned was the fact that profiling and targeting on the basis of profiling are already mature technologies, unlike ADM.

Special attention was called for the role of traditional and new data brokers, new and more (types of) automation of profiling, more types of data used to create individual profiles, new ways of segmenting and categorizing profiles, and new means of targeting individuals on the basis of profiles. Assessing the extent of the use, and especially the impact of profiling, however, were also seen as challenging.

Finally, some interviewees pointed to the need for more guidance in interpreting aspects of ADM (for example on the scope of “legal effect” in relation to ADM) and for more user awareness.

2.4 ADM market evidence

2.4.1 Introduction

As mentioned in the previous section, the majority, though not all experts interviewed found it unlikely that Privacy Shield-certified companies would take decisions with legal or similarly significant effects on E.U. data subjects based on automated processing of their personal after the data had been transferred to the U.S. However, they indicated that actual evidence might be challenging to find, either because of the sector's lack of transparency or simply owing to the emerging character of ADM.
Most interviewees, however were of the opinion that profiling is already a mature practice, largely automated, especially online, and likely to involve personal data of E.U. data subjects as well (probably in a directly customer-facing situation rather than in a situation where data are transferred from the EU). As in the case of ADM, the experts pointed to the lack of transparency of profiling practices in the commercial sector and indicated that evidence might be challenging to find.

In the absence of such evidence, a market analysis was deemed as a potential source of insights into the likelihood of the use of solely automated decision-making involving Privacy Shield self-certified companies on the basis of E.U. data transferred to the U.S. for further processing.
This part of the study undertook to examine the **demand** for this type of ADM and the **supply** of its constituent components, namely data (including profiles) and (analytics and decisioning) software.

2.4.2 The demand side

Although by no means a recent technology[15], the adoption of ADM (except within technology companies), is still largely emerging. Consequently, there are few statistics about ADM market adoption and those that do exist should be interpreted with caution. Some were found to conflate semi-automated systems with fully automated ones; automated decision-support systems (i.e. aiding the decision of a human) with solely automated decision systems (the subject of this study); and reporting about automation of decisions internal to the organizations was not always counted as separate from decisioning systems intended to automate commercial services to individuals.

[15] A dynamic ticket pricing system was being introduced in the air travel industry in the U.S. at the end of the 1980s.

Taking account of these limitations, available reports would indicate that the current adoption and use of ADM by businesses is low. On average, less than 10% of businesses were understood to have adopted the technology and, according to Gartner[16], accounting for less than 2% of the global AI-derived business value in 2018. The adoption and use of ADM is estimated to be higher in the financial sector, in online marketing and advertising, and for human resource-related services. A slightly higher proportion of businesses are estimated to have adopted ADM only for experimental purposes; and a significantly higher proportion (estimates ranging anywhere from 40% to 90%) are reported to have expressed an interest in either adopting or experimenting generally with various forms of artificial intelligence (AI), including for ADM purposes, in the near future (i.e. between one and three years). A Forrester[17] report would indicate that U.S. businesses are not yet ready for or satisfied with their ADM adoption and use. According to the same report, there is a preference for using cloud[18]-based decision automation platforms (i.e. making use of services that can be accessed via the internet to store data, analyse it, combine it with other data, use it to create and deliver new decisions automation services, etc.).

Conclusion

The available data on the adoption and use of ADM remains too generic to allow for any definitive conclusion regarding the topic of our study. It can only be assumed, on the basis of the available data, that the current adoption and use of ADM in general is low.

As a next step, we examined the supply side of the ADM market.

2.4.3 The supply side

Two elements were considered as essential to **enable** ADM, namely **personal data** (including profiles) and (analytics and decisioning) **software. The two enabling components** were examined through case studies.

Regarding analytics and decisioning **software,** we found few relevant offerings by Privacy Shield self-certified companies. Upon closer inspection, many of the offerings

[16] https://www.gartner.com/newsroom/id/3872933

[17] https://www.prnewswire.com/news-releases/research-us-businesses-not-ready-for-machine-learning-decision-automation-300594675.html

[18] WP29 defines cloud computing as “a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space.” Opinion 05/2012 on Cloud Computing Adopted July 1st 2012, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

would not qualify as solely automated decisioning systems, but likely semi-automated and intended to support the decision of a human. In addition, while some Privacy Shield-certified companies might offer these types of software, there is little information about the actual use of the offered systems, in particular about actual use for ADM by Privacy Shield self-certified companies. It is unlikely that companies that offer automated decisioning systems take automated decisions themselves.

Regarding E.U. data and profiles, we found the cloud offerings likely to be relevant from the point of view of international transfers of E.U. data to the U.S. Here, too, no information was available as to actual use involving the transfer from the E.U. to the U.S. during the period 2017-2018. Most providers of the data products, services and platforms examined would qualify mainly as data processors and, in a limited number of cases, as data controllers. It is worth mentioning that most of these providers are **not** customer-facing.

2.4.4 Conclusion

The quality of the information available allows only for a tentative conclusion that average use of ADM during the period 2017-2018 was low. The actual use of *solely* automated decisioning systems with a legal or similarly significant effect on the individual cannot be estimated.

The availability of automated data processing (including profiling), data analytics and decisioning automation appears to be still in an emerging phase.

Although some Privacy Shield self-certified companies are offering ADM-relevant data and software products, services and platforms, their number is very low compared to the overall offering, most of their decisioning automation capabilities are likely to be partial rather than full, and actual transfer of E.U. data to the U.S. cannot be estimated on the basis of the available data.

It has to be highlighted that companies offering data and software products, services and platforms involving ADM are unlikely to engage in ADM significantly affecting an individual themselves, as such decisions would be taken by the company using the offered products and services. In other words, most providers of ADM-related products, services and platforms (including both profiles and software) examined would qualify mainly as data processors and only in a limited number of cases as

data controllers. It is worth mentioning that many of these providers are not customer-facing.

The types of ADM products, services and platforms encountered included: financial (e.g. credit scoring, commercial loans, commercial insurance), human resources-related (applicant tracking, applicant background checks, talent management, hiring) and marketing and advertising-related. Emerging are health-related applications. ADM for compliance (including GDPR compliance), identity management and risk and fraud-related were also available, but would likely qualify for the exception allowed for this type of ADM.

2.5 Other developments

There is growing awareness of the importance of providing more transparency, explainability and accountability about the functioning and use of algorithms, whether in the public or the commercial spheres. Significant research effort is ongoing as are industry initiatives as well as consultations and investigations by regulators. A few examples are provided below.

In 2018, the FTC organized Hearings on Competition and Consumer Protection in the 21st Century[19]. Included was a consultation on consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics.

At local level, the first Automated Decision Systems Task Force[20] in the U.S. was established in May 2018 by the City of New York with the task to review and assess "City algorithmic tools to ensure equity and opportunity". A report is expected in December 2019.

OpenAI is an industry-led research initiative[21] focusing on potential future implications of general AI.

Another industry initiative is The Partnership on AI to Benefit People and Society, founded in 2016 by Amazon, DeepMind/Google, Facebook, IBM, and Microsoft "to advance public understanding of artificial intelligence technologies (AI) and formulate best practices on the challenges and opportunities within the field"[22].

The Defense Advanced Research Projects Agency (DARPA) is funding the Explainable Artificial Intelligence (XAI) research programme [23] focused on developing

[19] https://www.ftc.gov/policy/public-comments/2018/07/initiative-760
[20] https://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by
[21] https://openai.com/about/
[22] https://www.partnershiponai.org/industry-leaders-establish-partnership-on-ai-best-practices/
[23] https://www.darpa.mil/program/explainable-artificial-intelligence

machine learning techniques that produce explainable predictive models (see figure below).

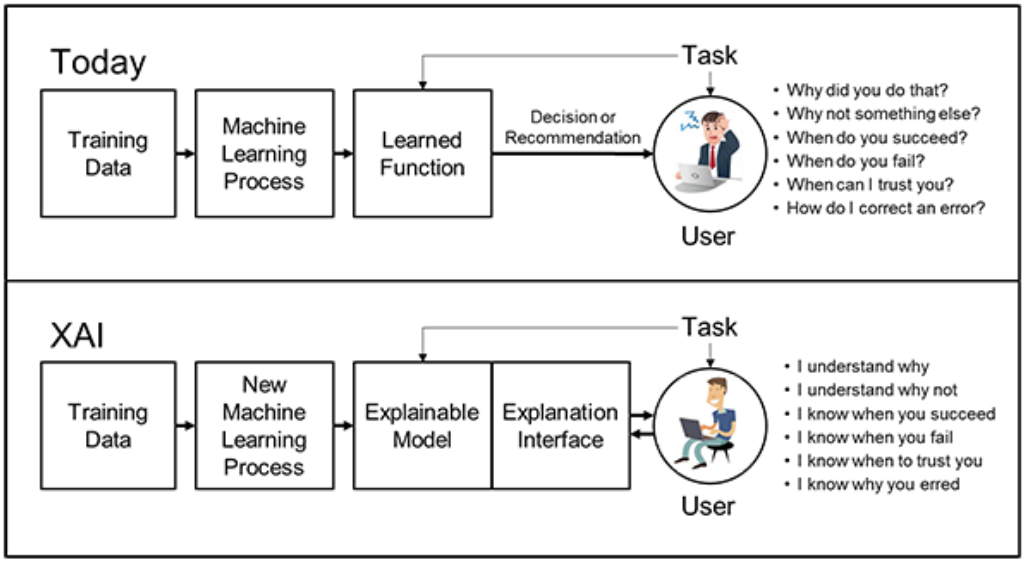

Figure 1 DARPA's XAI concept. Source: DARPA[24]

[24] https://www.darpa.mil/program/explainable-artificial-intelligence

3 Main conclusions – Part 1: Fact-finding

The first part of this report was dedicated to finding information about (the likelihood of) data of E.U. data subjects being transferred to the U.S. by Privacy Shield participants for further processing in the context of commercial ADM in the period 2017-2018.

To address this task, several complementary approaches were employed, in anticipation of and to compensate for the lack of relevant and publicly available information.

- In the first section, we presented the insights gained from examining complaints about ADM activities of PS programme participants.
- In the second section, we presented insights gained from a series of interviews with legal and technical experts.
- The third section used two case studies to illustrate the likelihood of ADM uses from a supply-side perspective. The case studies focused on the two main elements of ADM: data and (analytics and decisioning) software.

Finally, we presented a number of initiatives in the area of transparency, explainability and accountability about the functioning and use of algorithms.

Whilst most information indicated growing capabilities for ADM, including profiling capabilities, it was nonetheless inconclusive with regard to the actual use of solely ADM, including profiling, based on E.U. data transferred to the U.S. by Privacy Shield self-certified companies between 2017-2018.

1. No insights could be gained on the basis of the complaints lodged by E.U. data subjects during the reviewed period. The lack of standard reporting format as well as the absence of recent reports did not allow for a conclusion.

2. The expert interviewees found it difficult to assess the impact of current ADM applications in general, and on data transferred from the E.U. in particular. The majority, though not all experts interviewed, found it unlikely that Privacy Shield-certified companies would take decisions with legal or similarly significant effects on E.U. data subjects based on automated processing of their personal data that had been transferred to the U.S. However, they indicated that actual evidence might be challenging to find, either because of the sector's lack of transparency or simply owing to the emerging character of ADM. The experts suggested that, whilst

automated profiling and targeting were both mature technologies and broadly used for providing personalized content online, ADM was likely less so. According to the majority of interviewees, during the period 2017-2018, most ADM-based consumer services would have been aimed primarily at U.S. users and therefore not relevant for E.U. data subjects, with few possible exceptions (e.g. travel insurances, education, employment, advertising),

3. The analysis of the available automated data processing (including profiling), data analytics and decisioning automation systems would indicate that they are still largely in an emerging phase.
Although Privacy Shield self-certified companies are actively offering such data and software products, services and platforms, their number is very low compared to the overall offering, most of their decisioning automation capabilities are likely to be partial rather than full, and actual transfer of E.U. data to the U.S. cannot be estimated on the basis of the available data.

Most providers of the ADM-related products, services and platforms (including both profiles and software) examined would qualify mainly as data processors and, in a limited number of cases, as data controllers, and many of these providers are not customer-facing.

The types of ADM products, services and platforms encountered included: financial (e.g. credit scoring, commercial loans, commercial insurance), human resources-related (applicant tracking, applicant background checks, talent management, hiring) and marketing and advertising-related. Emerging are health-related applications. ADM for compliance (including GDPR compliance), identity management and risk and fraud-related were also available, but would likely qualify for the exception allowed for this type of ADM.

Current availability of ADM-based services does not imply adoption nor use of such systems. Available statistics are too generic to allow for any definitive conclusion regarding the topic of our study. It can only be assumed, however, that the current adoption and use of the type of ADM relevant for this study, on average, is low.

4. Finally, as knowledge development and investments in ADM in general are substantial, further monitoring would be recommended.

4 Legal analysis - Introduction

This part of the report is dedicated to the legal analysis. Firstly, it will present an **overview of the relevant U.S. legal framework**. As mentioned in the TOR, it covers "both general and sectoral rules (for instance, legislation, sub-statutory law, agency rules and guidelines; if applicable also other enforceable instruments contributing to the level of protection such as international agreements, self-regulatory instruments, certification schemes)".

In contrast to Article 22 of the GDPR, **there is no general prohibition in the U.S. on decisions based solely on automated processing, including profiling, which produce legal or similarly significant effects.** Indeed, as noted above in Chapter 3, the extent to which decisions that meet the Article 22 threshold are taking place, if at all, is unclear. However, it is clear that **automated processing**—as distinct from **decisions** based solely on that processing— is taking place in many U.S. sectors, some of which are covered by specific laws. Therefore, to understand the legal frameworks in the U.S. that are relevant to GDPR Article 22, it is important to take a slightly broader perspective and examine sectors where automated processing may be occurring. With this in mind, our analysis focused on sectors where decisions with legally significant or similar effects are being made and where some level of automated processing occurs.

Because of the scope of the TOR, the overview was limited to examining only measures at federal/horizontal level and generally did not include those at state or local level.

This task takes into account legal and regulatory changes that may have occurred in the past year, since the first review of the Privacy Shield. Updates will be included and analysed depending on both their availability and relevance for the topic of this study.

Additionally, this sub-task tried to identify **relevant new U.S. case law,** insofar as available and if deemed relevant in the context of the current study.

Secondly, the legal analysis consists of:

> "Assessing the protections offered by U.S. federal law for this kind of decisions and the conditions under which these protections apply, including but not limited to the protections provided by the laws that are already

> mentioned in the adequacy decision (the Equal Credit Opportunity Act, the Fair Credit Reporting Act and the Fair Housing Act). The assessment will cover both general and sectoral rules (for instance, legislation, sub-statutory law, agency rules and guidelines; if applicable also other enforceable instruments contributing to the level of protection such as international agreements, self-regulatory instruments, certification schemes), as well as relevant case law and will be informed by a limited number of interviews with relevant stakeholders in the U.S. (i.e. academia, privacy and data protection experts, policymakers)."

The analysis documents relevant protections offered by U.S. federal law, and other relevant instruments as described above, in the areas of employment, credit and lending, health, housing, and insurance (an area including a generalized consideration of relevant legal protections afforded at the state level). The analysis will consider the extent to which protections in the U.S. provide:

- *Notice that automated decision-making is taking place* (Articles 13-15),
- The *right to obtain an explanation* of a specific decision reached *after an automated decision-making assessment* (Recital 71)
- The *right to meaningful information about the logic* involved in *automated decision-making* (Articles 13-15)
- The *right to meaningful information about the significance and the envisaged consequences* of such processing for the data subject (Articles 13-15)

In addition, the analysis developed a framework for comparing explanations of decision-making afforded under the various U.S. laws and the GDPR that distinguishes between the:

- kinds of information provided (inputs, outputs, operation of a model, application of the model, limits and assumptions);
- modes and attributes of explanations (causal, contrastive, selective)[25]; and,
- goals explanations serve (oversight, corrective action, contestation).[26]

[25] Tim Miller. Explanation in artificial intelligence: Insights from the social sciences. arXiv preprint arXiv:1706.07269, 2017.
[26] Joshua A. Kroll, Nitin Kohli, and Deirdre K. Mulligan, "A Shared Lexicon for Research and Practice in Human Centered Software Systems," PLSC 2018 Draft on file with author.

A list of Relevant U.S. laws, other instruments and case law has been included in Annex 1.

4.1 Methodology

The method of research included primary and secondary sources, as well as interviews with experts in each domain (additional interviews have been conducted as part of the legal analysis to ensure that both industry and regulator views are included for each area analysed) to provide greater understanding of how the relevant protections operate in practice.

4.2 Background

The European Union has long been concerned with automated decisions. Article 15 of the 1995 Data Protection Directive (DPD), the precursor to the General Data Protection Regulation (GDPR), required Member States to "grant the right to every person not to be subject to decision which … is based solely on automated processing of data … ."[27] The right not to be subject to automated decision-making has been carried over from the DPD to the GDPR. The specific contours of the right - enshrined in GDPR Article 22 - have been subject to much debate and analysis.[28] Importantly, in 2017 the Article 29 Working Party[29] released a draft guidance document on automated decision-making under the GDPR which was adopted in final form in February 2018.[30] The WP29 Guidance, discussed in more detail below, provides the Working Party's interpretation of Article 22, including definitions of

[27] The full text of DPD Article 15(1) provides: "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." However, DPD Article 15 received scant attention and "played an extremely modest, if not marginal role in the operation of European data protection law." Isak Mendoza and Lee A. Bygrave, The Right not to be Subject to Automated Decisions based on Profiling, University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20 (2017).

[28] The debate has included whether Article 22 creates a blanket prohibition on, as opposed to a right to opt out of, automated processing (Andrew Burt and Stuart Shirrel, Why we're concerned about the WP29's guidelines on machine learning, IAPP Privacy Perspectives, December 2017, available at https://iapp.org/news/a/why-were-concerned-about-the-wp29s-guidelines-on-machine-learning/) and whether the GDPR provides for a right to explanation of automated decision-making (Sandra Wachter et al., Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, 7 International Data Privacy Law 76 n.1-3 (2017)).

[29] The WP29 was established by Article 29 of the DPD. On May 25, 2018, the WP29 was replaced by the European Data Protection Board (EDPB). See European Commission Newsroom, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492.

[30] *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* ("WP Guidelines"). The WP Guidelines were endorsed by the EDPB in May 2018. See EDPB, Our Documents, available at https://edpb.europa.eu/node/71.

profiling and automated decision-making and the GDPR approach to these in general.

Each year, the European Commission conducts an annual review of the EU-US Privacy Shield, the framework for transfers of personal data between the E.U. and the U.S. The Privacy Shield became operational in August 2016, replacing the previous data transfer agreement known as the US-EU Safe Harbor Framework. In its 2017 annual review, the Commission identified a need to "assess the relevance of automated decision-making for transfers carried out on the basis of the Privacy Shield."[31] The two major tasks under this assessment are:

1. to understand whether U.S. companies that are certified under the Privacy Shield take decisions based solely on automated processing; and
2. assessing the protections offered by U.S. law for this kind of decisions and the conditions under which these protections apply.

4.3 Privacy and Data Protection in the U.S. and EU

The United States makes and interprets law using a dual system, one federal and one state.[32] This system is enshrined in the U.S. Constitution, which delegates certain powers to the federal government and reserves the rest for states.[33] The federal system is made up of three branches of government—executive, legislative, and judicial—and it is national, that is it applies to the U.S. as a whole. In the federal system, the legislative branch (US Congress) debates and enacts laws (often called statutes), while the judicial branch (US federal courts) settles disputes that arise under those laws. Often, Congress will enact laws that are general in nature and require additional rulemaking to be effective. Thus, a major function of the executive branch (federal agencies) is to develop and enforce those rules.

Most of the fifty states in the U.S. operate under a similar tripartite system, with their own executive, legislative and judicial branches. That means that in addition to the federal system, there are fifty different sets of state statutes, court decisions, and agency actions. Additionally, there are even smaller units of government in the form

[31] Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield of 18 October 2017, COM (2017) 611 final. The Commission's detailed findings on the functioning of the Privacy Shield are presented in the accompanying Staff Working Document (SWD (2017) 344 final).
[32] Lewis Mayers, The American Legal System (1964).
[33] U.S. Const. amend. X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people.").

of counties, cities, and towns that also might have systems that mirror those of the states and the federal government.

Although the U.S. operates under this dual system, laws enacted by the U.S. congress are the "supreme law of the land" and in general will take precedence over state action in the case of any conflict.[34] Given the supremacy of federal law in the US, as well as the fact that it is not practical here to address the approaches taken by all fifty states toward automated decision-making, this report will focus on relevant protections in federal law. Where relevant we will note applicable developments at the state or sub-state level, but overall we will analyse relevant legal protections at the federal level.

Information privacy in the commercial sector in the U.S. is protected through **sector-specific statutes**[35] and enforcement of **generic consumer protection laws**[36] to halt deceptive and unfair practices with regard to personal information in the commercial marketplace.[37] U.S. and state constitutional provisions, as well as state tort law[38] provide additional protections for privacy. The sector-specific federal and state statutes provide uneven protection for personal information and at times unequal treatment for the same personal information and similarly situated industry players.[39] Privacy protections, for example, often depend on the entity collecting personal information.

Self-regulation—backed up with enforcement by the FTC for companies who make commitments to comply with self-regulatory regimes and then fail to live up to their

[34] U.S. Const. Art. VI ("This Constitution, and the laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the authority of the United States, shall be the supreme law of the land; and the judges in every state shall be bound thereby, anything in the Constitution or laws of any State to the contrary notwithstanding.").

[35] See, e.g., Right to Financial Privacy Act (RFPA) of 1978, 12 U.S.C. §§ 3401-3422 (2006) (protecting the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records); Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. §§ 2510-2522 (extending restrictions against wiretaps to include transmissions of electronic data by computer); Video Privacy Protection Act (VPPA) of 1988, 18 U.S.C. §§ 2710-2712 (preventing disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual materials"); Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), 15 U.S.C. §§ 6801-6809, 6821-6827 (empowering various agencies to promulgate data-security regulations for financial institutions); Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.) and 45 CFR parts 160 and 164 (regulating the use and disclosure of "Protected Health Information").

[36] Federal Trade Commission Act. 15 U.S.C. § 41 et seq. And state unfair and deceptive acts and practices statutes (UDAPS)

[37] For a discussion of the U.S. information privacy regulatory landscape see Kenneth Bamberger and Deirdre K. Mulligan, Privacy on the Books and on the Ground, 63 Stan. L. Rev. 247 (2010); for an analysis of the content and impact of Federal Trade Commission activity on privacy see Solove, Daniel J., and Woodrow Hartzog. "The FTC and the new common law of privacy." *Colum. L. Rev.* 114 (2014): 583.

[38] Schwartz, Paul M. "The value of privacy federalism" in *Social dimensions of privacy: Interdisciplinary perspectives*, Roessler, Beate, and Dorota Mokrosinska, eds. Cambridge University Press, 2015.

[39] For example HIPAA's Privacy Rule regulates only the use and disclosure of certain information held by "covered entit[ies]," such as health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions. 45 C.F.R. § 164.502 (2010).

commitments— has been promoted by the federal government as an additional method of protecting information privacy.[40] A wide variety of approaches are taken under the generic category of self-regulation.[41] These include privacy **codes of practice** developed by industry, as well as those developed collaboratively or in consultation with civil society organizations.[42] This pattern of targeted legislation and pressure for self-regulation to protect privacy seems set to continue with privacy issues in machine learning and artificial intelligence.

Currently there are a number of efforts to develop guidelines to address issues including fairness, transparency, and explainability[43] that fall under this broad category of self-regulation.[44] (See also chapter 2.5)

In the US, information privacy is a subset of the broader, and multi-faceted, concept of "privacy."[45] This broader concept is protected through a variety of mechanisms, including the U.S. Constitution--for example the Fourth Amendment's prohibition on unreasonable searches and seizures, decisions upholding rights to abortion and the right of same sex couples to marry based on privacy concerns and grounded in various USC Amendments--as well as privacy interests protected under state-specific statutes, constitutional provisions and tort laws,[46] among others.

[40] See Executive Office of the President, Consumer Data Privacy in a Networked World (Washington DC, February 2012) (promoting codes of conduct to implement the Administration's proposed Consumer Privacy Bill of Rights through voluntary private sector participation). Available at https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.; and William J. Clinton & Albert Gore, Jr., A Framework For Global Electronic Commerce 4 (1997) (promoting self-regulation as the preferred approach to protecting online privacy); Rubinstein, supra note 21, at 5 ("Clinton officials generally favored the view that private sector leadership would cause electronic commerce to flourish, and specifically supported efforts to 'implement meaningful, consumer-friendly, self-regulatory privacy regimes' in combination with technology solutions.") Some have made dim assessments of the effectiveness of self-regulation. See e.g. Chris Hoofnagle, Privacy Self-Regulation: A Decade of Disappointment, Electronic Privacy Information Center (2005), at 2 ("Today's self-regulatory approaches to Internet privacy are much like the failed ones employed by the DMA for telemarketing. They are difficult to use, confusing, and often offer no real protection at all.").

[41] Colin Bennett and Deirdre Mulligan, The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy (2012). Available at SSRN: https://ssrn.com/abstract=2230369 or http://dx.doi.org/10.2139/ssrn.2230369

[42] Colin Bennett and Deirdre Mulligan, The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy (2012), at 6-7.

[43] See, Partnership on AI, which has as one of its goals the development of "best practices in the research, development, testing, and fielding of AI technologies." Available at https://www.partnershiponai.org/about/; Corinne Cath et al., Artificial Intelligence and the 'Good Society': the US, EU, and UK approach, Science and Engineering Ethics (2017) ("Self-regulatory partnerships … have been a staple of the US's regulatory approach to AI.").

[44] These efforts vary, and some are multi-stakeholder rather than industry-only initiatives.

[45] Solove DJ. 2008 Understanding privacy. Cambridge, MA: Harvard University Press; Post RC. 2000 Three concepts of privacy. Georgetown Law J. 89, 2087; Allen, Anita L. *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield, 1988; Mulligan, Deirdre K., Colin Koopman, and Nick Doty. "Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy." *Phil. Trans. R. Soc. A* 374.2083 (2016): 20160118.

[46] Restatement (Second) of Torts § 652A (1977)

States and municipalities play an active and important role in privacy protection. For example, security breach notification laws exist in all fifty states,[47] and while there is a specific breach notification requirement for health information at the federal level[48] there is no general statute. State protections for privacy vary. California, an important state due to the size of its population, economy, and the prevalence of information-intensive industry is considered a leader in privacy protection.[49] California has adopted numerous laws protecting privacy,[50] including several specifically focused on facilitating transparency into corporate data handling practices[51] and controlling law enforcement access to personal information held by corporations[52], as well as those that protect the privacy of minors with respect to technology.[53] Most recently, in June 2018, California passed the California Consumer Privacy Act, which, when it goes into effect in January 2020, will create new rights for California consumers, including the right to be informed about what kinds of personal information companies have collected and provides for a private right of action in the event of a data breach.[54]

But California is not alone in its effort to bolster privacy protection. Many states have enacted statutes to protect privacy in recent years and are currently considering bills to further expand privacy protection.[55] For example, in May 2018, Vermont enacted a law regulating data brokers that requires them to among other things inform consumers of the data they collect and provide instructions for opting out when that option is available.[56] At the local level, cities such as Berkeley and Oakland in California, Nashville, Tennessee, Seattle, Washington, and Somerville, Massachusetts have passed ordinances creating oversight over law enforcement acquisition of surveillance technology.[57]

---

[47] National Conference of State Legislatures, Security Breach Notification Laws, available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[48] 45 CFR §§ 164.400-414.
[49] L. Determann, California Privacy Law 2017: Practical Guide and Commentary U.S. Federal and State Law, forward by Paul Schwartz.
[50] For a list see California Department of Justice, available at https://oag.ca.gov/privacy/privacy-laws.
[51] Online Privacy Protection Act of 2003, California Business and Professions Code sections 22575-22579 (requiring posted privacy policies); Information-Sharing Disclosure, "Shine the Light," California Civil Code sections 1798.83-1798.84 (giving consumers a right to receive information about the categories of personal information companies disclose to other companies for marketing purposes or providing consumers a cost-free opportunity to opt-out of such information sharing).
[52] California Electronic Communications Privacy Act (CalECPA) - Penal Code section 1546 et seq. (requiring warrants for law enforcement to access personal information and communications on electronic devices or from online service providers)
[53] Digital Privacy Rights for Minors - California Business and Professions Code sections 22580-22582 (requiring among other things that minors be able to have content they have contributed to web sites removed).
[54] 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375)
[55] Many states are currently considering additional privacy protections. For a regularly updated snapshot of state level legislative activity see http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-and-security.aspx
[56] H.764, Act 171, An act relating to data brokers and consumer protection, (2018).
[57] Robyn Greene, How Cities Are Reining in Out-of-Control Policing Tech, Slate May 18, 2018, available at https://slate.com/technology/2018/05/oakland-california-and-other-cities-are-reining-in-out-of-control-police-technologies.html

The E.U. takes a comprehensive or omnibus approach to data protection.[58] E.U. law distinguishes between two different fundamental rights: the right to privacy of individuals and the right to data protection.[59] Data protection seeks to regulate the specific practice of processing personal data. It accepts that processing of personal data will take place, but creates safeguards to protect individual liberty when processing occurs.

4.4 Automated Decisions

4.4.1 Placing E.U. and U.S. Approaches to Automated Decision-Making in Context

The E.U. and the U.S. legal frameworks reflect different perspectives on the risks and benefits of automated decisions. Automated individual decision-making, including profiling, is specifically addressed in Article 22 of the GDPR. Article 22(1) provides that "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." The WP29 has interpreted this provision to mean that "as a rule, there is a general prohibition on fully automated individual decision-making, including profiling that has a legal or similarly significant effect[.]"[60] The WP29 bases this conclusion on language in Recital 71[61] as well as on the manner in which the GDPR is organized.[62]

In the U.S. there is no parallel to the EU's "general prohibition" on decisions based solely on automated processing that produce legal or similarly significant effects. However, over the last few years there has been significant interest in the U.S. in the implications of algorithms, "big data," artificial intelligence, and other tools and processes that play a role in automated decisions. The Executive Branch of the U.S.

[58] For a summary of the differences see Kenneth Bamberger and Deirdre K. Mulligan, Privacy on the Books and on the Ground, 63 Stan. L. Rev. 247, 256 (2010) (noting that in contrast to the EU, in the US, "regulation of the use and disclosure of personal information focuses on 'specific, sectoral activities,' such as credit reporting, health care, or electronic commerce").
[59] For an overview of these distinct rights and their legal basis see, Gellert, Raphael, and Serge Gutwirth. "The legal construction of privacy and data protection." *Computer Law & Security Review* 29.5 (2013): 522-530.
[60] WP Guidelines at 19. This interpretation caused some controversy, and scholars and practitioners have debated whether or not the WP29's interpretation is correct. See David Meyer, Did the WP29 misinterpret the GDPR on automated decision-making?, IAPP (November 2018), available at https://iapp.org/news/a/did-the-wp29-misinterpret-the-gdpr-on-automated-decision-making/. The comments to this article note that some member states interpreted DPD Article 15, the precursor to GDPR Article 22, as a prohibition (France, Germany, Austria, and the Netherlands), while others interpreted it as an opt-out (United Kingdom, Spain, Sweden, Denmark, and Greece).
[61] Recital 71 "implies that processing under Article 22(1) is not allowed generally" because it states that "decision-making based on such processing, including profiling, **should be allowed**" under the exceptions enumerated in Article 22. WP Guidelines at 20 (emphasis in original).
[62] See WP Guidelines Annex 2, at 34 ("Article 22 is found in a section of the GDPR called "Right to object and automated individual decision-making", implying that Article 22 is not a right to object like Article 21.").

government and some federal agencies have held workshops and released reports on various issues posed by these technologies.[63] At the municipal level, New York city formed an "Automated Decision Systems Task Force" in May 2018 to develop a process for reviewing the equity, fairness and accountability of "automated decision systems."[64] Nevertheless, discussions in the U.S. have tended toward promoting best practices or avoiding specific harms, such as discriminatory impacts, rather than the regulatory approach found in the GDPR.

History provides some explanation for the differences in how E.U. and U.S. view automated decision-making. In Europe, data processing, including automated processing, has been associated with the oppression of individuals and groups since the 1900s.[65] National data protection frameworks, such as those of France and Germany, reflected this experience and connect data protection to dignity and personality. These member state regimes in turn influenced developments in E.U. data protection law.[66] As a result, "[a] particular idea of dignity can be found in rulemaking processes across Europe that protected humans from being treated as data to be processed by machines."[67] Additionally, the concept of dignity can be found in the references and nested frameworks in which data protection professionals position data protection.[68] To preserve this dignity, the European approach seeks to ensure a "human in the loop as a regulatory tool to address the effects of automation[.]"[69]

The GDPR's general prohibition on solely automated decisions that have legal or similarly significant effects reflects the EC's ongoing concern with the potential for data processing and automated decision-making systems to blind decision-makers to the humans behind the data. In addition, keeping humans in the decision-making

[63] Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion? (January 2016); Executive Office of the President, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights (May 2016); Executive Office of the President, Preparing for the Future of Artificial Intelligence (October 2016); Executive Office of the President, Artificial Intelligence, Automation, and the Economy (December 2016);
[64]https://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by
[65] Meg Leta Jones, The right to a human in the loop: Political constructions of computer automation and personhood, Social Studies of Science Vol. 47(2) (2017), at 220.
[66] Abraham Newman, Protectors of Privacy: Regulating Personal Data in the Global Economy 74-75 (2008) ("[T]he EU data privacy directive can be traced to its roots in the historical sequencing of national data privacy regulation and the role that the resulting independent regulatory authorities played in regional politics.") Newman also documented the formidable, and indeed outsized, role member state Data Protection Authorities played in the creation of the structure and requirements of the DPD. Ibid. at 95.
[67] Meg Leta Jones, The right to a human in the loop: Political constructions of computer automation and personhood, Social Studies of Science Vol. 47(2) (2017), at 220.
[68] Bamberger, Kenneth A., and Deirdre K. Mulligan. *Privacy on the ground: driving corporate behavior in the United States and Europe*, 89-94, 129-132 MIT Press, 2015 (discussing data protection officers' positioning of data protection work against Nazi atrocities and ethical frameworks emerging from them in German and France respectively).
[69] Meg Leta Jones, The right to a human in the loop: Political constructions of computer automation and personhood, Social Studies of Science Vol. 47(2) (2017), at 224.

loop may address concerns with loss of human decision-makers' agency and skill,[70] both over- and under-reliance on automated systems,[71] and the confusion about responsibility[72] and diminished accountability[73] that may arise due to automation.

In contrast to the experience of the EU, "[p]ostwar American technology policy was defined by the idea of technological development as national progress and national survival."[74] To be sure, U.S. policy makers explored the risks posed by automated processing, and an influential U.S. Advisory Committee on Automated Personal Data Systems was convened in 1972 to study the impact of computer databanks on individual privacy.[75] However, the misuse of administrative and statistical data was at that time less of a concern in the U.S. than it was in Europe, where data protection laws reflect lessons learned during the Nazi and Gestapo regimes and sought to "prevent the reappearance of an oppressive bureaucracy that might use existing data for nefarious purposes."[76]

[70] Lee J.D., Seppelt B.D. (2009) Human Factors in Automation Design. In Nof S. (eds) Springer Handbook of Automation. Berlin: Springer (detailing how automation that fails to attend to how it redefines and restructures tasks, and the behavioral, cognitive, and emotional responses of operators to these changes, produce various kinds of failure, including those that arise from deskilling due to reliance on automation).

[71] See Goddard, Kate, Abdul Roudsari, and Jeremy C. Wyatt. "Automation bias: a systematic review of frequency, effect mediators, and mitigators." Journal of the American Medical Informatics Association 19.1 (2011): 121-127 (reviewing literature on automation bias in health care clinical decision support systems); Bussone, Adrian, Simone Stumpf, and Dympna O'Sullivan. "The role of explanations on trust and reliance in clinical decision support systems." Healthcare Informatics (ICHI), 2015 International Conference on. IEEE, 2015 (discussing research findings on automation bias and self-reliance) at p. 160.

[72] For an overview of research on technology-assisted decision-making and responsibility see Mosier, Kathleen L., and Ute M. Fischer. "Judgment and decision making by individuals and teams: issues, models, and applications." Reviews of human factors and ergonomics6.1 (2010): 198-256. Pp. 232-233.

[73] Nissenbaum, Helen. "Computing and accountability." Communications of the ACM 37.1 (1994): 72-81; Simon, Judith, "Distributed epistemic responsibility in a hyperconnected era." The Onlife Manifesto. Springer, Cham, 2015. 145-159.

[74] Meg Leta Jones, The right to a human in the loop: Political constructions of computer automation and personhood, Social Studies of Science Vol. 47(2) (2017), at 225.

[75] Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems. This was the first body to propose the code of Fair Information Practices (FIPs). Bamberger and Mulligan, at 21.

[76] David H. Flaherty. Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (1989), 373-74. Only recently have researcers uncovered convincing evidence of the release of identifiable microdata on Japanese Americans during World War II (Anderson and Seltzer 2007, 2005), something that the U.S. Census Bureau and its leadership have historically denied, see e.g. Habermann, Hermann. "Ethics, confidentiality, and data dissemination." Journal of Official Statistics 22.4 (2006): 599, at 600 (stating that "the Census Bureau did not violate the confidentiality provisions of the Census law. The Census Bureau's contributions to the Japanese War Relocation Program were statistical data and the assistance of an expert from the Census Bureau, Mr. Calvin Dedrick") and (distinguishing between the Census Bureau's disclosure of aggregate statistical data to the Western Defense Command for use in relocating Japanese American and the disclosure of individual records protected by the confidentiality provision, but acknowledging that inadvertent disclosure of individuals in small areas is possible in the former due to improper use of disclosure avoidance rules.) Ibid. Recently a former Director of the Census Bureau acknowledged such microdata disclosures, Kincannon, Charles. 53-54, 54 2009. "Comment on Article by Anderson and Seltzer". Journal of Privacy and Confidentiality 1 (1). https://doi.org/10.29012/jpc.v1i1.564.(identifying two documents summarizing the tabulations prepared during 1942 by the Census Bureau containing microdata disclosures of both demographic and economic data); responding to Anderson, Margo J., and William Seltzer. "Federal statistical confidentiality and business data: Twentieth century challenges and continuing issues." Journal of Privacy and Confidentiality 1.1 (2009), and then rejoinder Anderson, Margo J., and William Seltzer. "Rejoinder." Journal of Privacy and Confidentiality 1.1 (2009). Notably Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems states that "the Census Bureau could, and did, refuse to give out the names and addresses" citing legal prohibition Ibid. at 89.

Although the U.S. adopted numerous laws to protect privacy throughout the 1970s, none prohibits or limits the use of technology to process personal data or make automated decisions about individuals. Instead, the focus has been "on the benefits of accuracy, efficiency, and computational neutrality"[77] offered by automated processing. This concept of computational neutrality--the idea that machines can act with a level of impartiality based on objective criteria--is a recurring theme in the U.S. where automation and computation are often framed as a means to reduce explicit and implicit human bias on decisions.[78] Concerns with the biases embedded in the data are raised,[79] but—at least historically—did not alter the generally optimistic perspective on the technologies' potential to constrain the explicit and implicit biases of human decision makers. This emphasis on the perceived objectivity and neutrality of computational methods stems both from a framing of automation as progress, and at times a belief in its power to address the specific U.S. history of racial discrimination.[80] Thus, "[w]hile the person and people of Europe may be legally constituted as entities protected from automated decision-making and deserving of a human in the loop, those in the U.S. are protected from the flaws of humanity through the computational neutrality of information systems."[81] While U.S. and E.U. law share concerns with the implications of data processing and data-driven decision-making, U.S. law does not distinguish between different levels of human to solely automated decision-making.

4.4.2 GDPR Terminology Regarding "Automation"

The GDPR uses several different formulations to refer to decisions and processing that involve automation. Article 2 states that the GDPR "applies to the processing of

[77] Meg Leta Jones, The right to a human in the loop: Political constructions of computer automation and personhood, Social Studies of Science Vol. 47(2) (2017), at 226 (emphasis added).
[78] For example, state legislatures have moved aggressively to require the use of risk scoring in some contexts, particularly at sentencing, as an effort to improve fairness and the overall management of the criminal justice system. State v. Loomis Case Note, Harvard Law Review, Vol. 130, No. 5, March 2017. https://harvardlawreview.org/2017/03/state-v-loomis/ (Note 55). The MacArthur Foundation, through their Safety and Justice Challenge program, has funded the deployment of risk assessments across the country. From the perspective of these legislatures and the MacArthur and Arnold foundations, risk assessment tools are a means to reduce bias. For a study documenting biased decisions by judges, see Rachlinski, Jeffrey J., Sheri Lynn Johnson, Andrew J. Wistrich, and Chris Guthrie. "Does unconscious racial bias affect trial judges." Notre Dame L. Rev. 84 (2008): 1195.
[79] For an older example see, Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems at 243 (discussing the potential for the NCIC database of arrests without conviction data to magnify the consequences of discriminatory policing practices); and more recently, Executive Office of the President, et al. *Big data: A report on algorithmic systems, opportunity, and civil rights*. Executive Office of the President, 2016.
[80] See Josh Lauer, Creditworthy: A History of Consumer Surveillance and Financial Identity in America (2017) ("By the 1970s, many Americans, including many in the business community, believed that it was unethical to reduce creditworthiness to biology or skin color. … As a technological fix for the problem of discrimination, scoring systems seemed ideal.").
[81] Meg Leta Jones, The right to a human in the loop: Political constructions of computer automation and personhood, Social Studies of Science Vol. 47(2) (2017), at 231.

personal data wholly or partly by *automated means* … ."[82] Articles 21 and 22 both have "*automated individual decision-making*" in their titles. And Article 22(1) prohibits "decision[s] based solely on automated processing, including profiling." Recital 71 maintains this terminology, discussing decisions based "solely on *automated processing*", which data subjects have a general right to not be subjected to, and "*automated decision-making* and *profiling* based on special categories of personal data" which are only allowed under limited conditions.

The GDPR does not define "automated" or any of the phrases (*automated processing, automated decision-making, decisions based solely on automated processing*) in which the word is used. The WP29 defines "solely automated decision-making" as "the ability to make decisions by technological means without human involvement,"[83] and emphasizes that adding token human involvement is not enough to avoid this definition and thereby escape Article 22.[84] "*Processing*" is defined in the GDPR as a set of operations performed on personal data "whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction[.]"[85] "Profiling" is a subset of processing defined by its *automated nature and its use to "analyse or predict" a person's "performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*[.]"[86]

Given the text of the GDPR and the WP29 guidance documents, we understand "automated decision-making" and "automated individual decision-making" to be essentially the same, and will refer to this concept using the term "automated decision." Likewise, we will assume that "processing … by automated means" and "automated processing" have similar or identical meanings, and will use the term "automated processing" to refer to this concept.

4.4.3 Explanations required under the GDPR

[82] GDPR Article 2 (emphasis added). It also covers "the processing...of personal data which form part of a filing system or are intended to form part of a filing system."
[83] WP Guidelines at 8.
[84] WP Guidelines at 21.
[85] GDPR Article 4(2) (emphasis added).
[86] GDPR Article 4(4) (emphases added). "Automated processing" has been defined by the Council of Europe as including "the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination[.]" Article 2, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

When automated decisions are allowed under the contract or consent exceptions to Article 22, data controllers are required to implement "at least" the following safeguards: "the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[87] According to the WP29, "suitable safeguards should also include: ... specific information to the data subject and the right (…) to obtain an explanation of the decision reached after such assessment and to challenge the decision."[88]

The WP29 characterizes this 'right to explanation' as a "transparency requirement" that encompasses the obligations of controllers set forth in Articles 13-15: data subjects are entitled to know about "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." (Emphasis added.) The WP29 positions the right to obtain an explanation as a suitable safeguard—an instrumental right designed to support the data subject in expressing her point of view or challenging a *specific* decision based solely on automated processing.

To illustrate how a controller could satisfy its obligation to provide "meaningful information about the logic involved," the WP29 uses a scenario of a data controller who relies on credit scoring to assess and reject an individual's loan application. In that scenario, the controller provides details of the main characteristics considered in reaching the decision, the source of this information and the relevance. This may include, for example:

- the information provided by the data subject on the application form;
- information about previous account conduct, including any payment arrears; and
- official public records information such as fraud record information and insolvency records.[89]

Additionally, "[t]he controller provides contact details for the data subject to request that any declined decision is reconsidered, in line with the provisions of GDPR Article 22(3)," and finally the "controller also includes information to advise the data subject that the credit scoring methods used are regularly tested to ensure they remain fair, effective and unbiased."[90] It is unclear whether this last requirement is met merely by

[87] GDPR Article 22(3).
[88] WP Guidelines at 27 (emphasis added).
[89] WP Guidelines at 25-26.
[90] WP Guidelines at 26.

assertions, or if some additional detail is required to "advise the data subject" on these aspects of the scoring system.

As discussed in more detail below, the requirements set out in this example are similar to, if not less stringent than, those required by the Fair Credit Reporting Act and the Equal Credit Opportunity Act. Regardless, the example illuminates the WP29's perspective on the instrumental goals of situations where automated decisions are allowed under Article 22(2): ensuring data subjects have the information necessary to contest the specific decision and a human in the loop to ensure that the right to contest is operationalized.

The WP29's examples of appropriate explanations under Article 22 can support a data subject in contesting *a decision* but are not robust enough to support a challenge to *the model* that rendered it. The WP29's interpretation would bring the explanations required under the GDPR in relative alignment with those found in relevant U.S. law. If this interpretation is followed, the GDPR may deliver little additional information to subjects of automated decision-making than what is afforded under U.S. law, at least where credit information is involved. Unfortunately, such explanations fall short of providing data subjects the sort of "meaningful information about the "logic" of automated decision-making systems necessary to contest the choice of model a controller uses to reach supposedly "fair and responsible lending decisions,"[91] but rather only support data subject's right to contest the relevance or accuracy of specific inputs to the model and the resulting decision.[92]

An alternative interpretation of the GDPR would require information that would allow individuals to contest the *models* on which automated decisions are based. This interpretation facilitates data subjects taking issue with the rules chosen, or more broadly at the justifications for the rules chosen. If that is the goal, then data subjects will need additional information about how decisions are made. Examples of the sort of information which could assist data subjects include: a functional description of the model;[93] meaningful information about the underlying rationale for the model;[94] and,

[91] See WP Guidelines at 25.
[92] WP Guidelines at 25-26.
[93] Andrew D. Selbst & Julia Powles, Meaningful Information and the Right to Explanation, 7 INT'L DATA PRIVACY L. 233, 236 (2017) (Arguing that the GDPR requires a functional description of the rules governing decision-making because without such information data subjects cannot assert their substantive rights)
[94] For example, in draft guidance implementing the 21st Century Cures Act (Cures Act) which excludes certain kinds of software functions from medical-device regulations the U.S. Food and Drug Administration requires information about the underlying rationale of a clinical decision support system, among other things, to be provided to the user. Center for Devices and Radiological Health, "Clinical and Patient Decision Support Software: Draft Guidance for Industry and Food and Drug Administration Staff" at 8 (Washington, D.C.: U.S. Food & Drug Administration, December 8, 2017), https://www.fda.gov/MedicalDevices/DigitalHealth/ucm562577.htm.

"a description of the assumptions and limitations of the algorithm."[95] As we discuss below, data subjects and other stakeholders can understand the logic of an automated decision-making system at different depths based on different kinds of information.

The second part of the requirement in Articles 13-15 is that the controller provide information about the "significance and the envisaged consequences of such processing for the data subject." According to the WP29, this requirement creates a right to a more general kind of explanation of processing that has yet to take place:

> This term suggests that information must be provided about intended or future processing, and how the automated decision-making might affect the data subject. In order to make this information meaningful and understandable, real, tangible examples of the type of possible effects should be given.[96]

To illustrate how controllers can comply with this requirement, the Working Party uses an example of an automobile insurance provider that bases premium prices on customer driving behavior:

> To illustrate the significance and envisaged consequences of the processing it explains that dangerous driving may result in higher insurance payments and provides an app comparing fictional drivers, including one with dangerous driving habits such as fast acceleration and last-minute braking.
>
> It uses graphics to give tips on how to improve these habits and consequently how to lower insurance premiums.[97]

The precise contours of the explanations of automated decisions to which data subjects are entitled under the GDPR has been the subject of much debate over the last several years.[98] For purposes of this analysis, reading Recital 71, Articles 13-15,

---

[95] For example, staff guidance on Robo-Advisors from the SEC directs that robo-advisors should make disclosures to close potential gaps in a client's understanding of how investment advice is generated including "information regarding its particular business practices and related risks" and specifically the guidance suggests providing information about the function the algorithm performs and its underlying "assumptions and limitations." Securities and Exchange Commission, Division of Investment Management, Guidance Update: Robo-Advisors, No. 2017-02, p. 3 February 2017

[96] WP Guidelines at 26 (emphasis added).

[97] WP Guidance at 26.

[98] Maja Brkan, Do Algorithms Rule the World? Algorithmic Decision-making in the Framework of the GDPR and Beyond; Bryan Casey et al., Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the rise of Algorithmic Audits in Enterprise; Lilian Edwards & Michael Veale, Slave to the Algorithm? Why a 'right to an Explanation' is Probably not the Remedy you are Looking for, 16 DUKE L.& TECH. REV. 17, 44, (2017); Gianclaudio Malgieri & Giovanni Comandé, Why a right to Legibility of

and Article 22 together, as well as the WP29's guidance on automated decisions, we believe that the GDPR requires the following kinds of disclosures to data subjects where decisions based solely on automated processing, including profiling, which produce legal or similarly significant effects are permitted under Article 22(2)(a) and (c) are involved:

1. **Information about the system**: generalized meaningful information of the system and its logic;
2. **Information about the decision**: meaningful specific information about the logic and data that contributed to a particular, rendered decision about an individual; and
3. **Information about the consequences**: general information about potential consequences of an automated decision-making process.

Although in our interpretation the GDPR requires these three categories of information, the third category, while conceptually separable, is in practice often addressed in the information about the system in general or the decision specifically. For this reason, we will not address information about consequences as a separate category when analysing protections in U.S. law for solely automated decisions. Where relevant we will point out where disclosures might be considered to provide information about the consequences of a decision.

The right to information about particular automated decisions plays an instrumental role in safeguarding the other safeguards available under Article 22(3):

- The right to obtain human intervention on the part of the controller;
- The right to express his or her point of view; and,
- The right to contest the decision.

With this framework established, we now explore the statutes, regulations, and relevant case law that govern areas where automated processing is potentially used

Automated Decision-Making Exists in the General Data Protection Regulation; Andrew D. Selbst & Julia Powles, Meaningful information and the right to explanation, 7:4 INT'L DATA PRIVACY L. 233 (2017); Selbst & Barocas, Intuitive Appeal, supra note ; Sandra Wachter, Brett Mittelstadt, & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7:2 INT'L DATA PRIVACY L. 76 (2017); Margot E. Kaminski, The Right to Explanation, Explained, U of Colorado Law Legal Studies Research Paper No. 18-24 (2018).

to support decision-making in contexts that can have “serious impactful effects” and compare them to the GDPR objectives with respect to fully automated processing.

5 Consumer Credit

GDPR Article 22(1) provides data subjects with the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significant effects. Profiling is a type of automated processing where personal data are used to predict a person's behavior.[99] Profiling can occur through companies' collection and analysis of personal data on a large scale, using algorithms, AI or machine-learning.[100]

One sector in the U.S. where automated processing and profiling have proliferated is the consumer credit system. Consumer files held by consumer reporting agencies (CRAs) are often created or maintained using matching algorithms or algorithms that assign personal identification numbers to consumers and link them to pieces of consumer information provided by furnishers.[101] Additionally, credit scores represent perhaps the canonical example of an attempt to predict how a person will behave. Credit risk scores--and likely most other kinds of credit scores are "calculated from an algorithm or mathematical model."[102]

There are a number of federal statutes that regulate the credit industry.[103] For our purposes we will focus on the Fair Credit Reporting Act (FCRA) and the Equal Credit Opportunity Act (ECOA), which are the most relevant to the GDPR's requirements for automated decisions. The FCRA focuses on informing consumers that their personal information is being used for credit, employment, and other legal or similarly significant decisions, and the ECOA focuses on ensuring that applicants for credit are not discriminated against on the basis of protected characteristics such as race or gender.

The FCRA and the ECOA apply regardless of whether a covered decision is "solely" automated, partially automated, or manual. However, given the prevalence of automated processing and automated decisions in the context of credit, the requirements imposed by these statutes are relevant to the question of what

[99] GDPR Article 4(4).
[100] UK ICO, What is automated individual decision-making and profiling?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/.
[101] CFPB, Key Dimensions and Processes in the U.S. Credit Reporting System, December 2012, at 22, available at https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf.
[102] National Consumer Law Center, Fair Credit Reporting § 16.2.2.2 (9th ed. 2017). Consumer reports, credit scores, and other relevant concepts are discussed in more detail below.
[103] These include statutes that regulate credit terms, such as the Truth in Lending Act, which also includes the Credit CARD Act, as well as federal regulators' guidance for banks involved in payday lending, see OCC Advisory Letter No. 2000-10 (Nov. 27, 2000), available at www.occ.gov. State laws may also regulate credit terms, especially when non-bank lenders are involved.

protections are available under U.S. law for decisions based solely on automated processing, including profiling.

While the regulation of credit might at first appear to be a rather narrow area of regulation, it actually has broad effects across the areas of credit and finance, employment, insurance, and housing. Credit decisions are a key output, often automated, used across contexts with legal or similar significant impacts. Therefore, the FCRA and the ECOA are important frameworks that offer protections where solely automated decisions are taken.

Box 2 Treatises of the National Consumer Law Center

This report relies heavily on two treatises published by the National Consumer Law Center (NCLC): Fair Credit Reporting (9th ed. 2017), and Credit Discrimination (7th ed. 2018). The NCLC is a nonprofit organization whose mission is to work for consumer justice and economic security for low-income and other disadvantaged people. Its treatises are used by courts and scholars interpreting laws related to consumer protection.

5.1 Fair Credit Reporting Act (FCRA)

5.1.1 Background and Terminology

By the late 1960s, the credit reporting industry in the U.S. had reached an enormous scale. Credit reporting agencies maintained credit files on over 110 million people, or over half the 1968 U.S. population, and in 1967 these agencies issued over 97 million credit reports.[104] Despite the industry's size, it operated largely without regulation, and most Americans at that time did not realize how big the industry was or how much information credit reporting agencies maintained and distributed.[105] According to Senator William Proxmire, the author of SB 823, the bill that became the FCRA, "the increasing volume of complaints makes it clear that some regulations are vitally necessary to insure that higher standards are observed with respect to the information in the files of commercial credit bureaus."[106]

[104] 115 Cong. Rec. 2410 (1969).
[105] 115 Cong. Rec. 2410 (1969).
[106] 114 Cong. Rec. 24,902 (1968).

Senator Proxmire's main concerns were with the accuracy, relevancy, and confidentiality of information in consumer credit files.[107] He noted that "credit bureaus frequently confuse one individual with another, sometimes with tragic results." He highlighted that credit reporting agencies often denied credit on the basis of irrelevant offenses committed years or decades prior. And he was "disturb[ed by] the lack of any public standards to insure that the information is kept confidential and used only for its intended purpose."[108] Indeed, protecting consumer privacy was one of the main goals of the FCRA, as highlighted in the Congressional findings at the beginning of the statute.[109]

Congress recognized that credit reporting agencies played a "vital role" in the operation of the U.S. credit system.[110] Yet they also wanted "to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[111] Through the FCRA Congress sought to strike a balance between allowing the collection and dissemination of credit information about consumers while ensuring that that information was accurate, up to date, and used for appropriate purposes.

Whether Congress successfully struck the balance is a matter of debate, and the effort has continued over the years through several amendments to the statute. The two most significant amendments are the Consumer Credit Reporting Reform Act of 1996 (CCRRA) and the Fair and Accurate Credit Transactions Act of 2003 (FACTA).[112] The CCRRA amendments expanded the duties of "consumer reporting agencies" (CRAs) (commonly referred to as "credit bureaus") as well as "users" of consumer reports, and created new duties for "furnishers" of information to CRAs.[113] The FACTA amendments "added several sections to assist consumers and businesses in combating identity theft and reducing the damage to consumers when that crime occurred."[114]

The FCRA primarily regulates (1) "consumer reporting agencies," (2) those who "use"[115] information compiled by consumer reporting agencies (CRAs) (for example,

[107] 115 Cong. Rec. 2410, 2411 (1969).
[108] 115 Cong. Rec. 2410, 2413 (1969).
[109] 15 USC § 1681(a)(4) ("There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.").
[110] 15 USC § 1681(b).
[111] 15 USC § 1681(a).
[112] Pub. L. No. 108-159 (Dec. 4, 2003).
[113] FTC, Forty Years of Experience With the Fair Credit Reporting Act (July 2011), 2-3. CRAs, users, and furnishers are discussed in more detail below.
[114] FTC, Forty Years of Experience With the Fair Credit Reporting Act (July 2011), 3
[115] The FCRA does not define the term "users." In general it means "anyone receiving a consumer report and applying it to a consumer[.]" National Consumer Law Center, Fair Credit Reporting § 7.1.4.2 (9th ed. 2017).

first party lenders, such as banks), and (3) those who provide information to CRAs (generally referred to as "furnishers"[116]). The use of "consumer reports" that CRAs create are limited to certain specific purposes, which include determining eligibility for credit, insurance, employment, and governmental licenses, among others.[117] It requires CRAs to follow reasonable procedures to keep consumer information accurate and updated, provides access and correction rights to consumers, and includes remedies to consumers where they are impacted by consumer reports.[118] Of particular relevance to GDPR Article 22, the FCRA requires disclosures to consumers, that help to explain the credit system and the logic of credit scores.

5.1.1.1 Consumer Reports

A "consumer report" is (1) any "communication of any information by a consumer reporting agency" that (2) "bear[s] on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living," and (3) is "used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for" one or more of several purposes specifically enumerated in the statute.[119] These purposes include when "credit or insurance [is] to be used primarily for personal, family, or household purposes," employment purposes,[120] or where a user has a legitimate business need for the information in connection with a business transaction that is initiated by the consumer.[121]

Beyond the three-prong definition set out above, **"consumer report" is a broad term that encompasses many different kinds of reports**. It includes a "credit report"--consumer reports focused on consumer credit information--as well as employment and tenant reports. Reports based on information such as social media activity, spending patterns, educational background, and phone service history could be consumer reports. Reports that track specific purchases can also be included in this definition (for example, creditors believe that people who buy cheap motor oil

[116] "'Furnishers' are creditors, debt collectors, and other third parties who provide information about consumers to the CRAs." National Consumer Law Center, Fair Credit Reporting § 2.1.2 (9th ed. 2017). There is one broad category that permits the use of consumer reports when a user has a "legitimate business need for the information—(i) in connection with a business transaction that is initiated by the consumer." 15 USC § 1681b(a)(3)(F).
[117] 15 USC § 1681a(d), 1681b.
[118] See 15 USC § 1681n-o.
[119] 15 USC § 1681a(d). See Ernst v. Dish Network, LLC, 49 F. Supp. 3d 377, 381 (S.D.N.Y. 2014) (listing elements).
[120] 15 USC § 1681a(d).
[121] 15 USC § 1681b(a)(3)(F).

are a higher credit risk than those who purchase carbon monoxide monitors[122]). Finally, one of the most important aspects of credit reporting, the credit score, is included in the definition of a consumer report.[123]

5.1.1.2 Consumer Reporting Agencies

CRAs are defined as any entity that "regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties … ."[124] This is a functionally defined set of entities, allowing the statute to cover new entries in the marketplace that engage in this activity. The most common conception of a CRA is one of the so-called "nationwide CRAs"-- Equifax, TransUnion, and Experian.[125] However, the definition is broad enough to include other entities that produce consumer reports such as tenant screening bureaus, check approval services, and employment screening agencies, which can also fall within the definition of a CRA.[126] These are often referred to as "specialty CRAs."

In addition to specialty CRAs, other entities, such as data aggregators, can fall within the definition depending on how they market their services. For example, in 2012 the FTC levied an $800,000 penalty on Spokeo,[127] a data aggregation company that collects personal information about consumers from numerous data sources and creates profiles with information on consumers' names, addresses, age ranges, as well as details about their hobbies, ethnicity, religion, use of social media, and photos.[128] According to the FTC, "Spokeo marketed those profiles to human resources professionals, job recruiters, and others as an employment screening tool" and invited recruiters to "explore beyond the resume."[129]

---

[122] Charles Duhigg, What Does Your Credit-Card Company Know About You?, New York Times, May 12, 2009, available at https://www.nytimes.com/2009/05/17/magazine/17credit-t.html.
[123] FTC, Forty Years of Experience With the Fair Credit Reporting Act (July 2011) (stating that the term "consumer report" also "includes numerical or other evaluation of data by a CRA, such as a credit score that bears on a consumer's creditworthiness), available at https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.
[124] 15 USC § 1681a(f).
[125] Searches under the Privacy Shield Framework portal (https://www.privacyshield.gov/list) for "Equifax" and "TransUnion" did not return any results, suggesting that these companies have not self-certified under the Privacy Shield. A search for "Experian" reveals Experian Holdings, Inc. is an active participant, suggesting that Experian has self-certified under the Privacy Shield.
[126] National Consumer Law Center, Fair Credit Reporting § 1.2.1 (9th ed. 2017). In this report we rely extensively on treatises published by the National Consumer Law Center (NCLC).
[127] Spokeo does not appear to have self-certified under the Privacy Shield.
[128] Leslie Fair, Speaking of Spokeo: Part 1, FTC Business Blog (June 2012), available at https://www.ftc.gov/news-events/blogs/business-blog/2012/06/speaking-spokeo-part-1.
[129] Leslie Fair, Speaking of Spokeo: Part 1, FTC Business Blog (June 2012), available at https://www.ftc.gov/news-events/blogs/business-blog/2012/06/speaking-spokeo-part-1.

The FTC first concluded that Spokeo was subject to the FCRA. It alleged that the consumer profiles that Spokeo created were "consumer reports" because they bore on a person's character and were used as a factor in determining eligibility for employment.[130] In providing consumer reports, Spokeo became a CRA that was subject to the requirements of the statute. The FTC then determined that Spokeo had failed to comply with several requirements of the FCRA. For example, Spokeo failed to maintain reasonable procedures to limit the furnishing of consumer reports for "permissible purposes" only and to use reasonable procedures to assure maximum possible accuracy of consumer report information. Additionally, Spokeo furnished consumer reports to persons that it did not have reason to believe had a permissible purpose to obtain the report.

One important aspect of the FTC's case against Spokeo was that "in 2010, Spokeo changed its website Terms of Service (TOS) to state that it was not a consumer reporting agency and that consumers may not use the company's website or information for FCRA-covered purposes."[131] Despite this change, Spokeo could not escape the FCRA's requirements. That is because the company did not revoke access to or otherwise ensure that existing users did not use the company's website or information for FCRA-covered purposes. What remains unclear after Spokeo is the extent to which to which the company's 2010 disclaimers can shield it from claims brought based on information used by employers after the TOS was changed.

In another case involving a data broker, years of litigation led to a change in the policies of a group of companies run by LexisNexis[132] that sold an identity reporting service called Accurint for Collections (Accurint).[133] "The Accurint database contains information on over 200 million people, and millions of Accurint reports are sold each year. For years, Lexis sold Accurint without complying with the FCRA, on the theory that Accurint is not a 'consumer report' that triggers the Act's protections."[134] Consumers filed a lawsuit against Lexis arguing that its Accurint reports were "consumer reports" subject to the FCRA.

Ultimately, the parties reached a settlement under which Lexis agreed to split Accurint into two products, one subject to the FCRA and the other free of FCRA requirements:

[130] Complaint, U.S. v. Spokeo, Inc., No. 12-05001 (C.D. Cal. June 7, 2012) at para. 12.
[131] Complaint, U.S. v. Spokeo, Inc., No. 12-05001 (C.D. Cal. June 7, 2012) at para. 11.
[132] Several of these companies have self-certified under the Privacy Shield. For more information see https://www.relx.com/~/media/Files/R/RELX-Group/documents/privacy-shield-notice.pdf.
[133] Berry v. Schulman, 807 F.3d 600, 605 (4th Cir. 2015).
[134] Berry v. Schulman, 807 F.3d 600, 605 (4th Cir. 2015).

The first, “Collections Decisioning,” will be treated as falling within the FCRA's “consumer report” definition. This means, among other things, that Collections Decisioning reports can be used only for permissible purposes under the FCRA, and so will be available only to buyers that have completed a detailed credentialing process. Consumers also will have the right to view the information in their reports, free of charge in certain circumstances, and to dispute information they believe to be inaccurate, all as provided by the FCRA.

The second suite of products, called “Contact & Locate,” is intended only for the “limited purpose of finding and locating debtors or locating assets,” and will not include any of the “seven characteristic” information that makes a communication a “consumer report.” Accordingly, “Contact & Locate” is not treated as subject to the FCRA, and the Agreement stipulates that “the Contact & Locate suite of products and services do not constitute ‘consumer reports' as that term is defined under the FCRA.” Nevertheless, consumers will be given certain FCRA-like protections in connection with Contact & Locate. For example, consumers will be able to obtain free copies of their Contact & Locate reports once each year, and they will be able to submit statements disputing the information they find.

Box 3 LexisNexis Accurint

LexisNexis’s Accurint product actually consists of several different products such as Accurint for Collections, Accurint for Government, and Accurint for Law Enforcement. According to LexisNexis, Accurint for Collections “delivers access to robust search tools that streamline skip trace efforts and pinpoint right-party contacts,” while Accurint for Government “enables government agencies to locate people, detect fraud, uncover assets, verify identity, perform due diligence and visualize complex relationships.” Accurint for Law Enforcement is designed to “locate suspects, witnesses and fugitives and quickly uncover assets.” LexisNexis claims that its Law Enforcement product is used by over 4,000 federal, state and local law enforcement agencies in the U.S. who through the product have “access to over 34 billion public and proprietary records.”

Although the court in Berry v. Shulman did not specifically rule on whether Lexis was a CRA, that case and the FTC’s action against Spokeo demonstrate that at least in theory the FCRA’s protections are broad enough to apply to a new breed of players in the credit market, such as social credit systems being aggressively rolled out in

China.[135] In practice, however, the statute's text creates limitations that might make it inapplicable to certain instances of automated decisions. For example, because only reports that pertain to an individual will be a "credit report," reports at the aggregate level, such as on the activities of a household or a neighborhood, or reports that purport to strip out personal information, may or may not be covered by the FCRA.[136]

Other limitations may be imposed by the manner in which courts interpret the statute. For example, in a recent case involving a research platform called CLEAR offered by the Thomson Reuters[137] company that "provides subscribers with access to proprietary and public records information for investigative purposes," the court decided that Thomson Reuters was not a CRA.[138] The court's interpretation was based "on reading the definition of CRA to turn on the relevant entity's subjective intentions … ." The court stated that while companies could not escape the FCRA simply by stating "But we're not a CRA!," Thomson Reuters's actions, including admonitions and disclaimers on its marketing materials, requiring its subscribers to agree in writing to not use CLEAR for prohibited purposes, and vetting its customers before providing them access to the platform through a credentialing process, demonstrated that Thomson Reuters did not intend the CLEAR reports to be credit reports and thus it was not a CRA.[139]

The CFPB is also monitoring the use of "alternative data" in making credit decisions. As part of its authority to facilitate consumer access to and innovation in consumer financial products, the CFPB issued a Policy on No-Action Letters (NAL Policy) in February 2016 to incentivize companies to develop new products in the face of regulatory uncertainty.[140] Under the NAL Policy, the CFPB reviews requests from companies developing financial products and decides whether to issue a No-Action Letter informing the requester that the CFPB does not have a present intention to recommend initiation of an enforcement or supervisory action. This decision is based on a variety of factors listed in the NAL Policy, including: the extent to which the requester's product disclosures to consumers enable consumers to meaningfully

[135] Shazeda Ahmed, Cashless Society, Cached Data: Security Considerations for a Chinese Social Credit System, The Citizen Lab, Jan. 24, 2017, available at https://citizenlab.ca/2017/01/cashless-society-cached-data-security-considerations-chinese-social-credit-system/.
[136] Mikella Hurley & Julius Adebayo, Credit Scoring in the Era of Big Data, 18 Yale J. L. & Tech. 148, 185 (2016).
[137] It is difficult to ascertain whether Thomson Reuters has self-certified under the Privacy Shield..
[138] Kidd v. Thomson Reuters Corp., 299 F. Supp. 3d 400, 402 (S.D.N.Y. 2017).
[139] Kidd v. Thomson Reuters Corp., 299 F. Supp. 3d 400, 405 (S.D.N.Y. 2017) (quoting Tony Rodriguez & Jessica Lyon, Background Screening Reports and the FCRA: Just Saying You're Not a Consumer Reporting Agency Isn't Enough, FTC BUSINESS BLOG (Jan. 10, 2013, 2:00 p.m.), https://www.ftc.gov/news-events/blogs/business-blog/2013/01/background-screening-reports-fcra-just-saying-youre-not).
[140] 81 Fed. Reg. 8686 (Feb. 22, 2016).

understand and appreciate the terms, characteristics, costs, benefits, and risks associated with the product; the extent to which evidence, including the requester's own testing, indicates that the product's aspects in question may provide substantial benefits to consumers; and the extent to which the requester controls for and effectively addresses and mitigates risks to consumers.

In 2017, the agency issued a No-Action Letter to Upstart,[141] "an online lending platform (sometimes referred to as a "marketplace") that enables people with limited credit or work history, among others, to obtain credit and/or obtain credit on better terms," requested a No-Action Letter.[142] The CFPB granted the request based on Upstart's application and a confidential Model Risk Management & Compliance Plan the company agreed to enter into.[143] The CFPB did not elaborate on the specific factors in the NAL Policy it relied on to reach its decision, but it did state that it would not be seeking enforcement of the Equal Credit Opportunity Act (the ECOA is discussed in more detail). Although the No-Action Letter specifically referenced the ECOA, the CFPB can also issue such letters in regard to the FCRA.

While some companies are specifically seeking the CFPB's guidance in developing new methods of measuring creditworthiness, others, such as Facebook,[144] are developing technologies that might be used for credit assessments in the future. As part of its efforts to combat fake news, Facebook is developing a "reputation score" that the company will use to predict the trustworthiness of its users.[145] According to Facebook, the reputation scores will help the company address the problem of users flagging posts as false simply because they disagree with the content of the post. If a user consistently flags posts as false when in fact they are true, the user's future feedback will be weighted less than other users whose feedback is considered more trustworthy.[146]

If Facebook only uses this information for internal purposes, the FCRA would not apply. However, if Facebook sells the information to third parties who could

[141] It does not appear that Upstart has self-certified under the Privacy Shield..
[142] Upstart Request for No-Action Letter (undated), available at https://files.consumerfinance.gov/f/documents/201709_cfpb_upstart-no-action-letter-request.pdf.
[143] Christopher M. D'Angelo, CFPB No-Action Letter (September 14, 2017), available at https://files.consumerfinance.gov/f/documents/201709_cfpb_upstart-no-action-letter.pdf
[144] Facebook has self-certified under the Privacy Shield. See https://www.facebook.com/about/privacyshield.
[145] Elizabeth Dwoskin, Facebook is Rating the Trustworthiness of its Users on a Scale from Zero to 1, Washington Post (August 21, 2018), available at https://www.washingtonpost.com/technology/2018/08/21/facebook-is-rating-trustworthiness-its-users-scale-zero-one/?noredirect=on&utm_term=.f4953b509e27.
[146] Elizabeth Dwoskin, Facebook is Rating the Trustworthiness of its Users on a Scale from Zero to 1, Washington Post (August 21, 2018), available at https://www.washingtonpost.com/technology/2018/08/21/facebook-is-rating-trustworthiness-its-users-scale-zero-one/?noredirect=on&utm_term=.f4953b509e27.

reasonably be expected to use the information for credit decisions, it would arguably fall within the definition of a CRA.[147]

5.1.2 Credit Scores

A credit score is a numerical value used to predict the likelihood that a consumer will engage in certain behavior, such as missing loan payments or entering into bankruptcy.[148] The most well-known kind of credit score is a "credit risk score" which is a number derived from information in a consumer's file at one of the nationwide CRAs. Credit risk scores are an example of a "generic" score used to anticipate consumer performance on a wide range of credit products.[149] There are also "industry" scores which are used to predict payment behavior for a specific type of credit, such as automobile or student loans, and "custom" scores, which large lenders develop internally to predict their customers' performance.[150]

The leading creator of models used to determine credit scores is a company called FICO.[151] As of 2010, FICO had over 90 percent of the market share of scores sold for use in credit-related decisions.[152] FICO creates 28 different kinds of scores, including industry scores used for car and mortgage loans, as well as credit card decisions.[153] FICO charges consumers $19.95 for a score based on a credit report from one of the nationwide CRAs or $59.85 for scores from all three.[154]

"The credit score may be the single most influential, critical piece of information associated with a consumer's file at a CRA."[155] Beyond their use as a tool for deciding whether to grant loans, credit scores are used for numerous other purposes. In the context of credit, some of these uses are:

> "to pre-screen and preselect consumers for direct marketing, to determine interest rates and credit limits, to collect on mortgage loans, and for sale of

[147] Adam Levitin, Facebook: The New Credit Reporting Agency?, Credit slips (August 21, 2018), available at http://www.creditslips.org/creditslips/2018/08/facebook-the-new-credit-reporting-agency.html.
[148] The FCRA defines a "credit score" as "a numerical value or a categorization derived from a statistical tool or modelling system used by a person who makes or arranges a loan to predict the likelihood of certain credit behaviors, including default (and the numerical value or the categorization derived from such analysis may also be referred to as a "risk predictor" or "risk score") … ." 15 USC § 1681g(f)(2)(A)(i).
[149] CFPB, The impact of differences between consumer- and creditor-purchased credit scores (July 2011), available at https://s3.amazonaws.com/files.consumerfinance.gov/f/2011/07/Report_20110719_CreditScores.pdf.
[150] CFPB, The impact of differences between consumer- and creditor-purchased credit scores (July 2011).
[151] FICO has self-certified under the Privacy Shield. See https://www.fico.com/en/newsroom/fico-joins-eu-us-privacy-shield-program-to-protect-clients-data-01-09-2017. The FICO acronym comes from "Fair, Isaac & Co.," the company's former name. For more background on FICO see Martha Ann Poon, What Lenders See—A History of the Fair Isaac Scorecard, (2013) (unpublished Ph.D. dissertation, University of California, San Diego), available at http://search.proquest.com/docview/1520318884.
[152] CFPB, The impact of differences between consumer- and creditor-purchased credit scores (July 2011).
[153] FICO, Understanding Fico Scores, available at https://www.myfico.com/Downloads/Files/myFICO_UYFS_Booklet.pdf.
[154] myFICO, One Time Credit Reports, available at https://www1.myfico.com/products/onetimereports.
[155] National Consumer Law Center, Fair Credit Reporting § 16.1 (9th ed. 2017).

> loans to Wall Street and secondary market purchasers. Some credit card issuers periodically review cardholders' credit scores to decide whether to re-issue the card or whether to raise a consumer's interest rate, which is a particularly controversial practice called "universal default." Payday lenders use specialty scores to determine whether to grant a payday loan. Scoring is also used to increase recovery rates from debt collection and to detect credit card fraud.[156]"

Additionally, some utilities use credit scores to decide whether consumers need to first pay a deposit to receive a utility service. Insurance companies also use credit scores to set rates for home and auto insurance, and employers may use them to differentiate job applicants.[157] Because the FCRA permits the use of consumer reports "in connection with a business transaction that is initiated by the consumer,"[158] there are likely few limits on when a credit score can be used for non-credit related purposes. Regardless of where consumer reports are used, however, the protections of the FCRA will apply.

5.1.3 FCRA Disclosure Requirements

Disclosure requirements form a pillar of the FCRA. They can be triggered in a number of different ways, including proactively by consumer request or reactively in response to a specific event covered by the statute. This section will discuss in detail the disclosures that are most relevant in the context of the GDPR.[159]

5.1.3.1 Background

The FCRA imposes disclosure requirements on CRAs and users of credit reports. These disclosures tell consumers that they have rights under the FCRA as well as what information about them is being disseminated and when a consumer report is used in ways that may negatively impact consumers. The disclosures required by the FCRA further the purposes of the statute by giving consumers information that they can act on to improve the accuracy of their files.

[156] National Consumer Law Center, Fair Credit Reporting § 16.3.2 (9th ed. 2017).
[157] CFPB, Key Dimensions and Processes in the U.S. Credit Reporting System, December 2012, available at https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf.
[158] 15 USC § 1681b(a)(3)(F)(i).
[159] The FCRA also requires numerous notices that will not be discussed in detail in this report. These include negative information notices, notices related to disputes under the FCRA, notice when information may be shared by affiliates, notices required of government agencies, and notices related to the possible fraudulent use of credit. For a detailed discussion of what these notices require see National Consumer Law Center, Fair Credit Reporting Chapter 8 (9th ed. 2017).

During his remarks introducing the bill that would become the FCRA, Senator Proxmire explained that inaccuracy in credit reporting was a major problem. He pointed out that it was difficult for consumers to deal with inaccuracies for at least three reasons. First, many consumers "are unaware of the existence of credit reporting agencies or of the fact that their file contains inaccurate information."[160] Second, many retailers did not inform consumers that a credit application had been rejected, leaving consumers unaware that any decisions had been made about them, much less what those decisions were based on. Third, and "most disturbing" to Senator Proxmire, was the fact that at the time it was common practice for contracts between CRAs and creditors to prohibit creditors from revealing the identity of CRAs to consumers.[161] This withheld information from consumers that limited opportunities to correct inaccuracies in CRA's files.

To help insure the accuracy of credit information he included a provision in the bill requiring CRAs to allow individuals to correct inaccurate or misleading information in their files.[162] Senator Proxmire explained that requiring disclosures by the CRAs was necessary to effectuate this provision:

> "In order to make the ... provision effective, creditors and other firms using credit reports would have to disclose to individuals that they are being rejected for credit, insurance, employment, and so forth, wholly or partly on the basis of a credit report when such is the case and to disclose the name and address of the credit reporting agency. In this way the individual is alerted to the existence of possible inaccuracies in his credit file and has an opportunity to take corrective action.[[163]]"

The FCRA requires notice from CRAs when they entered a derogatory item in a person's credit file based upon public records such as notices of judgments, suits, arrests. Senator Proximire explained that "this alerts the individual to the fact the credit bureau has recorded the adverse item" and allows the individual to take corrective action if necessary.[164]

The purposes of the FCRA as a whole and its disclosure requirements in particular are relevant to the manner in which the GDPR deals with automated decisions. Through the FCRA consumers are informed that a system of ranking them exists and

[160] 115 Cong. Rec. 2410, 2412 (1969).
[161] ibid.
[162] 115 Cong. Rec. 2410 (1969).
[163] 115 Cong. Rec. 2410, 2145 (1969) (emphasis added).
[164] 115 Cong. Rec. 2410 (1969).

they are allowed to have a voice in that ranking, at least with regard to ensuring that the information the ranking is based on is accurate.

5.1.3.2 Comparison of FCRA to GDPR

In Section I.C.3. above we distinguished three forms of information the GDPR requires controllers to provide to data subjects where solely automated decisions are made:

1. **Information about the system**: generalized meaningful information of the system and its logic;
2. **Information about the decision**: specific meaningful information about the logic and data that contributed to a particular, rendered decision about an individual; and
3. **Information about consequences**: general information about potential consequences of an automated decision-making process.

We also noted that we will not separately address the third category, information about consequences, when discussing relevant frameworks, given that this category is generally subsumed in requirements focused on the first two or not addressed at all. We now use this framework to analyze the protections afforded by the FCRA.

5.1.3.2.1 Information about the system

5.1.3.2.1.1 Consumer file disclosure

The FCRA provides a process for consumers to access information in their credit "file" from CRAs. The definition of a "file" under the FCRA is quite broad: "The term 'file', when used in connection with information on any consumer, means all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored."[165] When consumers make a request to the CRA for information in their file, CRAs are required to "clearly and accurately disclose to the consumer … [a]ll information in the consumer's file at the time of the

[165] 15 USC § 1681a(g).

request … ."[166] This information is to "be provided in a form that can be understood by the average consumer."[167]

Along with the actual information about the consumer that must be disclosed (e.g. bill payment history and account balances), the FCRA stipulates certain specific categories of information that must accompany the consumer's file. One category is the sources of the information in a consumer's file held by a CRA.[168] In practice this means that the identities of all "furnishers" must be disclosed, although the statute includes an exception for medical furnishers. Another category is the identity of each recipient of a consumer report on the consumer within the year prior to the consumer's request for disclosure.[169] "The disclosure of recipients shows up on a consumer file disclosure in the form of 'inquiries.'"[170] Additionally, the consumer file disclosure must also contain a summary of consumer rights to obtain and dispute information in consumer reports and to obtain credit scores.[171] It is important to note, however, that credit scores are not required to be disclosed as part of the consumer file disclosure.[172]

CRAs are also required to "provide trained personnel to explain to the consumer any information" that is disclosed as part of the consumer file disclosure.[173] "The CRA's employees must be prepared to make thorough and efficient disclosures and to answer questions concerning the items disclosed."[174] CRAs have run into compliance issues with this requirement and have paid fines and entered into consent decrees as a result.[175]

Overall, this disclosure helps data subjects gain some understanding of how the system works. As the WP29 states to meet the obligations Article 15(1)(h) GDPR "the

[166] 15 USC § 1681g(a). Despite the broad definition of a "file," CRAs often do not disclose "all information," a practice which courts have upheld over the years based on a narrow interpretation of what constitutes a "file" under the FCRA. One of the major cases in this mold is Gillespie v. Trans Union Corp., 482 F.3d 907 (7th Cir. 2007), in which the court held that the date of delinquency assigned to a debt need not be disclosed because it did not fall within the FCRA's definition of a "file." *See also* Shaw v. Experian Info. Sols., Inc., 891 F.3d 749 (9th Cir. 2018) (following *Gillespie v. Trans Union*).
[167] Gillespie v. Equifax Info. Servs., 2008 WL 4316950, at *7 (N.D. Ill. Sept. 15, 2008) (quoting S.Rep. No. 104-185, at 42-43 (1995)).
[168] 15 USC § 1681g(a)(2).
[169] 15 USC § 1681g(a)(3). If the consumer report was obtained for employment purposes, the time frame for disclosure is two years from the date of the request.
[170] National Consumer Law Center, Fair Credit Reporting § 3.5.4.3 (9th ed. 2017).
[171] 15 USC § 1681g(c).
[172] 15 USC § 1681g(a)(1)(B) ("[N]othing in this paragraph shall be construed to require a consumer reporting agency to disclose to a consumer any information concerning credit scores or any other risk scores or predictors relating to the consumer").
[173] 15 USC § 1681g(h).
[174] National Consumer Law Center, Fair Credit Reporting § 3.6.3 (9th ed. 2017).
[175] See United States v. Experian Info. Solutions, Inc., CA 3-00CV0056-L (N.D. Tex. Jan. 12, 2000) (consent decree); Chris Hoofnagle, How the Fair Credit Reporting Act Regulates Big Data, Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet, 2013. Available at https://ssrn.com/abstract=2432955.

controller should provide the data subject with information about the envisaged consequences of the processing, rather than an explanation of a particular decision … The controller should provide the data subject with general information (notably, on factors taken into account for the decision-making process…) ."[176] The provisions give consumers information about the data in their file, the sources from which it was obtained, and entities that have accessed their file. Together, this information provides consumers with general information about the kinds of information used to make determinations, where it comes from, and implicitly given the record of "inquiries", the sorts of activities that are affected by creditor reports.

5.1.3.2.1.2 Notice accompanying request for a consumer's credit score

In the U.S., CRAs are required to disclose credit scores upon a consumer's request.[177] With certain exceptions, CRAs are allowed to charge for the score they disclose to consumers. The FCRA requires that the purchased score be accompanied by a disclosure that includes the following information:

- The current credit score of the consumer or most recent credit score that was previously calculated by the CRA related to the extension of credit.
- The range of possible credit scores, e.g., 400 to 900, produced by the scoring model that generated the disclosed credit score.
- The key factors that adversely affected the credit score of the consumer, listed in order of impact. The CRA cannot provide more than four key factors, unless one of the factors is the number of "inquiries," in which case that factor must be included notwithstanding the four factor limit. FICO assists CRAs and users in disclosing key factors by providing "reason codes" that can be used to explain why a credit score is not higher.[[178]]
- The date on which the credit score was created.
- The name of the provider of the credit score or the credit file used to generate the score.
- A statement indicating that the information and credit scoring model may be different than the credit score used by a lender.[179]

[176] WP Guidelines at 27
[177] 15 USC § 1681g(f)(4).
[178] FICO provides over 50 reason codes, which are listed in CoreLogic CREDCO, Understanding Credit & Credit Risk Scores 17–25 (2011), available at www.credco.com. These include "Too few bank revolving accounts"; "Too many bank or national revolving accounts"; "Number of revolving accounts"; and "Length of time accts have been established." These reasons are either contradictory or do not tell consumers which direction they should aim in order to improve their credit.
[179] 15 USC § 1681g(f)(1); National Consumer Law Center, Fair Credit Reporting § 16.4.1.2 (9th ed. 2017).

The last requirement is critical information for consumers because CRAs have wide latitude in regard to the specific scores they sell. This is because CRAs are allowed to "supply the consumer … with a credit score that assists the consumer in understanding the credit scoring assessment of the credit behavior of the consumer and predictions about the future credit behavior of the consumer[.]"[180] Under this broad authority, CRAs often sell "educational scores," which were originally developed for use by lenders but now may not be used by lenders at all,[181] or a "VantageScore," a score developed by joint venture of Equifax, Experian, and TransUnion to compete with FICO.[182]

In practice this means that the score a consumer--call him Consumer A--purchases may not be the same as the score for Consumer A that a lender purchased to make a credit decision about him. In a study of these differences conducted by the CFPB in 2012, the agency found that approximately 20 percent of consumers who purchased a score from a CRA would receive a score that was meaningfully different from the score that a lender purchased about them.[183] This in turn could lead consumers to waste time applying for credit they will not receive or overpaying for credit when they could shop around for better terms.

Additionally, the FCRA only requires the CRAs to disclose risk scores that predict credit behavior. The CRAs have no obligation to disclose any other type of credit score, such as specialty scores.[184] This form of access to credit scores provides consumers with some more detailed yet general—in that it is not about how a particular decision was rendered—knowledge about how they may fare under a particular credit scoring model. The difficulty is that consumers have no way of knowing whether the credit scoring model presented to them is *the one*, or *similar* to the one, that will be used to make a decision about them at a later date. Finally, while the score can give a consumer information about how they fare under a particular model, the FCRA does not require explanations of how the score influences the ultimate decision a lender makes, because the decision may be based on additional

[180] 15 USC § 1681g(f)(7)(A).
[181] CFBP, Analysis of Differences between Consumer- and Creditor-Purchased Credit Scores, September 2012, available at https://files.consumerfinance.gov/f/201209_Analysis_Differences_Consumer_Credit.pdf.
[182] CFPB, The impact of differences between consumer- and creditor-purchased credit scores, July 2011, at 7.
[183] CFBP, Analysis of Differences between Consumer- and Creditor-Purchased Credit Scores, September 2012, available at https://files.consumerfinance.gov/f/201209_Analysis_Differences_Consumer_Credit.pdf. One expert challenged this based on an understanding that the scores disclosed to consumers are those the CRA believes to be the best and most broadly representative of the consumer's overall credit situation, even though they may vary from those sold to mortgage companies, payday lenders, and insurers, and that the variations among these scores for any one consumer are modest.
[184] National Consumer Law Center, Fair Credit Reporting § 16.4.1.4 (9th ed. 2017)

information. Explanations of the overall lending decisions are only required under the Equal Credit Opportunity Act, which is narrower in scope of coverage, and discussed in more detail below.

5.1.3.2.1.3 Pre-screening Notices

Another notice requirement in the FCRA is for pre-screening, a form of marketing that companies use to solicit new consumers. "Prescreening is the process whereby consumer reporting agencies compile or edit lists of consumers who meet specific criteria, often specified by the user [generally a lender], and then provide the lists to [lenders] who solicit consumers with firm offers for credit and for insurance purposes."[185] The solicitation must be a "firm offer," that is an "offer ... that will be honored if the consumer is determined, based on information in a consumer report on the consumer, to meet the specific criteria used to select the consumer for the offer … ."[186]

Pre-screening is only allowed in connection with credit or insurance transactions.[187] The FCRA provides a mechanism for consumers to opt out of pre-screening either by calling or writing to a CRA.[188]

Solicitations for pre-screened offers of credit or insurance must be accompanied by pre-screening notices. According to the National Consumer Law Center, the notice serves two purposes:

> "First, it provides the consumer with information about the immediate transaction. The consumer is given to believe that they preliminarily qualify for the offered transaction, but is warned that if they respond, further evaluation may determine that the consumer does not qualify after all. This is a partial description of how pre-screening is allowed to work.
>
> The second purpose of the notice has broader applicability. It informs consumers that their consumer reports have been used. This should alert the consumer to the fact that personal information has been collected and is

[185] National Consumer Law Center, Fair Credit Reporting § 8.8.1 (9th ed. 2017) (emphasis added).
[186] 15 USC § 1681a(l). The FCRA allows firm offers to be further conditioned on other criteria as set forth in 15 USC § 1681a(l).
[187] 15 USC § 1681b(c).
[188] 15 U.S.C. § 1681b(e)(2).

being used, and that consumer may wish take steps to ensure the accuracy of that information."[189]

The notice must contain the following information:

- "information contained in the consumer's consumer report was used in connection with the transaction;
- the consumer received the offer of credit or insurance because the consumer satisfied the criteria for credit worthiness or insurability under which the consumer was selected for the offer;
- if applicable, the credit or insurance may not be extended if, after the consumer responds to the offer, the consumer does not meet the criteria used to select the consumer for the offer or any applicable criteria bearing on credit worthiness or insurability or does not furnish any required collateral;
- the consumer has a right to prohibit information contained in the consumer's file with any consumer reporting agency from being used in connection with any credit or insurance transaction that is not initiated by the consumer; and
- the consumer may exercise the right referred to in subparagraph (D) by notifying a notification system established under section 1681b(e) of this title."[190]

The notice must be "clear and conspicuous, and simple and easy to understand."[191] The CFPB has created a list of factors to be considered in determining whether a pre-screening notice meets this standard. These factors include the use of: short explanatory sentences; definite, concrete, everyday words; active voice; and language that is not misleading. Additionally, they include avoidance of: multiple negatives; legal and technical business terminology; and explanations that are imprecise and reasonably subject to different interpretations.[192]

Notably, there is no requirement that the user explain why the consumer received the specific offer.

5.1.3.2.2 Information about decisions

[189] National Consumer Law Center, Fair Credit Reporting § 8.8.2.1 (9th ed. 2017) (emphasis added).
[190] 15 USC § 1681m(d)(1).
[191] 12 C.F.R. § 1022.54(c).
[192] 12 C.F.R. § 1022.54(b)(1).

In addition to the notices described above, there are certain instances where the FCRA places additional requirements on the information that must be provided to consumers. The major instances where this occurs are when: credit scores are used for mortgage decisions; a user takes an adverse action based on a consumer report; creditors make changes to credit terms (risk-based pricing); and credit information is used to make employment decisions.

5.1.3.2.2.1 Mortgage Notices

Mortgage lenders will often use a credit score to evaluate an application for credit secured by residential real estate. In such cases, the general rule is that they are **required to provide the actual credit score they used as well as a notice containing the information about credit scores discussed** above (e.g. the range of scores, the factors that affected the scores, etc.).[193] This is in contrast to situations where CRAs are allowed to provide an educational credit score because the consumer has requested a credit score on his own initiative. In addition to the notice containing the information about credit scores discussed above, mortgage lenders are also required to include a "Notice to home loan applicants" that includes **background information about credit scores**.[194]

An important tool used in the mortgage lending is automated underwriting systems. Automated underwriting is a blanket term that generally applies to the process of creating a *mortgage rating* and issuing an approval or denial decision for a borrower based on her credit score (traditionally the FICO score) as well as her ability to carry debt and a collateral assessment using a statistical appraisal of property.[195] Automated underwriting is promoted by "[t]he two government-sponsored enterprises [(GSE)] that dominate the conventional mortgage markets, the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Corporation (Freddie Mac) … ."[196] In fact, these GSEs have developed their own automated decisioning models that they require mortgage lenders to use in the underwriting

[193] 15 U.S.C. § 1681g(g)(1)(A).
[194] 15 USC § 1681g(g)(D). The text of the "Notice to home loan applicants" is provided in the FCRA. For example, the notice provides that "The scores are based on data about your credit history and payment patterns. Credit scores are important because they are used to assist the lender in determining whether you will obtain a loan."
[195] Wayne Passmore and Roger Sparks, The Effect of Automated Underwriting on the Profitability of Mortgage Securitization (Draft, April 8, 1997), at 4, available at SSRN: https://ssrn.com/abstract=36643 or http://dx.doi.org/10.2139/ssrn.36643.
[196] Wayne Passmore and Roger Sparks, The Effect of Automated Underwriting on the Profitability of Mortgage Securitization (Draft, April 8, 1997), at 5, available at SSRN: https://ssrn.com/abstract=36643 or http://dx.doi.org/10.2139/ssrn.36643.

process. If the mortgage score meets a certain threshold, the GSEs will agree to buy the loan; if it does not, the loan may be referred to "manual underwriting."[197]

A new development in automated underwriting occurred recently with the enactment of the Economic Growth, Regulatory Relief, and Consumer Protection Act (ERCP Act),[198] which was signed into law in May 2018. The ERCP Act in part addresses the current status quo of relying on FICO scores for the credit scoring portion of the GSEs' mortgage scoring model. The ERCP Act opens the door to the use of credit scoring models other than FICO's in the mortgage scoring process. The senators who introduced the legislation stated that the FICO scoring model mandated by the GSEs "does not take into account consumer data on rent, utility, and cell phone bill payments. This exclusion disproportionately hurts African-Americans, Latinos, and young people who are otherwise creditworthy."[199] Those supporting the status quo FICO model argue that even under a different model, few additional consumers would qualify for a mortgage loan.[200]

Importantly, the FCRA does not require that the *mortgage score*--in contrast to the credit score on which the mortgage score is partially based--be disclosed to consumers.[201] And in certain situations, the mortgage lender may also avoid the requirement to provide the actual credit score it used. This exception applies when the mortgage lender using an automated underwriting system "uses a credit score, other than a credit score provided by a consumer reporting agency" (for example, if the lender develops its own credit score).[202] In that scenario, the FCRA provides those mortgage lenders with two options[203]: They can either **(1) disclose the score they actually developed and used, or (2) obtain and disclose a score and the associated risk factors from a CRA, even though they did not actually use the CRA's score**.[204] While consumers might prefer to receive the actual credit score used by the mortgage lender, the second option under this subsection is presumably

[197] Wayne Passmore and Roger Sparks, The Effect of Automated Underwriting on the Profitability of Mortgage Securitization (Draft, April 8, 1997), at 5, available at SSRN: https://ssrn.com/abstract=36643 or http://dx.doi.org/10.2139/ssrn.36643.
[198] S.2155, 115th Cong. § 310 (2018).
[199] Press Release, Senators Tim Scott (R-SC) and Mark Warner (D-VA), Senators Scott, Warner Champion Homeownership for the "Credit Invisible" (Aug. 1, 2017), available at https://www.scott.senate.gov/media-center/press-releases/senators-scott-warner-champion-homeownership-for-the-credit-invisible.
[200] Joe Light, There's One Mortgage Monopoly the U.S. Government Wants to Keep, Bloomberg, Aug. 25, 2017, available at https://www.bloomberg.com/news/articles/2017-08-25/there-s-a-mortgage-monopoly-the-u-s-government-wants-to-keep.
[201] 15 USC § 1681g(f)(2)(A) ("The term "credit score"-- … does not include-- … any mortgage score or rating of an automated underwriting system that considers one or more factors in addition to credit information … .").
[202] 15 USC § 1681g(g)(1)(C).
[203] 15 U.S.C. § 1681g(g)(1).
[204] National Consumer Law Center, Fair Credit Reporting § 8.4.3.1.2 (9th ed. 2017) (emphasis added).

better than simply receiving an educational score, which as discussed above might be significantly different from the scores that a lender receives from a CRA.

5.1.3.2.2.2 Adverse action notices

An important element of the FCRA's disclosure framework is notices required when an "adverse action" is taken against consumers. The FCRA defines "adverse action" in five contexts:

- **Credit**: a denial or revocation of credit, a change in the terms of an existing credit arrangement, or a refusal to grant credit in substantially the amount or on substantially the terms requested;
- **Insurance**: a denial or cancellation of, an increase in any charge for, or a reduction or other adverse or unfavorable change in the terms of coverage or amount of, any insurance, existing or applied for, in connection with the underwriting of insurance;
- **Employment**: a denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee;
- **Business transactions**: an action taken or determination that is made in connection with an application that was made by, or a transaction that was initiated by, any consumer; and
- **Government licensing**: a denial or cancellation of, an increase in any charge for, or any other adverse or unfavorable change in the terms of, any government license.
- **"Catch-all" category:** an action determination that is made in connection with an application that was made by or a transaction that was initiated by the consumer or in connection with an account review and that is adverse to the interests of the consumer.[205]

Although complex corporate structures can make determining responsibility for issuing an adverse action difficult, "[a] consensus now holds that all parties involved in rendering decisions that rely on the report must issue the notice."[206] In general, notices when an adverse action is based on information in a consumer report must include the following information:

- A statement of the adverse action taken;

[205] 15 USC § 1681a(k)(1).
[206] National Consumer Law Center, Fair Credit Reporting § 8.5.3.1 (9th ed. 2017).

- The credit score actually **used** by the person in taking the adverse action, if there is one;
- **Information about the credit score** (this information is discussed above);
- The name, address, and phone number of the CRA that supplied the report;
- A statement that the CRA did not make the decision and cannot supply the reasons for the adverse action;
- A notice that, upon a request by the consumer made within sixty days, the **consumer may obtain a free copy of their consumer report**; and
- Disclosure of the **consumer's right to dispute with the CRA the accuracy or completeness of the repor**t.[207]

What is noteworthy about these requirements is that the **consumer will receive the actual credit score used and the statutorily required factors for how the credit score was calculated**. However, there is no requirement that the user disclose the reasons for the adverse action itself, unlike the ECOA adverse action notice discussed below.

Different requirements apply when an adverse action involving the denial of or increase in a charge for credit is based on information obtained from third parties other than consumer reporting agencies.[208] In those circumstances, "the user of such information" (generally a creditor) must inform the consumer that **the consumer has a right to request "the reasons for such adverse action" with sixty days**.[209] If the creditor receives a timely request, it is required to "disclose the nature of the information to the consumer."[210] The FTC has explained that this phrase means "the **creditor need disclose only the nature of the information that led to the adverse action (e.g., history of late rent payments or bad checks**) … ."[211] However, the creditor need not identify the source that provided the information or the criteria that led to the adverse action. In practice, this notice requirement is encompassed by the notice requirements of the ECOA, discussed in more detail below.

5.1.3.2.2.3 Risk-based pricing notices

Creditors[212] often make adjustments to the terms offered to consumers on the basis of the perceived risk gleaned from those consumers' credit reports. In situations where a consumer report is used to provide credit on "materially less favorable" terms

[207] 15 USC § 1681m(a).
[208] 15 USC § 1681m(b).
[209] ibid.
[210] ibid.
[211] FTC, Forty Years of Experience With the Fair Credit Reporting Act (July 2011), at 86.
[212] The requirements of this section apply to any "person" but in practice most people that use consumer reports and provide credit are creditors.

than most other consumers receive, creditors must provide consumers with a "risk-based pricing notice."[213]

Risk-based pricing notices must contain the following information:

- A statement that a consumer report (or credit report) includes information about the consumer's credit history and the type of information included in that history;
- That the creditor has set the offered terms based on information from such a report;
- That the terms offered may be less favorable than those offered to consumers with better credit histories;
- That the consumer should verify the accuracy of the information in the consumer report and has the right to dispute any inaccurate information;
- The identity of each CRA that furnished a consumer report in connection with the credit decision;
- That the consumer has the right to obtain a free credit report from that CRA;
- How to obtain their report along with contact information;
- Credit scoring information, ...; and
- The website of the Consumer Financial Protection Bureau.[214]

As with adverse action notices, risk-based pricing notices must include **the actual credit score used by the person making the credit decision**.[215] Risk-based pricing notices must be provided either at the time of an application for credit or at the time the approval of the application is communicated.[216] In practice, most risk-based pricing notices are required to be provided when the approval of the application is communicated, which means that only consumers whose credit price has actually been impacted by their scores or reports will receive notice.[217]

[213] 12 C.F.R. § 1022.72(a) (emphases added). The definition of "material terms" is limited to the annual percentage rate (APR) that creditors charge for credit. This requirement is subject to certain exceptions, such as if the if the consumer has applied for specific credit terms and receives those terms, if the offer is in a pre-screened solicitation and the offer is a firm offer of credit. See 12 C.F.R. § 1022.74.
[214] National Consumer Law Center, Fair Credit Reporting § 8.7.3.1 (9th ed. 2017) (emphasis added).
[215] 12 C.F.R. § 1022.72(a)(1)(ix)(B).
[216] 15 USC § 1681m(h)(2).
[217] National Consumer Law Center, Fair Credit Reporting § 8.7.4.1 (9th ed. 2017). This addresses the concern that if creditors could provide notice at the time of the application, they could comply with their obligations by providing generic notices to consumers.

5.1.3.2.2.4 Notices related to employment

CRAs that furnish consumer reports to users for employment purposes must obtain a certification from the user stating that the user (1) has obtained the consumer's consent, (2) will provide the consumer with a copy of his or her report and a summary of rights under the FCRA before taking adverse action, and (3) will not use the report to violate employment opportunity laws.[218] With regard to the consent requirement, "the FCRA requires employers who use a consumer report to obtain the employee or applicant's authorization, and to make certain disclosures in connection with so doing."[219] This disclosure may include a brief description of the nature of consumer reports and the request for written consumer authorization.[220]

If the employer takes an adverse action[221] based on the consumer report, it must provide two separate notices. "The first notice must be given prior to the employer's taking the adverse action."[222] In this notice the employer must provide a copy of the consumer report and a description of the consumer's rights under the FCRA.[223] The second notice is provided after the adverse action. This notice is subject to the same requirements for adverse action notices discussed above.

5.1.4 Safeguards Listed in Article 22(3)

5.1.4.1 GDPR right to contest

As noted above, solely automated decisions that cause legal or similarly significant effects are generally prohibited by GDPR Article 22. But even when they are allowed under the exceptions enumerated in Article 22(2), GDPR Article 22(3) requires data controllers to at least safeguard data subjects' "right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[224]

The Working Party does not elaborate further on GDPR Article 22(3), other than to highlight the importance of human involvement in the review of automated decisions:

[218] FTC, Forty Years of Experience With the Fair Credit Reporting Act (July 2011), at 50.
[219] National Consumer Law Center, Fair Credit Reporting § 8.11.1.1.1 (9th ed. 2017).
[220] FTC, Forty Years of Experience With the Fair Credit Reporting Act (July 2011), at 50.
[221] An adverse action in the context of employment means "a denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee." 15 U.S.C. § 1681a(k)(1)(B)(ii).
[222] National Consumer Law Center, Fair Credit Reporting § 8.11.1.1.1 (9th ed. 2017).
[223] 15 USC § 1681b(b)(3). In practice the requirement applies to "the person intending to take such adverse action," which means it is not limited only to employers.
[224] As discussed above, these safeguards have been interpreted by the WP29 to include a right to an explanation. However, in the context of equal protection laws there is no analogous right to an explanation, although some form of explanation might be provided during the process of contesting the decision.

> "Human intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject."[225]

The Working Party also suggests that controllers consider "a mechanism for human intervention in defined cases, for example providing a link to an appeals process at the point the automated decision is delivered to the data subject, with agreed timescales for the review and a named contact point for any queries."[226]

U.S. law will not generally provide for a specific "right to obtain human intervention" or right "to express [a] point of view" as enumerated in Article 22(3). However, in certain contexts, such as credit, it will provide the right to correct inaccurate or incomplete data. As described in more detail below, in many situations U.S. law allows for the right to contest decisions themselves, which may or may not mean that a human is brought into the loop, and an opportunity to express an opinion. Indeed, the language of the GDPR and the WP29 suggests that the focus of Article 22(3) is on providing data subjects with a way to challenge the automated decisions to which they may be subject. Another way of putting it is that Article 22(3) requires automated decisions to be rendered "justiciable."[227] As the UK ICO explains in its guidance on Article 22(3), controllers "should have a process in place for individuals to challenge or appeal a decision, and the grounds on which they can make an appeal. You should also ensure that any review is carried out by someone who is suitably qualified and authorised to change the decision."[228]

With this approach in mind, we will focus generally on the right to "contest the decision" in Article 22(3). The GDPR does not define "contest," and thus it is unclear whether the term means a general right to challenge a decision or whether it refers to a specific path, such as the right to contest the decision in a court of law.[229] Regardless, the FCRA and the statutes discussed below provide numerous ways for

[225] WP Guidance at 27.
[226] WP Guidance Annex I at 32 (emphasis added).
[227] Emre Bayamlloolu, Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation, SSRN Electronic Journal, 10.2139/ssrn.3097653 (2018), at 39.
[228] UK ICO, What else do we need to consider if Article 22 applies?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-else-do-we-need-to-consider-if-article-22-applies/.
[229] The WP29 has suggested "a mechanism for human intervention in defined cases, for example providing a link to an appeals process at the point the automated decision is delivered to the data subject, with agreed timescales for the review and a named contact point for any queries." WP Guidelines at 32.

people to contest decisions, and therefore we will focus on these rights under U.S. statutes when contemplating protections that may be analogous to those in GDPR Article 22(3).

5.1.4.2 FCRA right to contest

5.1.4.2.1.1 Contesting the accuracy of information

Under the FCRA, consumers are entitled to dispute the accuracy or completeness of any item of information in their file.[230] Once a CRA receives notification of a dispute from a consumer, it must conduct an investigation "to determine whether the disputed information is inaccurate and record the current status of the disputed information, or delete the item from the file …" within thirty days.[231] The CRA must also notify the furnisher of the disputed information, which in turn triggers certain duties on the part of the furnisher.[232]

It is important to note that this is a right to contest the accuracy of information that may be used to make automated decisions rather than the decisions themselves. It should also be noted that disputing the accuracy of information is now itself a largely automated process that runs through a system owned by CRAs known as the Online Solution for Complete and Accurate Reporting (e-OSCAR).[233] This system has been criticized in the past for failing to fulfil basic requirements of dispute resolution,[234] although it has been "upgraded" to allow for relevant documents to be shared between CRAs and furnishers.[235]

5.1.4.2.1.2 Private right of action

In addition to this right to dispute the accuracy of information in a consumer's file, the FCRA provides for additional and more general methods of contestation. The FCRA "imposes liability on 'any person' who fails to comply with any 'requirement' of the Act with respect to consumers, with separate provisions for willful and negligent violations."[236] This broad liability provision generally allows consumers to file lawsuits

[230] 15 U.S.C. § 1681i(a)(1)(A).
[231] 15 U.S.C. § 1681i(a)(1).
[232] 15 U.S.C. § 1681i(a)(2).
[233] FTC and Fed. Reserve Board, Report to Congress on the Fair Credit Reporting Act Dispute Process 15 (2006), available at https://www.ftc.gov/reports/federal-trade-commission-board-governors-federal-reserve-system-report-congress-fair-credit .
[234] Ruffin-Thompkins v. Experian Info. Sols., Inc., 422 F.3d 603, 610 (7th Cir. 2005) ("It seems that Experian has a systemic problem in its limited categorization of the inquiries it receives and its cryptic notices and responses.").
[235] Press Release, CFPB, CFPB Puts Companies on Notice About Duty to Investigate Consumer Credit Report Disputes (Sep. 4, 2013), available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-puts-companies-on-notice-about-duty-to-investigate-consumer-credit-report-disputes/.
[236] National Consumer Law Center, Fair Credit Reporting § 7.7.1 (9th ed. 2017).

alleging that entities subject to the FCRA have violated the law. However, the provision is subject to a number of exceptions that in practice limit the ability of consumers to enforce certain aspects of the FCRA on their own. One important limitation is that while creditors and others who furnish information to CRAs are subject to a number of FCRA requirements, many of these furnisher requirements cannot be enforced through a "private right of action."[237]

Another important element of the private right of action is that consumers must have "standing"[238] in order to enter the courthouse doors to allege a violation of the FCRA. The standing requirement is usually expressed as requiring plaintiffs to have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.[239] "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"[240]

The question of standing in the context of the FCRA was recently addressed by the 9th Circuit Court of Appeals and the U.S. Supreme Court in a case involving the data broker Spokeo.[241] That case involved an individual seeking to hold Spokeo--which marketed its services to businesses as a way to learn more about prospective employees--responsible under the FCRA for inaccurate information about the individual:

> "Spokeo operates a "people search engine." If an individual visits Spokeo's Web site and inputs a person's name, a phone number, or an e-mail address, Spokeo conducts a computerized search in a wide variety of databases and provides information about the subject of the search. Spokeo performed such a search for information about Robins, and some of the information it gathered and then disseminated was incorrect. When Robins learned of

[237] "Broadly understood, a private right of action is the right of a private party to ... enter the courthouse and engage judicial resources on your behalf." Gwendolyn Mckee, Injury Without Relief: The Increasing Reluctance of Courts to Allow Negligence Per Se Claims Based on Violations of Fda Regulations, 83 UMKC L. Rev. 161, 164 (2014).
[238] The standing requirement is usually expressed as requiring plaintiffs to have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016). "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (citation omitted).
[239] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).
[240] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (citation omitted).
[241] See Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016); Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017).

these inaccuracies, he filed a complaint on his own behalf and on behalf of a class of similarly situated individuals."[242]

The issue in the Spokeo case was whether Robins had standing to sue Spokeo for FCRA violations. Ultimately, the Ninth Circuit concluded that Robins satisfied the standing requirement based on his specific allegations of inaccuracies regarding a broad range of material facts about his life, including age, marital status, educational background, and employment history.[243]

5.1.4.2.1.3 Enforcement by public agencies

In addition to private enforcement, the FCRA is also enforced by public agencies, most importantly the CFPB and the FTC. States are also provided with broad enforcement authority under the FCRA.

5.1.5 Conclusion

The FCRA imposes several requirements on the use of credit information to make decisions in the context of employment, insurance, lending, and other areas. Many of these requirements, particularly in regard to disclosures of information, meet in whole or in part the requirements imposed by the GDPR—at least as interpreted by the Working Party—on automated decision-making processes.

- When consumers make proactive requests for their consumer file or credit score, or receive a pre-screening notice, they are provided with **information about the credit system in general and information about themselves held by consumer reporting agencies**..
- When they receive notices triggered by mortgage loans, adverse actions, or employment decisions, they are generally provided with the **actual credit score or consumer report (in case of employment) used to make that decision and the major factors that influenced that score**. In that sense, they receive **information that is more relevant to the specific decision** that was made about them.
- Finally, the FCRA provide**s rights to contest in certain situations, both by giving consumers avenues to correct information about them as well as access to judicial procedures when the requirements of the statute have been violated**.

[242] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544 (2016).
[243] Robins v. Spokeo, Inc., 867 F.3d 1108, 1117 (9th Cir. 2017).

5.2 Equal Credit Opportunity Act[244]

5.2.1 Background and Terminology

The Equal Credit Opportunity Act (ECOA) grew out of Congress's concern over the difficulty women faced in obtaining credit.[245] Efforts to address this issue began with bills in the early 1970s, and the first version of the ECOA was enacted in 1974. This version only prohibited discrimination on the basis of sex or marital status, although Congress debated adding other protected categories such as race.[246] In 1976, Congress enacted major revisions to the ECOA, including prohibiting credit discrimination on the basis of several protected characteristics such as age, race, color, and religion.[247] Courts construe the provisions of the ECOA liberally in line with its remedial purpose of providing equal access to credit regardless of protected characteristics.[248]

The statute itself is relatively brief, at least in comparison to the FCRA. Most of its more specific requirements are found in the regulations issued by the agencies charged with implementing the ECOA. Known commonly as "Regulation B," this regulation is now issued and interpreted by the CFPB.[249]

In contrast to the FCRA's focus on "users" and "consumers," the ECOA regulates credit transactions between "creditors" and "applicants." A creditor is "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit."[250] An applicant is "any person who applies to a creditor directly for an extension, renewal, or continuation of credit, or applies to a creditor indirectly by use of an existing credit plan for an amount exceeding a previously established credit limit."[251]

5.2.2 ECOA Disclosure Requirements

[244] The Equal Credit Opportunity Act is considered an Equal Protection Law. While Equal Protection Laws are discussed below in Chapter 6, we discuss the Equal Credit Opportunity Act in this section given its direct relevance to credit.
[245] See S. Rep. No. 93-278, at 3 (1973). Along with statutes such as Title VII of the Civil Rights Act discussed below, the ECOA is considered an equal protection statute. However, given its focus on consumer credit, we discuss it in this section.
[246] National Consumer Law Center, Credit Discrimination § 1.3.2.1 (7th ed. 2018).
[247] Pub. L. No. 94-239, 90 Stat. 251 (1976).
[248] Bros. v. First Leasing, 724 F.2d 789, 794 (9th Cir. 1984) (noting "the liberal construction we must give" to the ECOA).
[249] See 12 C.F.R. part 1002.
[250] 15 U.S.C. § 1691a(e).
[251] 15 U.S.C. § 1691a(b).

Like the FCRA, the ECOA requires disclosure in the case of an "adverse action" against applicants, but the scope of the statute is narrower.[252] The ECOA only applies to the grant, denial, or change in terms of an applicant's credit,[253] whereas the FCRA also applies when credit is used to make determinations in other contexts, such as employment, insurance, and government licenses.[254]

While the ECOA applies in narrower circumstances than the FCRA, it arguably requires more meaningful explanations of decisions when it does apply. This is discussed in more detail below, but in brief the major difference between the two statutes is that under the FCRA, users taking an adverse action are only required to disclose the key factors that led to a particular credit score, if the score was a factor in taking the adverse action. In contrast, the **ECOA requires creditors to provide *the reasons for the adverse action itself* (which could include relying on a certain credit score)**.

Congress explained that requiring creditors to provide reasons for adverse actions would not only discourage discrimination but also educate consumers and allow them to correct mistakes:

> "The requirement that creditors give reasons for adverse action is in the Committee's view, a strong and necessary adjunct to the antidiscrimination purpose of the legislation, for only if creditors know they must explain their decisions will they effectively be discouraged from discriminatory practices. Yet this requirement fulfils a broader need: rejected credit applicants will now be able to learn where and how their credit status is deficient and this information should have a pervasive and valuable educational benefit. Instead of being told only that they do not meet a particular creditor's standards, consumers particularly should benefit from knowing, for example, that the reason for the denial is their short residence in the area, or their recent change of employment, or their already over-extended financial situation. In those cases where the creditor may have acted on

[252] Treadway v. Gateway Chevrolet Oldsmobile Inc., 362 F.3d 971, 982 (7th Cir. 2004) ("The FCRA defines 'adverse action' more broadly than does the ECOA.")
[253] ECOA defines "adverse action" to mean "a denial or revocation of credit, a change in the terms of an existing credit arrangement, or a refusal to grant credit in substantially the amount or on substantially the terms requested." 15 USC § 1691(d)(6). "Applicant means any person who requests or who has received an extension of credit from a creditor, and includes any person who is or may become contractually liable regarding an extension of credit." 12 C.F.R. § 1002.2(e).
[254] The ECOA also lacks the FCRA's so-called "catch-all" provision which defines adverse actions to include actions taken in the context of business transactions initiated by the consumer. Treadway v. Gateway Chevrolet Oldsmobile Inc., 362 F.3d 971, 982 (7th Cir. 2004) (quoting H.R.Rep. No. 103–486 at 26 (1994)).

misinformation or inadequate information, the statement of reasons gives the applicant a chance to rectify the mistake."[255]

5.2.2.1 Requirements When Age is Used a Predictive Factor

In order to use age as a predictive factor in granting credit, creditors must use an "empirically derived, demonstrably and statistically sound, credit scoring system."*256* To meet these criteria, the system must be:

(i) Based on data that are derived from an empirical comparison of sample groups or the population of creditworthy and non-creditworthy applicants who applied for credit within a reasonable preceding period of time;
(ii) Developed for the purpose of evaluating the creditworthiness of applicants with respect to the legitimate business interests of the creditor utilizing the system (including, but not limited to, minimizing bad debt losses and operating expenses in accordance with the creditor's business judgment);
(iii) Developed and validated using accepted statistical principles and methodology; and
(iv) Periodically revalidated by the use of appropriate statistical principles and methodology and adjusted as necessary to maintain predictive ability.

While these requirements only apply to the use of credit scoring systems that use age as a predictive factor in granting credit, in practice regulator comments suggest that statistical validation of credit scoring systems is a key tool that the FTC and CFPB use to assess compliance with ECOA and that regulated entities meet these guidelines to manage risk.*257*

5.2.2.2 Comparison of ECOA to GDPR

5.2.2.2.1 Information about the system

Congress enacted the ECOA "to prohibit creditors from discriminating against credit applicants on the basis of sensitive characteristics such as race, religion, national

[255] S. Rep. No. 94-589 (1976), at 4 (emphases added).
[256] See 12 C.F.R. § 1002.2(p) (defining empirically derived and other credit scoring systems); 12 CFR. Pt. 1002, Supp. I(2)(p)(1) ("The definition under §§ 1002.2(p)(1)(i) through (iv) sets the criteria that a credit system must meet in order to use age as a predictive factor.")
[257] Testimony of Sandra F. Braunstein, Director, Division of Consumer and Community Affairs, Federal Reserve, "Credit Scoring," Before the Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit, U.S. House of Representatives, Washington, D.C. March 24, 2010; https://www.federalreserve.gov/newsevents/testimony/braunstein20100323a.htm.

origin, sex, or marital status."[258] Unlike the FCRA, the ECOA does not provide a right for individuals on their own initiative to obtain general information about the credit system, such as through requesting the consumer's file or a credit score. Instead, the ECOA's focus is on ensuring that when creditors make decisions they do not discriminate against applicants and they provide applicants with reasons for the actions they take.[259] Thus, **most notices under the ECOA are provided when creditors take specific decisions involving credit applicants**.

5.2.2.2.2 Information about the decision

The most important notices under the ECOA are provided in the context of adverse actions. When a creditor[260] takes an adverse action, the ECOA requires the following information to be provided in the notice:

- a statement of the action taken;
- the name and address of the creditor;
- a statement of the provisions of section 701(a) of the Act[[261]];
- the name and address of the Federal agency that administers compliance with respect to the creditor; and
- either: (i) **A statement of specific reasons for the action taken**; or (ii) A disclosure of the applicant's right to a statement of specific reasons within 30 days, if the statement is requested within 60 days of the creditor's notification.[262]

With regard to the statement of specific reasons, the ECOA requires that it "**be specific and indicate the principal reason(s) for the adverse action**. Statements that the adverse action was based on the creditor's internal standards or policies or that the applicant, joint applicant, or similar party failed to achieve a qualifying score on the creditor's credit scoring system are insufficient."[263]

[258] Mikella Hurley & Julius Adebayo, Credit Scoring in the Era of Big Data, 18 Yale J. L. & Tech. 148, 190 (2016).
[259] See 12 C.F.R. § 1002.9(a)(2)(i) (requiring creditors to provide "[a] statement of specific reasons for the action taken").
[260] "Creditor means a person who, in the ordinary course of business, regularly participates in a credit decision, including setting the terms of the credit." 12 C.F.R. § 1002.2(l).
[261] This section provides that "It shall be unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction--(1) on the basis of race, color, religion, national origin, sex or marital status, or age (provided the applicant has the capacity to contract); (2) because all or part of the applicant's income derives from any public assistance program; or (3) because the applicant has in good faith exercised any right under this chapter." 15 U.S.C.A. § 1691(a).
[262] 12 C.F.R. § 1002.9(a)(2) (emphasis added).
[263] 12 C.F.R. § 1002.9(b)(2) (emphasis added).

The CFPB has created several model forms for communicating to applicants the specific reasons that an adverse action was taken.[264] For the purposes of this report, three of these forms are particularly relevant. The first two forms, Form C-1 and Form C-2, use different methods to present the specific reasons for the action taken. Form C-1 presents a list of over twenty reasons with blanks next to each reason that a lender can select. Some of the listed reasons are: Credit application incomplete; Insufficient number of credit references provided; Unacceptable type of credit references provided; Unable to verify employment; Length of employment; Length of residence; Number of recent inquiries on credit bureau report; Value or type of collateral not sufficient; and Other, specify: ___." Although some of these reasons do give applicants an understanding of whether they have too much or too little of a listed reason, the CFPB has concluded that "[a] creditor need not describe how or why a factor adversely affected an applicant. For example, the notice may say 'length of residence' rather than 'too short a period of residence.'"[265]

Form C-2 takes a different approach. In form C-2, four major categories (income, employment, credit history, and application) are listed, with reasons listed below each category. For example, under income, the options are "is below our minimum requirement," "is insufficient to sustain payments on the amount of credit requested," or "could not be verified."[266]

Both Form C-1 and C-2 also contain model language for telling applicants that the creditor obtained a credit score from a CRA and used that score in making a credit decision. The form provides blanks for where the actual score should be provided and where the key factors that affected the score are listed. The content of the forms implies that the credit score is a factor, but not the only factor, in the creditor's decision.

In contrast to Forms C-1 and C-2, Form C-3 applies when the creditor's decision is based solely on a credit score. As the NCLC has pointed out, "[i]t is not always obvious what the actual reason for denial of credit is when a creditor uses a credit scoring system, as the system bases the applicant's score on many different variables."[267] In the CFPB's official interpretation of notice that is required when credit scoring systems are used, the agency notes that all "principal reasons" for the adverse action must be included in the disclosure and provides examples of methods

[264] 12 CFR § 1002.9 Appendix C.
[265] Official Interpretations of Reg. B, 12 C.F.R. pt. 1002, supp. I, § 1002.9(b)(3). (emphasis added).
[266] 12 CFR § 1002.9 Appendix C.
[267] National Consumer Law Center, Credit Discrimination § 10.5.4.2.3 (7th ed. 2018).

that creditors can use for selecting reasons for an adverse action based on a credit scoring system:

> If a creditor bases the denial or other adverse action on a credit scoring system, the reasons disclosed must relate only to those factors actually scored in the system. Moreover, no factor that was a principal reason for adverse action may be excluded from disclosure. **The creditor must disclose the *actual reasons for denial* (for example, "age of automobile") even if the relationship of that factor to predicting creditworthiness may not be clear to the applicant**.
>
> Credit scoring—method for selecting reasons. The regulation does not require that any one method be used for selecting reasons for a credit denial or other adverse action that is based on a credit scoring system. Various methods will meet the requirements of the regulation. One method is to identify the factors for which the applicant's score fell furthest below the average score for each of those factors achieved by applicants whose total score was at or slightly above the minimum passing score. [(This method can be viewed as selective, it focuses on the most salient information.)] Another method is to identify the factors for which the applicant's score fell furthest below the average score for each of those factors achieved by all applicants. [(This method can be considered both selective and contrastive, in that it adds additional information allowing an applicant to understand their position among other candidates.)] These average scores could be calculated during the development or use of the system. Any other method that produces results substantially similar to either of these methods is also acceptable under the regulation.[268]

Form C-3 seeks to embody these requirements by explaining the credit score in two different ways. The first section of the form provides the following sample language:

> "The information you provided in your application did not score a sufficient number of points for approval of the application. The reasons you did not score well compared with other applicants were:
>
> - Insufficient bank references
> - Type of occupation

[268] Official Interpretations of Reg. B, 12 C.F.RCFR. pt. 1002, supp. I, § 1002.9(b)(2) paras. 4-5. (emphases added).

- Insufficient credit experience
- Number of recent inquiries on credit bureau report[269]

Form C-3 also contains model information about credit scores that is identical to that in Form C-1 and Form C-2. It is not clear whether the reasons in the two sections need to be different. Thus, where credit is denied on the basis of a credit score alone, it may be that effectively the same requirements apply to an ECOA adverse action notice as those that apply to an FCRA adverse action notice. Ultimately, whether a notice satisfies the requirements of ECOA is often a matter of judicial interpretation.[270]

5.2.3 Safeguards Listed in Article 22(3)

Under the ECOA, "[a]ny creditor who fails to comply with any requirement imposed [by the statute] shall be liable to the aggrieved applicant for any actual damages sustained by such applicant acting either in an individual capacity or as a member of a class."[271] Overall, the private remedies available under the ECOA are similar to those of the FCRA.[272] In addition to private remedies, several state and federal agencies are responsible for ensuring compliance with the ECOA. Depending on the circumstances these include the CFPB, the FTC,[273] and the U.S. Attorney General.

5.2.4 Conclusion

The ECOA serves as an important check on discrimination in the context of credit, and it requires creditors to disclose the reasons for credit decisions. Similar to the FCRA, many of these requirements meet in whole or in part the requirements imposed by the GDPR regarding meaningful information about the logic involved in automated decision-making processes.

- When consumers receive notices triggered an adverse action, they are generally provided with **a statement of specific reasons for the action taken, the actual credit score used to make that decision and the major factors that influenced that score**. In that sense, they receive **information that is more relevant to the specific decision** that was made about them.

[269] 12 CFR § 1002.9 Appendix C.
[270] See NCLC, Credit Discrimination § 10.5.4.2.1 (7th ed. 2018) (noting that "Courts have, for example, approved notices that were ambiguous and required some interpretation by the consumer" and citing cases).
[271] 15 U.S.C. § 1691e(a).
[272] National Consumer Law Center, Credit Discrimination § 11.8.1 (7th ed. 2018).
[273] The Dodd-Frank Act shifted primary enforcement authority of ECOA from the FTC to the CFPB, although the FTC continues to retain jurisdiction over automobile dealers.

This information also provides **information about the credit system in general**.

- Finally, the ECOA provides **a right to contest by providing access to judicial procedures when the requirements of the statute have been violated**.

6 Equal Protection Laws

In this section, we turn to U.S. equal protection laws that prohibit discrimination on the basis of characteristics such as race, gender, and age. In general, these statutes make no reference to automation per se. However, algorithms, data mining, and other technologies that facilitate automated decisions "can reproduce existing patterns of discrimination, inherit the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society."[274] Thus, equal protections laws are a critical check on the potential for automated decisions to lead to unlawful discrimination.

As with privacy law, federal equal protection laws in the U.S. are largely sectoral. Employment discrimination is proscribed by Title VII of the Civil Rights Act and the Age Discrimination in Employment Act.[275] The Fair Housing Act prohibits discrimination in housing decisions, while the Americans with Disabilities Act (ADA) prohibits discrimination on the basis of covered disabilities. In general, to prove a violation of these equal protection laws, plaintiffs must demonstrate that they have been subject either to "disparate treatment" or "disparate impact."[276] Disparate treatment occurs when people are treated differently on the basis of a protected characteristic such as race or age. Disparate impact "occurs when a company employs facially neutral policies or practices that have a disproportionate adverse effect or impact on a protected class, unless those practices or policies further a legitimate business need that cannot reasonably be achieved by means that have less disparate an impact."[277]

Scholars have debated the extent to which equal protection laws are suited to dealing with harms caused by discrimination in the context of big data and automated decisions.[278] In the employment context, some have concluded that neither disparate treatment nor disparate impact theories are well-suited to addressing discrimination

[274] Solon Barocas and Andrew Selbst, Big Data's Disparate Impact, 104 California Law Review 671, 673 (2016).
[275] The Genetic Information Nondiscrimination Act is another statute that prohibits discrimination in the employment context. It also prohibits discrimination based on genetic information in health insurance.
[276] See Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion? (January 2016), at 18; U.S. Department of Housing and Urban Development, Office of General Counsel, Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions (April 2016) (discussing disparate treatment and disparate impact in the context of the FHA), available at https://www.hud.gov/sites/documents/HUD_OGCGUIDAPPFHASTANDCR.PDF.
[277] Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion? (January 2016), at 19. This is a generalization, as the specific requirements for demonstrating disparate impact will vary by statute.
[278] See, e.g., Solon Barocas and Andrew Selbst, Big Data's Disparate Impact, 104 California Law Review 671, 673 (2016); Pauline Kim, Data-Driven Discrimination at Work, 58 Wm. & Mary L. Rev. 857, 861-62 (2017).

in the context of automated decisions.[279] This conclusion is based on the argument that most data mining models that rely on legitimate job-related traits as inputs will be justified as a business necessity, which is a defense available under Title VII. One scholar has argued that because the ADA "protects only individuals who are currently disabled, have records of past disabilities, or are regarded as having existing impairments … [i]t does not stretch to cover individuals who are perfectly healthy at present but whom an employer suspects of being at risk of serious ailments later in life based on big data analysis[.]"[280] Others recognize that challenges exist but argue that Title VII could be interpreted to prohibit "classification bias" and therefore address discrimination caused by automated decisions.[281]

Solely automated decisions that cause legal or similarly significant effects are generally prohibited by GDPR Article 22. But even when they are allowed under the exceptions enumerated in Article 22(2), GDPR Article 22(3) requires data controllers to at least safeguard data subjects' right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.[282] As discussed above, these safeguards collectively are analogous to a general right to contest found in many U.S. laws. In the context of equal protection laws the GDPR safeguards find a corollary in provisions that entitle aggrieved persons to file complaints with courts and administrative bodies such as the EEOC. However, beyond parallels with the safeguards in Article 22(3), equal protection laws will generally not require proactive notice about the use of or results of automated decisions as called for in other articles in the GDPR.

6.1 Employment

6.1.1 Title VII of the Civil Rights Act

Title VII of the Civil Rights Act[283] was enacted to prohibit workplace discrimination on the basis of race, color, religion, sex, or national origin. The statute does not specifically address automated decisions or automated processing. However, it is well-documented that automated decisions in the context of employment is on the rise. Automation is used in many ways, from screening applicants, to workplace monitoring, to monitoring off-duty behavior.[284]

[279] Solon Barocas and Andrew Selbst, Big Data's Disparate Impact, 104 California Law Review 671, 701 (2016)
[280] Sharona Hoffman, Big Data and the Americans with Disabilities Act, 68 Hastings L.J. 777, 779 (2017).
[281] Pauline Kim, Data-Driven Discrimination at Work, 58 Wm. & Mary L. Rev. 857, 861-62 (2017)
[282] As discussed above, these safeguards have been interpreted by the WP29 to include a right to an explanation. However, in the context of equal protection laws there is no analogous right to an explanation.
[283] 42 USC § 2000e et seq.
[284] Pauline Kim, Data-Driven Discrimination at Work, 58 Wm. & Mary L. Rev. 857, 861-62 (2017).

The WP29 has used employment screening as an example of automated decisions that may allowed under the contract exception of Article 22(2)(a):

> "A business advertises an open position. As working for the business in question is popular, the business receives tens of thousands of applications. Due to the exceptionally high volume of applications, the business may find that it is not practically possible to identify fitting candidates without first using fully automated means to sift out irrelevant applications. In this case, automated decision-making may be necessary in order to make a short list of possible candidates, with the intention of entering into a contract with a data subject.[285]"

Even if allowed, however, the safeguards enumerated in GDPR Article 22(3) still apply.

Employee screening is of particular importance to the Equal Employment Opportunity Commission, the agency charged with enforcing Title VII. In 1978 it issued Uniform Guidelines on Employee Selection Procedures (Uniform Guidelines),[286] which are designed "to assist employers, labor organizations, employment agencies, and licensing and certification boards to comply with requirements of Federal law prohibiting employment practices which discriminate on grounds of race, color, religion, sex, and national origin."[287]

The Uniform Guidelines specify that selection procedures which have an adverse impact on these protected characteristics are prohibited:

> "The use of any selection procedure which has an adverse impact on the hiring, promotion, or other employment or membership opportunities of members of any race, sex, or ethnic group will be considered to be discriminatory and inconsistent with these guidelines, unless the procedure has been validated in accordance with these guidelines, or the provisions of section 6 below are satisfied.[288]"

[285] WP Guidelines at 23 (emphases added).
[286] 29 CFR Part 1607.
[287] 29 CFR § 1607.1.
[288] 29 CFR § 1607.3.

Although the Uniform Guidelines were issued thirty years ago, their focus on the *impacts* of selection procedures continues to make them relevant in the context of automated decisions today.

The EEOC is aware of the potential risks and benefits that big data can have in the employment context, and it held a meeting on this issue in October 2016.[289] The Chair of the EEOC noted at the meeting that big data offered both opportunities and challenges in the employment context: "As we consider how to best apply our anti-discrimination protections to this reality, we are mindful of the value in promoting innovation, while at the same time, recognizing that it is critical to ensure that reliance on these vast sources of data do not create new barriers to opportunity." At this time, it is not clear whether the EEOC is acting on outcomes from the meeting.

Like other equal protection laws, Title VII provides an avenue to contest decisions, including automated decisions, that may involve employment discrimination. The process for enforcement of the provisions of Title VII can be complex:

> "Title VII of the Civil Rights Act of 1964 creates a federal cause of action for employment discrimination. Before a federal court may assume jurisdiction over a claim under Title VII, however, a claimant must exhaust the administrative procedures enumerated in 42 U.S.C. § 2000e-5(b), which include an investigation of the complaint and a determination by the EEOC as to whether "reasonable cause" exists to believe that the charge of discrimination is true. … [W]here state law protects persons against the kind of discrimination alleged, "complainants are required to resort" to "state and local remedies" before they may proceed to the EEOC, and then to federal court, on their claims of discrimination under federal law.[290]"

6.1.2 The Due Process Clause

In addition to Title VII protection, the U.S. Constitution can also provide more general protections that are relevant in the context of automated decisions and employment. The due process clauses of the Fifth and Fourteenth Amendments of the U.S. Constitution prohibit the federal and state government from depriving individuals of "life, liberty, or property, without due process of law."[291] Due process imposes procedural constraints on government actions that are measured by fairness, risk of

[289] See EEOC, Meeting of October 13, 2016 - Big Data in the Workplace: Examining Implications for Equal Employment Opportunity Law, available at https://www.eeoc.gov/eeoc/meetings/10-13-16/
[290] Davis v. N. Carolina Dep't of Correction, 48 F.3d 134, 136–37 (4th Cir. 1995).
[291] U.S. CONST. amend. V and XIV (applicable to federal and state government actions respectively).

erroneous deprivation, the seriousness of those risks, and the costs of providing more process.[292] When protected interests—such as employment contracts—are involved, "the right to some kind of prior hearing is paramount."[293] Constitutional due process protections will limit and shape the use of automated decision-making systems. It will take time for the courts to sort out how due process principles apply to automated decision-making systems. Due process precedent as well as, administrative law[294], and regulatory and administrative rules affirm the importance U.S. law places on transparency and rationality in both the development of rules and their application to specific individuals in specific cases.[295] While applying these to various automated processing and decision-making systems will take time these bedrock principles will channel and determine their use.

Like the GDPR Article 22(3), which requires data controllers to "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision" the purpose of Constitutional due process is to ensure fairness and to protect individuals from mistakes.[[296]] However, it is important to note that unlike the GDPR, Constitutional Due Process only limits governmental authorities. As a result, it does not create direct limitations on private actors, although, as discussed below, it can affect private parties

[292] See, Mathews v. Eldridge 424 U.S. 319 (1976). (holding that existing administrative procedures were sufficient to terminate Social Security disability payments and that an evidentiary hearing was not required and setting forth a three factor test for considering whether due process is provided: (1) the private interest that will be affected by the official action; (2) the risk of an erroneous deprivation of such interest through the procedures used, and probable value, if any, of additional procedural safeguards; and (3) the Government's interest, including the fiscal and administrative burdens that the additional or substitute procedures would entail.) at 335. For a detailed discussion of due process and its relevance to concerns related to automated processing generally see, Crawford, Kate, and Jason Schultz. "Big data and due process: Toward a framework to redress predictive privacy harms." BCL Rev. 55 (2014): 93.

[293] Bd. of Regents of State Colleges v. Roth, 408 U.S. 564, 569–70 (1972).

[294] Principles of transparency, expertise, rationality, public participation, and accountability in a variety of administrative laws ensure that the public is aware of the activities of government and in particular transparency for government decisions about the development and application of rules are fully explained, and the public can access the evidentiary basis. Administrative Procedure Act 5 USC §§ 552-3 (2012); Freedom of Information Act 5 U.S.C. § 552 (2012); the Privacy Act, 5 USC § 552a; The Government in the Sunshine Act, 5 USC § 552b; Digital Accountability and Transparency Act of 2014, 31 USC § 6101 note; Federal Register and Code of Federal Regulations, 44 USC Ch. 15.

[295] See Malenchik v. State, 928 N.E.2d 564, 575 (Ind. 2010) (allowing algorithmic risk assessment score to be "considered as a supplemental source of information to assist a trial court in formulating the manner a sentence is to be served"); State v. Loomis, 881 N.W.2d 749, 753 & n.10 (Wis. 2016) (concluding that judges can use algorithmic risk assessment tools when deciding how to sentence defendants, but holding that "risk scores may not be considered as the determinative factor in deciding whether the offender can be supervised safely and effectively in the community"); State v. Gordon, No. 17-0395, 2018 WL 2084847, at *9 (Iowa Ct. App. May 2, 2018) (vacating a defendant's prison term because the district court considered the defendant's risk level scores as an aggravating factor when imposing the sentence without statutory authority to do so).

[296] Fuentes v. Shevin, 407 U.S. 67, 80–81 (1972) (The constitutional right to be heard is a basic aspect of the duty of government to follow a fair process of decision-making when it acts to deprive a person of his possessions. The purpose of this requirement is not only to ensure abstract fair play to the individual. Its purpose, more particularly, is to protect his use and possession of property from arbitrary encroachment—to minimize substantively unfair or mistaken deprivations of property …")

hired by states for governmental purposes. A recent case illustrates how the Fourteenth Amendment has been used to challenge decisions based on automated processing developed in the private sector.

Early cases have generally addressed decision support systems—those that provide an input into a broader decision-making process—rather than fully automated decision-making systems and largely avoided questions about whether any information about the logic of an algorithmic system must be provided.[297] While not representative of the range of court reasoning to date, we describe a recent case to illustrate both how the Fourteenth Amendment can be used to challenge decisions based on automated processing, and to show how such challenges can address systems developed in the private sector but used by the government.

Public school teachers in Houston, Texas, challenged the use of an algorithmic process introduced in 2012 to assess teacher performance.[298] The assessment process involved a statistical model called the Educational Value–Added Assessment System (EVAAS) developed by SAS, a private software company, and licensed for use by the Houston school district (the District). After adopting the EVAAS model, the District implemented a policy whereby it terminated the employment of teachers who did not achieve a certain rating under the model. SAS treated the algorithm as a trade secret and did not divulge it either to the District or the teachers.

Texas law creates several procedural requirements before a teacher can be terminated. For example, teachers have a right to hear the evidence on which the proposal to terminate their contracts is based, present evidence on their own behalf, and present oral argument to the Board of Trustees before any final ruling on their employment status.[299] The teachers argued that these requirements were violated because they were not allowed to access to the computer algorithms and data necessary to verify the accuracy of their scores. According to the teachers, due

[297] See e.g., Malenchik v. State, 928 N.E.2d 564, 575 (Ind. 2010) (allowing algorithmic risk assessment score to be "considered as a supplemental source of information to assist a trial court in formulating the manner a sentence is to be served"); State v. Loomis, 881 N.W.2d 749, 753 & n.10 (Wis. 2016) (concluding use of an algorithmic risk assessment tool developed for pretrial determination risk at sentencing was permissible because the algorithm inputs consisted of data that was either publicly available data or supplied by the defendant who therefore could have denied or explained it; the judge and defendant "had access to the same copy of the risk assessment"; and, the "risk scores may not be considered as the determinative factor"); State v. Gordon, No. 17-0395, 2018 WL 2084847, at *9 (Iowa Ct. App. May 2, 2018) (vacating a defendant's prison term because the district court considered the defendant's risk level scores as an aggravating factor when imposing the sentence without statutory authority to do so).
[298] Houston Fed'n of Teachers v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1171 (S.D. Tex. 2017).
[299] Houston Fed'n of Teachers v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1176 (S.D. Tex. 2017).

process requires "an opportunity by teachers to test on their own behalf the accuracy of their HISD–sponsored value-added scores."[300] The court agreed.

The court concluded that while SAS did not have to turn over its algorithm, "[w]hen a public agency adopts a policy of making high stakes employment decisions based on secret algorithms incompatible with minimum due process, the proper remedy is to overturn the policy, while leaving the trade secrets intact."[301] The court also addressed the District's argument that the EVAAS assessment was merely one factor in the overall termination decision. Looking to the District's policies of firing 85% of teachers with low EVAAS ratings and adding low ratings as grounds for not renewing contracts, the court stated that "it beggars belief that any HISD hearing officer would (or could) freely disregard the very score used by HISD to identify 'ineffective' teachers."[302] Shortly after the court's ruling, the District agreed in a settlement with the teachers to stop using value-added scoring systems such as the EVAAS to terminate teacher employment.

The court's decision in the Houston teachers' case demonstrates that the Due Process Clause can serve as an important safeguard when automated decisions have a legal effect.

6.2 Housing: Fair Housing Act

The Fair Housing Act (FHA) prohibits discrimination on the basis of race, sex and other protected characteristics in residential dwellings.[303] The statute defines a "dwelling" broadly as "any building, structure, or portion thereof which is occupied as, or designed or intended for occupancy as, a residence by one or more families, and any vacant land which is offered for sale or lease for the construction or location thereon of any such building, structure, or portion thereof."[304] The FHA makes it unlawful to refuse to sell, rent, or otherwise make unavailable a dwelling on the basis of race, color, religion, sex, familial status, national origin, or handicap.[305] It is also illegal to discriminate in the terms of sales or rentals, to advertise housing in a discriminatory manner, or to misrepresent the availability of a dwelling.

[300] Houston Fed'n of Teachers v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1178 (S.D. Tex. 2017).
[301] Houston Fed'n of Teachers v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1179 (S.D. Tex. 2017).
[302] Houston Fed'n of Teachers v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1180 (S.D. Tex. 2017).
[303] 42 USC § 3601 et seq.
[304] 42 USC § 3602(b).
[305] 42 USC § 3604.

In general, automated decisions in the context of housing have not received the same level of attention that they have in the context of employment. Still, there are areas where an increase in automated decisions might implicate the FHA and thus trigger its remedies. For example, the FHA prohibits racial steering, where people are steered toward one area or community on the basis of race.[306] Traditionally this took place in the offline context, where real estate agents encouraged people to look at homes in particular neighborhoods.[307] However, as searches for housing increasingly takes place online, it is possible that automated processing could play a role in steering people toward certain listings on the basis of protected categories such as race or sex.[308]

Another area where automated decisions may implicate the FHA is in the context of housing advertisements. The statute prohibits housing advertisements that "indicate[] any preference, limitation, or discrimination based on" protected characteristics.[309] As described in more detail below, whether solely automated targeting of housing advertisements has legal or similarly significant effects will depend on a number of factors enumerated by the WP29 in the WP Guidance.[310]

Like Title VII, the FHA provides avenues for people to contest discriminatory decisions that have been made about them. "Perhaps no area of the law accords a complainant a greater choice of procedures to remedy discrimination than fair housing law. Many states and local governments provide remedies. Federal remedies range from HUD conciliation efforts to federal court litigation."[311] In contrast to Title VII, plaintiffs alleging FHA violations do not have to exhaust administrative remedies before filing an action in state or federal court. However, beyond parallels with the safeguards in Article 22(3), the FHA does not require proactive notice about the use of or results of automated decisions as called for in other articles in the GDPR.

6.3 Other Equal Protection Statutes

In addition to Title VII and the Fair Housing Act, the FTC has noted that other equal protection statutes might be relevant in the context of big data. These include the Americans with Disabilities Act (ADA), the Age Discrimination in Employment Act

[306] 42 USC § 3604(e).
[307] See Gladstone Realtors v. Vill. of Bellwood, 441 U.S. 91 (1979).
[308] See Teke Wiggin, Steering 2.0? Data may undermine fair housing laws, Inman News (April 2014), available at https://www.inman.com/2014/04/29/steering-2-0-data-may-undermine-fair-housing-laws/.
[309] 42 USC § 3604(c).
[310] WP Guidance at 22.
[311] Fair Housing Legal Support Center and Clinic, A Primer on Fair Housing Law, The John Marshall Law School (2014), at 16.

(ADEA), and the Genetic Information Nondiscrimination Act (GINA). Like Title VII and the FHA, these statutes prohibit discrimination on the basis of disability, age, or genetic information. The processes for filing claims under these statutes will differ in the particulars but will generally bear resemblance to that of Title VII and the FHA.

Although these statutes provide important protections in regard to discrimination, they face a particular limitation in the context of automated decisions: they do not cover predictions about the future. For example, while the GINA prohibits discrimination based on information derived from genetic tests, it "does not limit the use of information about such a disposition—even if it is grounded in genetics—inferred through machine learning techniques that mine other sorts of data. In other words, machine learning that predicts future health status from nongenetic information—including health status changes due to genetic predisposition—would circumvent existing legal protections."[312] Similarly, "[t]he ADA protects only individuals who are currently disabled, have records of past disabilities, or are regarded as having existing impairments. As such, it … does not stretch to cover individuals who are perfectly healthy at present but whom an employer suspects of being at risk of serious ailments later in life based on big data analysis."[313]

6.4 Conclusion

In general, equal protection statutes make no reference to decisions based on automated processing. However, equal protection statutes are relevant to such decisions because they seek to prohibit discrimination on the basis of certain characteristics, and provide avenues for contesting decisions where discrimination is present. Because decisions based on automated processing can reproduce existing patterns of discrimination, the ability to contest these decisions through equal protection statutes provide protections analogous to some of the safeguards in GDPR Article 22(3).

[312] Eric Horvitz and Deirdre Mulligan, Data, Privacy, and the Greater Good, 349 Science 6245, 253-54 (2015); Mark Rothstein, Is GINA Worth the Wait?, 36 J. Law, Medicine & Ethics 174, 177 (2008).
[313] Sharona Hoffman, Big Data and the Americans with Disabilities Act, 68 Hastings L.J. 777, 779 (2017).

7 The Federal Trade Commission Act

7.1 Overview

Section 5 of the Federal Trade Commission Act[314] is another U.S. law that creates protections relevant to automated decisions. In contrast to the sectoral laws discussed above, Section 5 generally applies to most companies acting in commerce, and prohibits unfair or deceptive acts or practices on their part.[315] "For a consumer injury to be unfair, it must be substantial, the injury must not be outweighed by countervailing benefits to competition or consumers produced by the practice, and it must be an injury that could not have been reasonably avoided."[316] "An act or practice is deceptive if it involves a material statement or omission that is likely to mislead a consumer acting reasonably under the circumstances."[317]

In its 2016 report on the potential impacts of big data, the FTC highlighted the importance of Section 5 in the context of algorithms and other tools involved in automated decisions. The violation of material promises and the failure to disclose material information could violate Section 5. For example, in 2008 the FTC sued a company that deceived consumers through the use of a behavioral scoring model:

> In CompuCredit, for instance, the FTC included an allegation in the complaint that although a credit card marketing company touted the ability of consumers to use the card for cash advances, it deceptively failed to disclose that, based on a behavioral scoring model, consumers' credit lines would be reduced if they used their cards for such cash advances **or if they used their cards for certain types of transactions**, including marriage counseling, bars and nightclubs, pawn shops, and massage parlors. Among other things, the settlement prohibits CompuCredit from making misrepresentations to consumers in the marketing of credit cards, including misrepresentations about the amount of available credit.[318]

[314] 15 USC § 45.
[315] Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion? (January 2016), at 21.
[316] Chris Hoofnagle, Federal Trade Commission: Privacy Law and Policy (2016), 132.
[317] Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion? (January 2016), at 21.
[318] Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion? (January 2016), at 22 (emphasis added).

The FTC has also brought Section 5 complaints against companies that sell personal data to entities they know or have reason to know will use the data for fraudulent purposes.[319]

7.2 Conclusion

As with the equal protection statutes discussed above, Section 5 of the FTC Act does not specifically refer to decisions based on automated processing. Yet Section 5 is relevant because it prohibits unfair and deceptive acts and practices, which can certainly arise where decisions based on automated processing are being made.

[319] See FTC v. Sequoia One, LLC, No. 2:15-cv-01512 (D. Nev. Aug. 10, 2015), https://www.ftc.gov/system/files/documents/cases/150812sequoiaonemcdonnellstip.pdf; Complaint, Sequoia One, No. 2-15-cv-01512 (D. Nev. filed Aug. 7, 2015), https://www.ftc.gov/system/files/documents/cases/150812sequoiaonecmpt.pdf.

8 Health information

8.1 Relevant Statutes and Guidelines

As with other sectors discussed in this report, the health care sector is an area where automation is increasingly prevalent. This is particularly true with regard to heuristic and rule-based approaches to clinical decision support (CDS) systems. CDS systems are designed to help filter through information to suggest next steps for treatments and catch potential problems, such as dangerous medication interactions, among other uses. While CDS systems have been used in clinical settings for decades, recent increases in the availability of massive datasets and advances in computing have ushered in CDS systems that incorporate artificial intelligence, particularly machine learning, to mine data before generating a decision recommendation.[320] AI/ML-based systems are being deployed across a wide range of health settings, including to predict potential drug interactions,[321] to evaluate foetal well-being,[322] to model chronic disease progression,[323] to predict the risk of disease or hospital readmission,[324] and to mine electronic health records to identify previously unrecognized patterns within and across texts.[325] Some CDS systems aid providers in making diagnostic decisions about individual patients such as distinguishing benign from malignant cancers,[326] and treating heart disease.[327]

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule is an important statute in the context of CDS systems. The Privacy Rule gives individuals

[320] See Middleton, B., D. F. Sittig, and A. Wright. "Clinical Decision Support: A 25 Year Retrospective and a 25 Year Vision." Yearbook of Medical Informatics Suppl 1 (2016): S103-16.
[321] Cheng, Feixiong, and Zhongming Zhao. "Machine Learning-Based Prediction of Drug–drug Interactions by Integrating Drug Phenotypic, Therapeutic, Chemical, and Genomic Properties." Journal of the American Medical Informatics Association : JAMIA 21, no. e2 (October 2014): e278–86. https://doi.org/10/f6hpts
[322] Ocak, Hasan. "A Medical Decision Support System Based on Support Vector Machines and the Genetic Algorithm for the Evaluation of Fetal Well-Being." Journal of Medical Systems 37, no. 2 (April 1, 2013): 9913. https://doi.org/10/gbcwv4
[323] Wang, Xiang, David Sontag, and Fei Wang. "Unsupervised Learning of Disease Progression Models." In KDD 2014 - Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. Association for Computing Machinery, 2014. https://doi.org/10.1145/2623330.2623754
[324] See Caruana, Rich, Yin Lou, Johannes Gehrke, Paul Koch, Marc Sturm, and Noemie Elhadad. "Intelligible Models for HealthCare: Predicting Pneumonia Risk and Hospital 30-Day Readmission." In Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1721–1730. KDD '15. New York, NY, USA: ACM, 2015. https://doi.org/10.1145/2783258.2788613
[325] Shickel, Benjamin, Patrick Tighe, Azra Bihorac, and Parisa Rashidi. "Deep EHR: A Survey of Recent Advances in Deep Learning Techniques for Electronic Health Record (EHR) Analysis." IEEE Journal of Biomedical and Health Informatics (forthcoming 2018). https://doi.org/10/gddkw8
[326] See, e.g., Esteva, Andre, Brett Kuprel, Roberto A. Novoa, Justin Ko, Susan M. Swetter, Helen M. Blau, and Sebastian Thrun. "Dermatologist-Level Classification of Skin Cancer with Deep Neural Networks." Nature 542, no. 7639 (February 2017): 115–18. https://doi.org/10/bxwn (using a deep convolutional neural network to classify images of skin lesions as benign or malignant and finding it outperforms expert dermatologists in the classification task).
[327] Sennaar, Kumba. "Artificial Intelligence Applications for Treating Heart Disease - 6 Current Use Cases." TechEmergence, January 15, 2018. https://www.techemergence.com/artificial-intelligence-applications-treating-heart-disease-5-current-use-cases/ (reviewing how AI/ML-based systems are being used to detect heart disease through analyzing medical images, predict the risk of heart disease, and automate abnormal heart rhythms).

the right to access[328] protected health information (PHI) in "designated record sets"[329] held by healthcare providers and health plans. The information available to individuals under the Privacy Rule is quite extensive and includes medical and billing records, as well as payment and claims records, health plan enrolment records, case management records, as well as other records used, in whole or in part, by or for a covered entity *to make decisions about individuals*.[330] While the language provides an access right to information used by the "covered entity"[331] to make decisions about the individuals, guidance from the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), which is responsible for the law's implementation and enforcement, limits the scope of information covered entities must provide to patients.

The OCR guidance explains that the Privacy Rule's access rights include "a broad array of health information (...) including medical records, billing and payment records, insurance information, clinical laboratory test reports, X-rays, wellness and disease management program information, and notes[332] among other information generated from treating the individual or paying for the individual's care or otherwise used to make decisions about individuals." But it also clarifies that covered entities are not "required to create new information, **such as explanatory materials or analyses**, that does not already exist in the designated record set" and that PHI may exist in records or systems such as a hospital formulary, which generally includes organizational guidelines and potentially decision support tools for choosing which medications, products and devices to use in a given treatment context.[333] There is

[328] 45 CFR 164.524 https://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-524.pdf

[329] 45 CFR 164.501 https://www.gpo.gov/fdsys/pkg/CFR-2004-title45-vol1/pdf/CFR-2004-title45-vol1-sec164-501.pdf

[330] 45 CFR 164.501(1) A group of records maintained by or for a covered entity that is:
(i) The medical records and billing records about individuals maintained by or for a covered health care provider;
(ii) The enrolment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.
(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
There are exemptions to the right of access, including but not limited to two statutory exemptions: psychotherapy notes defined as the personal notes of a mental health care provider documenting or analyzing the contents of a counselling session that are maintained separate from the rest of the patient's medical record, 45 CFR 164.524(a)(1)(i) and 164.501; and, information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding, 45 CFR 164.524(a)(1)(ii).

[331] A "covered entity" is (1) A health plan, (2) A health care clearinghouse, or (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. 45 C.F.R. § 160.103.

[332] Access is not provided to psychotherapy notes per statute. For a complete list of exceptions to the right of access see 45 CFR 164.524(a)(1) – (a)(3).

[333] HHS FAQ, available at https://www.hhs.gov/hipaa/for-professionals/faq/2042/what-personal-health-information-do-individuals/index.html. "A formulary is a preferred list of medicines that aims to accommodate treatment for the majority (80-90 per cent) of patients presenting with common conditions

no patient right to access information about the logic of a clinical decision support system, or other automated tool that a provider consults in the context of patient care, and no right to notice of the use of these automated systems.

CDS systems in medicine are subject to regulations, and in instances where CDS are not regulated as a medical device, they are subject to requirements aimed at ensuring that medical professionals understand the logic and data underlying the treatment guidance offered.[334] In general, if CDS software is designed to support medical providers in exercising their independent decision-making about patient treatment, they may be excluded from the more stringent FDA device regulations.[335] The FDA's Center for Devices and Radiological Health issued draft guidance[336] interpreting the criteria for CDS software to come under the exclusion that focuses on the ability of the medical provider to exercise independent-review. The draft guidance interprets this independent-review to require software functions that "*clearly explain*":

1) The purpose or intended use of the software function;
2) The intended user (e.g., ultrasound technicians, vascular surgeons);
3) The inputs used to generate the recommendation (e.g., patient age and gender); and
4) The rationale or support for the recommendation.[337]

While these requirements do not afford patients a right to understand the logic of a CDS a medical provider uses to inform patient care, it does require medical providers to receive information that they can use to inform patients about the rationale behind the overall treatment plan. Another effect of the draft guidance is that government review is required before systems capable of fully automated decisions can be deployed.

---

that are likely to need treatment with a medicine." Rosalind Grant, Joint drug formularies: are they worth developing?, 17 Prescriber 28 (2006).

[334] Section 3060(a) of the 21st Century Cures Act, Pub. L. No. 114-255 (2016) added a new subsection to the Food, Drug and Cosmetic Act (FDCA) that excludes from the Food and Drug Administration's (FDA) medical-device regulations and approval processes certain kinds of software functions.

[335] 21 USC § 360j(o)(1)(E) excludes a "software function" that meets the following conditions:
1) not intended to acquire, process, or analyze a medical image or a signal from an in vitro diagnostic device or a pattern or signal from a signal acquisition system;
2) intended for the purpose of displaying, analyzing, or printing medical information about a patient or other medical information (such as peer-reviewed clinical studies and clinical practice guidelines);3) intended for the purpose of supporting or providing recommendations to a health care professional about prevention, diagnosis, or treatment of a disease or condition; and
4) intended for the purpose of enabling such health care professional to independently review the basis for such recommendations that such software presents so that it is not the intent that such health care professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient.

[336] Center for Devices and Radiological Health, "Clinical and Patient Decision Support Software: Draft Guidance for Industry and Food and Drug Administration Staff" (Washington, D.C.: U.S. Food & Drug Administration, December 8, 2017), https://www.fda.gov/MedicalDevices/DigitalHealth/ucm562577.htm

[337] Ibid. at 8.

8.2 Conclusion

While automated processing is likely playing an increasing role in all aspects of health care, one area of particular relevance is its use in CDS systems. The HIPAA Privacy Rule does create some rights that are analogous to those available under the GDPR, particularly in regard to accessing personal health information. However, these systems do not act directly on patients (data subjects), but rather organize and highlight information for medical professionals. The guidance documents emphasize the need for medical professionals to understand the logic behind CDS systems they use in making decisions about treating patients, but do not address patient access to such information.

9 Advertising

9.1 WP29's Analysis

According to the WP29, "online advertising … increasingly relies on automated tools and involves solely automated individual decision-making"[338] but "in many typical cases" it would not be prohibited under Article 22 as it does "not have a similarly significant effect on [the] individual." However, the WP29 recognized that there may be cases where Article 22 does apply to online advertising. Determining whether or not solely automated ad targeting has a "similarly significant effect" requires attention to a variety of factors including:

- the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; or
- using knowledge of the vulnerabilities of the data subjects targeted.[339]

The WP29 also notes that the same practice may have different implications depending upon the potential negative outcome for the subject. For example, targeting advertisements for high interest loans to those in financial distress can lead vulnerable individuals deeper into debt, or differential pricing that produces "prohibitively high prices effectively bar[ing] someone from certain goods or services."[340]

9.2 UK Information Commissioner's Office

In a set of recently issued reports on the use of data analytics during the E.U. Referendum,[341] the UK Information Commissioner opined that "Micro-targeting by political parties and campaigns *may be* a type of automated decision-making that does have sufficiently significant effects on individuals to bring [it] under Article 22." [342] While the WP29's guidance emphasizes traits such as intrusiveness, individual expectations, and the specific vulnerabilities of targeted individuals, the ICO's report also highlights the societal level impacts from "'invisible processing'" and micro targeting, stating that they "could have a damaging long-term effect on the fabric of

[338] WP Guidance at 22.
[339] ibid.
[340] ibid.
[341] ICO Democracy Disrupted?: Personal information and political Influence, July 11, 2018; ICO Investigation into the use of data analytics in political campaigns, July 11, 2018
[342] ICO Democracy Disrupted?: Personal information and political Influence, 16, July 11, 2018.

our democracy and political life."[343] Similarly, the recent opinion of the European Data Protection Supervisor (EDPS) states, "In particular, the notion of public interest under data protection law and how it is distinct from the private interests of companies or political movements is key to addressing abuses and manipulation occurring in the online political space."[344]

From these texts it appears that solely automated ad targeting could be considered to have "similarly significant effects" under Article 22 depending upon the

- intrusiveness and comprehensiveness of profiling,
- inconsistency with contextual expectations of data subjects, or
- targeting of data subject vulnerabilities in ways foreseeable to harm the data subject specifically or through manipulation of the data subject harm democratic processes and outcomes.

The Future of Political Campaigning,[345] commissioned by the ICO, provides an overview of the use of personal data and technology in political campaigns, with an emphasis on micro-targeting. It mentions *several U.S. firms* that provide a wide range of data and technology used by political campaigns including:

- data exchanges and data silos[346]
- "assistance in mining and targeting voters, including so called 'marketing clouds'"[347]
- "software platforms [that] allow political parties to target individual members of a given constituency, allowing for more targeted messaging"[348]
- cross-device marketing[349]
- social media, web and mobile advertising platforms[350]

Of particular relevance is research on the Dutch 2017 national election campaign finding widespread use of Facebook 'lookalike'[351] service to engage in "political behavioural targeting".[352] This service helps advertisers target based on traits including age, gender, relationship status, education, workplace, job titles, as well as behavior and location.[353] In addition researchers found some campaigns employed

[343] ICO Democracy Disrupted?: Personal information and political Influence, 16, July 11, 2018, at 9.
[344] Opinion 3/2018, EDPS Opinion on online manipulation and personal data P. 19
[345] Bartlett, Jamie, Josh Smith, and Rose Acton. "The Future of Political Campaigning."
[346] Ibid. at 8 (discussing BlueKai Exchange, Facebook, Microsoft and IBM)
[347] Ibid. at 27 (noting services offered by Adobe, Oracle, Salesforce, Nielsen, and IBM)
[348] Ibid. (identifying Nationbuilder and NGP Van)
[349] Ibid. at 30 (identifying Drawbridge)
[350] Ibid. at (Facebook, Google)
[351] https://www.facebook.com/business/a/lookalike-audiences
[352] T Dobber et al (2017), 'Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques', Internet Policy Review. ("Nearly all campaigns use its lookalike audiences function to find new potential voters.") Id. p. 12.
[353] https://www.facebook.com/business/products/ads/ad-targeting

"'dark posts', a Facebook function that enables campaigns to opaquely target specific audiences, while its messages are not visible to untargeted Facebook users."[354]

The researchers concluded that despite "the relatively strict Dutch data protection law, labelling political preference as 'sensitive personal data', which can only be processed with explicit consent from the potential voter"..."Dutch campaigns...can (and do) rely on election results on voting booth level (which comprises a couple of streets). They can (and do) combine these results with detailed, accurate, and a multitude of data about the neighbourhoods surrounding those voting booths. And then there is Facebook, facilitating easy targeting of its users with personalised messages."[355]

The UK ICO's investigation found that political parties uploaded contact details of voters, telephone numbers and emails into Facebook's Custom Audience function.[356] In addition, the UK ICO is continuing to investigate whether insurance customer data of UK citizens was transferred to the University of Mississippi, by Eldon Insurance Services[357] and used to target voters during the E.U. referendum campaign.[358] In addition, the UK ICO raised concerns about the use of Facebook's Partner Categories service by UK political parties. The service allows advertisers to target Facebook users with advertisements based on information third-party data brokers such as Acxiom, Experian and Oracle Data Cloud know about individuals.[359] In effect Facebook combines the data the political party knows about individuals with offline demographic and behavioral information provided by data brokers. In March 2018 Facebook announced it was retiring the program over the next six months.[360]

The analyses of the UK ICO, DEMOS, and various academic researchers documents that multiple non-European Economic Area companies are involved in targeting political advertising. The relationships, as the UK ICO notes, are quite complicated and in some scenarios US-based companies appear to be controllers and in others processors. When an advertiser places advertisements based on information people provide directly to Facebook, or collected through the Facebook pixel, Facebook is the controller. Facebook is operating in the European market and collecting personal data directly from E.U. individuals. In contrast, where an advertiser uploads its customers personal information to use the Custom Audiences or other measurement

[354] T Dobber et al at 12.
[355] Ibid. at 18.
[356] ICO Investigation into the use of data analytics in political campaigns, July 11, 2018 at 35.
[357] This company does not appear to have self-certified under the Privacy Shield.
[358] ICO Investigation into the use of data analytics in political campaigns, July 11, 2018 at 35
[359] All of these companies have self-certified under the Privacy Shield.
[360] https://newsroom.fb.com/news/h/shutting-down-partner-categories/

and analytics services Facebook is most likely a data processor. In the context of the soon to be retired Partner Categories service the UK ICO report suggests that Facebook may be a controller rather than or in addition to a processor.[361]

9.3 U.S. Approaches

In the U.S. online targeted advertising has been challenged under civil rights and consumer protection laws. Claims have been lodged against platforms[362] and companies using online advertising platforms.[363] Researchers have documented the various ways that advertising can be targeted toward or away from people along the lines of protected categories such as gender, including through advertising platform interfaces that specifically allow for demographic targeting, advertising platform interfaces that allow for categories or terms correlated with protected traits, through dynamic targeting based on consumer responses to ads, or because of the bidding and tailoring decisions of other advertisers.[364] In addition, legislation was introduced in both the House and Senate of the U.S. Congress to increase the transparency of political advertising on social media platforms.[365]

There is growing concern and action by Congress, regulators, civil society organizations, and consumer protection authorities regarding the use of automated decisions to target advertisements. General prohibitions on discrimination (intentional and disparate impact) discussed above in Section 8 as well as specific prohibitions on advertisements that indicate a preference based on race, color, religion, sex, national origin, or age, cover advertising regardless of the level of automation[366] in

[361] ICO Investigation into the use of data analytics in political campaigns, July 11, 2018 at 40.
[362] https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/2018_07_23%20AOD.pdf (settling a complaint that Facebook's advertising platform that allowed third parties to target advertisements to individuals in ways that implicated protected characteristics and potential use by advertisers to exclude individuals from receiving advertisements for housing, credit, insurance, employment, or public accommodation in violation of state civil rights law was an unfair or deceptive practice); https://nationalfairhousing.org/wp-content/uploads/2018/03/NFHA-v.-Facebook.-Complaint-w-Exhibits-March-27-Final-pdf.pdf (alleging Facebook's advertising platform that allowed advertisers offering housing to exclude families with children and women from receiving advertisements, as well as users with interests based on disability and national origin, among other variables, and then approved those ads violated the federal Fair Housing Act).
[363] https://cwa-union.org/sites/default/files/20171220-facebook-ads-age-discrimination-complaint.pdf (alleging violation of federal Age Discrimination in Employment Act (ADEA) for using Facebook's advertising platform to restrict the age range of ad recipients.
[364] Datta, Amit, Anupam Datta, Jael Makagon, Deirdre K. Mulligan, and Michael Carl Tschantz. "Discrimination in Online Advertising: A Multidisciplinary Inquiry." In *Conference on Fairness, Accountability and Transparency*, pp. 20-34. 2018.
[365] Honest Ads Act, H.R. 4077, 115th Cong. (1st Sess. 2017); Honest Ads Act, S.1989 115th Cong. (1st Sess. 2017).
[366] Section 704(b) of Title VII of the Civil Rights Act of 1964, codified at 42 USC x2000e-3(b) (prohibiting employers, labor organizations, employment agencies, and joint labor-management committees from advertisements that indicate a discriminatory preference); Fair Housing Act 42 USC x3601 et seq. (same); For an explanation of the interaction between online advertising and prohibitions on ads that indicate a discriminatory preference see Datta, Amit, Anupam Datta, Jael Makagon, Deirdre K. Mulligan, and Michael

areas of employment, housing, and public accommodations do apply to online advertising. However, the extent to which they will provide remedies to all forms of algorithmic targeting that has a discriminatory impact on an advertisement's availability is uncertain.[367]

In addition to equal protection statutes, advertisers themselves have adopted guidelines and other self-regulatory measures. For example, the Interactive Advertising Bureau (IAB) adopted a set of Privacy Principles in 2008 that include providing consumers with: meaningful notice about the information collected and used for interactive advertising, information about the choices they have concerning the collection and use of information for interactive advertising purposes, and a readily accessible means to express concerns and complaints regarding adherence to these principles.[368] More broadly, several advertising industry groups have developed Self-Regulatory Principles for Online Behavioral Advertising "to apply consumer-friendly standards to online behavioral advertising across the Internet."[369]

There are many ways to indicate improper preferences through advertising. These include not only the written or visual text of the ads, but also the ways in which advertisements are distributed or targeted. For example, in the context of the Fair Housing Act (FHA), courts have found limiting an advertisement to a "racially homogenous [white] county",[370] publishing advertisements exclusively in a language other than English,[371] and indicating a language preference, which could mask a preference for people of a specific national origin[372] to express discriminatory preferences. FHA regulations clarify that *targeting* can indicate an illegal preference, stating that "selecting media or locations for advertising. . . which deny particular segments of the housing market information" or "refusing to publish advertising for the sale or rental of dwellings. . . " because of a protected class indicates a discriminatory preference.[373]

Carl Tschantz. "Discrimination in Online Advertising: A Multidisciplinary Inquiry." In *Conference on Fairness, Accountability and Transparency*, pp. 20-34. 2018.

[367] Datta, Amit, Anupam Datta, Jael Makagon, Deirdre K. Mulligan, and Michael Carl Tschantz. "Discrimination in Online Advertising: A Multidisciplinary Inquiry." In *Conference on Fairness, Accountability and Transparency*, at 29-34. 2018.

[368] IAB, Interactive Advertising Privacy Principles, https://archive.iab.com/iab.atlasworks.com/guidelines/508676/1464.html.

[369] American Association of Advertising Agencies, Self-Regulatory Principles for Online Behavioral Advertising (2009).

[370] United States v. City of Warren, MI, 138 F.3d 1083 (6th Cir. 1998).

[371] Hous. Rights Ctr. v. Sterling, 404 F. Supp. 2d 1179, 1193-94 (C.D. Cal. 2004) (notices and banners in Korean would suggest to the ordinary reader a racial preference for Korean tenants.)

[372] Holmgren v. Little Village Community Rptr., 342 F. Supp. 512, 513 (N.D. Ill. 1971)

[373] 24 C.F.R. § 100.75

9.4 Conclusion

Advertising is a complex sector that raises many issues under GDPR Article 22. As the WP29 has stated, whether advertising falls within the scope of Article 22 is context-specific and involves a number of factors. The UK ICO and others have analysed ways in which advertisements have been used to influence elections, which would arguably involve legal or similarly significant effects. However, in the US, there are few if any specific limitations on the use of automated decisions to target advertisements. Aside from equal protection statutes discussed above and industry self-regulation, few protections exist in the U.S. regarding advertising that might come under the reach of decisions governed by GDPR Article 22.

10 Insurance

10.1 Federal Approaches

The insurance industry is generally regulated at the state level,[374] and thus a full overview of relevant legal protections in the insurance context is outside the scope of this report. However, it is worth noting a few general issues in insurance that are important to automated decisions.

At the federal level the FCRA applies to the use of credit information to make insurance decisions. That means that insurers must have a permissible purpose before obtaining a consumer report and must take certain steps if they take an adverse action based on information in the report.[375] The FTC has provided scenarios that illustrate how the FCRA applies to insurers who use consumer reports to make decisions. For example,

> *"A person with an unfavorable credit history, say, due to a bankruptcy, is denied automobile insurance at standard rates. Although the credit history was considered in the decision, the applicant's limited driving experience was a more important factor."*

> "*The applicant is entitled to [an] adverse action notice because the credit report played a part — even a small one — in the insurer's decision to charge a higher premium*.[[376]]"

Because pricing insurance relies heavily on predicting the likelihood that an insurable event will occur in the future, the industry is rapidly adopting methods of automated processing that can assist with more accurate pricing. Car insurance is one area where the processing of data at an individual level is being used to price insurance policies.[377] Cars often have technology such as Event Data Recorders (EDR) or ports for such devices that track a variety of information including location, speed, and breaking activity.

---

[374] Max N. Helveston, Consumer Protection in the Age of Big Data, 93 Wash. U.L. Rev. 859, 902 (2016) ("Insurance regulation is predominantly a matter of state law.")
[375] Federal Trade Commission, Consumer Reports: What Insurers Need to Know (Ed. March 2018), available at https://www.ftc.gov/tips-advice/business-center/guidance/consumer-reports-what-insurers-need-know.
[376] Federal Trade Commission, Consumer Reports: What Insurers Need to Know (Ed. March 2018), available at https://www.ftc.gov/tips-advice/business-center/guidance/consumer-reports-what-insurers-need-know.
[377] For example, Metromile provides consumers with a dongle tracks the distance driven by the vehicle and prices insurance according to the number of miles driven. See https://www.metromile.com.

10.2 State Approaches

At the state level, "[s]ome insurance statutes identify specific factors that may not be grounds for rejecting a risk. Apart from those narrow prohibitions, 'an insurance company generally is entitled to determine the risks it considers profitable to insure,' and '[t]he insurer is at liberty to choose its own risks and may accept or reject applicants as it sees fit.'"[378] Insurers are using "big data" to conduct marketing campaigns, set rates using predictive models, and even to adjudicate claims.

Although insurers are generally free to use new modelling techniques for the purposes described above, insurance industry regulators have begun to grapple with the use of statistical models in insurance underwriting. In Nevada, for example, insurers are required to submit models to the state insurance regulatory body for approval: "any mathematical model used in underwriting or rating of any personal line of property and/or casualty insurance, … must be filed with the Division for prior approval … ."[379] Regulators in other states, such as California, Delaware, and Connecticut are also weighing in the use of statistical modelling to set insurance rates and warning insurers that such methods must not discriminate.

In addition to individual state action, the National Association of Insurance Commissioners (NAIC)—an organization of state insurance regulators that establishes standards and best practices—has formed a Big Data Working Group (BDWG).[380] The BDWG is considering the formation of a Predictive Analytics Team to review complex pricing models and to assist state regulators in determining whether those models meet applicable legal standards.

10.3 Conclusion

Federal protections for notice ***apply*** when a credit report is used to determine insurance rates. ***But*** insurance regulation largely occurs at the state level in the US and therefore a full analysis is outside the scope of this report. The insurance industry is a sector where decisions based on automated processing is only going to increase

[378] Robert D. Helfand, Big Data and Insurance: What Lawyers Need to Know and Understand, 21 J. Internet L. 1, 12 (2017) (citation omitted).
[379] Nevada Department of Business and Industry, Division of Insurance, Bulletin 17-001 (Jan. 26, 2017). "Rating" is the process of identifying "characteristics of insured persons or properties (such as age, location or past experience) that might increase or decrease the costs associated with individual policies, relative to other members of the insured population." Robert D. Helfand, Big Data and Insurance: What Lawyers Need to Know and Understand, 21 J. Internet L. 1, 10 (2017).
[380] https://naic.org/cmte_ex_bdwg.htm

in the future. Many states are beginning to address this issue, including through requirements that mathematical models be approved by insurance authorities before they can be applied. Through the NAIC, states are also working together to develop model rules for the use of big data that might be consistent at a national level.

11 Main conclusions - Part 2: Legal analysis

The differing legal regimes in the E.U. and U.S. make it difficult to compare their protections for decisions based solely on automated processing which produces legal or similarly significant effects. The GDPR is a law of general applicability that contains provisions dealing explicitly with automated decisions. In contrast, legal frameworks in the U.S. apply to specific sectors, and do not depend on whether decisions are automated, solely, partially, or otherwise. As a result, the rights in the GDPR that are triggered by Article 22 automated decisions—the right to an explanation, right to human intervention, right to contest, among others—do not neatly map on to requirements established in U.S. statutes, instruments, and case law.

Despite these differences, protections do exist in U.S. law in some contexts where automated processing informs decision-making. First, the FCRA and the ECOA set forth detailed requirements for the content of disclosures that must be made in several situations. These laws, particularly the FCRA, have broad effects in sectors such as housing, employment and insurance, and can reach to new methods of evaluating individuals so long as the information provided falls within the definition of a "credit report." Both the FCRA and the ECOA provide consumers with some form of a right to explanation and a right to contest the decision.

Second, a series of equal protection statutes provides a check on models used in automated decision-making that might discriminate on the basis of protected characteristics. These statutes, such as Title VII of the Civil Rights Act and the Fair Housing Act, provide individuals with rights to challenge decisions, including decisions that involve automated processing, however they do not require individuals to be notified of such processes. The Due Process Clause of the U.S. Constitution also provides important substantive and procedural protections where states make decisions that impact rights and entitlements. Additionally, Section 5 of the FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce. This prohibition serves as a broad check on decisions based on automated processing that may be unfair or deceptive under Section 5.

Third, guidelines issued by agencies charged with enforcing these statutes, and decisions of courts interpreting relevant statutes, all play a role in the protection that the law provides in the context of automated decisions. For example, agencies such as CFPB provide specific information about what information must be in an ECOA

adverse action notice, and courts review specific facts to determine whether an entity qualifies as a CRA or whether a person's due process rights have been violated.

While there is therefore no overarching legislation in the U.S., protections that are similar to those of the GPDR exist in relevant areas where automated decision-making is used. Since these business models are rapidly evolving, these areas require close monitoring.

12 References

Ahmed, S. (January 2017). *Cashless Society, Cached Data: Security Considerations for a Chinese Social Credit System*, The Citizen Lab, Jan. 24, 2017. https://citizenlab.ca/2017/01/cashless-society-cached-data-security-considerations-chinese-social-credit-system/

AICPA (2018). *Data Analytics Learning Program*. https://certificates.aicpastore.com/certificates/data-analytics

Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield.

American Association of Advertising Agencies (2009). *Self-Regulatory Principles for Online Behavioral Advertising* (2009)

Amit, D., Datta, A., Makagon, J., Mulligan, D. K. & Tschantz, M.C. (2018). *Discrimination in Online Advertising: A Multidisciplinary Inquiry*. In *Conference on Fairness, Accountability and Transparency*, pp. 20-34.

Anderson, M. J., & Seltzer. W. (2009). *Federal statistical confidentiality and business data: Twentieth century challenges and continuing issues*. Journal of Privacy and Confidentiality 1.1, http://margoanderson.org/govstat/integrity.htm

Android Authority. (June 2018). *Report: Facebook still allows third-parties to access you and your friends' data (Update: Apple responds).* https://www.androidauthority.com/facebook-data-scandal-continued-872397/

Article 29 Data Protection Working Party (13 April 2016). *Opinion 01/2016 of 13 April 2016 on the EU-US Privacy Shield draft adequacy decision*, Adopted on 13 April 2016, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

Article 29 Data Protection Working Party (26 July 2016) *Statement on the decision of the European Commission on the EU-U.S. Privacy Shield*, http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

Article 29 Data Protection Working Party (28 November 2017) E.U. – *U.S. Privacy Shield – First annual Joint Review,* Brussels*,* https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

Article 29 Data Protection Working Party (6 February 2018). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

Attorney General of Washington State. (July 2010). Assurance of Discontinuance, In re Facebook. https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/2018_07_23%20AOD.pdf

Bamberger, K.A. & Mulligan, D.K. (n.d.). *Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. p. 21.

Bamberger, K. A. & Mulligan, D. K. (2010). *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247.

Bamberger, K. A. & Mulligan, D.K. (2015). *Privacy on the ground: driving corporate behavior in the United States and Europe*, 89-94, 129-132 MIT Press, 2015

Barocas, S. & Selbst, A. (2016). *Big Data's Disparate Impact*, 104 California Law Review 671, 673.

Bartlett, J., Smith, J. Acton, R. (July 2018). *The Future of Political Campaigning*. pp. 8-30, https://ico.org.uk/media/2259365/the-future-of-political-campaigning.pdf

Bayamlloolu, E. (2018). *Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation*, SSRN Electronic Journal, 10.2139/ssrn.3097653 (2018), at 39.

Bd. of Regents of State Colleges v. Roth, 408 U.S. 564, 569–70 (1972).

Bennett, C. & Mulligan, D. K. (2012). *The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy*. https://ssrn.com/abstract=2230369 or http://dx.doi.org/10.2139/ssrn.2230369

Bergen, M. & Surane, J. (August 2018). *Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales.* https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales

Berkman Klein Center, (2018). *Immunity for Online Publishers Under the Communications Decency Act,* Digital Media Project, http://www.dmlp.org/legal-guide/immunity-online-publishers-under-communications-decency-act

Bernstein Litowitz Berger & Grossmann LLP. (August 2018). *Bernstein Litowitz Berger & Grossmann LLP Announces Securities Class Action Suit Filed Against Oracle Corporation And Certain of Its Executives*. https://www.prnewswire.com/news-releases/bernstein-litowitz-berger--grossmann-llp-announces-securities-class-action-suit-filed-against-oracle-corporation-and-certain-of-its-executives-300695598.html

Berry v. Schulman, 807 F.3d 600, 605 (4th Cir. 2015).

Brkan, M. (2018). *Do Algorithms Rule the World? Algorithmic Decision-making in the Framework of the GDPR and Beyond.*

Bros. v. First Leasing, 724 F.2d 789, 794 (9th Cir. 1984)

Bureau of Consumer Financial Protection (2017). *Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process*. https://files.consumerfinance.gov/f/documents/20170214_cfpb_Alt-Data-RFI.pdf

Burt, A. & Shirrel, S. (December 2017). *Why we're concerned about the WP29's guidelines on machine learning*, IAPP Privacy Perspectives, https://iapp.org/news/a/why-were-concerned-about-the-wp29s-guidelines-on-machine-learning/)

Bussone, A., Stumpf, S. & O'Sullivan, D. (2015). *The role of explanations on trust and reliance in clinical decision support systems*. Healthcare Informatics (ICHI), 2015 International Conference on. IEEE, 2015. p. 160.

California Business and Professions Code sections 22575-22579, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22575.

California Electronic Communications Privacy Act, (CalECPA) - Penal Code section 1546 et seq. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1546.&lawCode=PEN

Caruana, R., Lou, Y., Gehrke, J., Koch, P., Sturm, M., and Elhadad. N. (2015). *Intelligible Models for HealthCare: Predicting Pneumonia Risk and Hospital 30-day Readmission.* In Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (2015). ACM, New York, NY, USA, 1721-1730. https://dl.acm.org/citation.cfm?doid=2783258.2788613

Casey, B., Farhangi, A. & Vogl, R. (2018). *Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the rise of Algorithmic Audits in Enterprise*.

Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M. & Floridi, L. (2017). *Artificial Intelligence and the 'Good Society': the US, EU, and UK approach*, Science and Engineering Ethics.

CB Insights (2018). *The AI Industry Series: Top Healthcare AI Trends To Watch*. https://www.cbinsights.com/research/report/ai-trends-healthcare/#pharma

CB insights (2018). *The State of Artificial Intelligence 2018*. https://www.cbinsights.com/research/briefing/artificial-intelligence-trends-2018/

CB Insights (2018). *Top AI Trends to Watch in 2018*. https://www.cbinsights.com/reports/CB-Insights_State-of-Artificial-Intelligence-2018.pdf?utm_campaign=state-of-ai_2018-02&utm_medium=email&_hsenc=p2ANqtz-9J-XoLyqmCVkkUByvOpG8TVvms6EqJmuCXipp_jj8FpO4P_TqetNxhhLABVJH_xoiQTvXUy-agdvy68x00VvRmFfB0Pw&_hsmi=60665752&utm_content=60665752&utm_source=hs_automation&hsCtaTracking=be5990ad-0aed-432b-a2e3-c76dfdc898e8%7C57a6f99e-da54-4bac-8857-8e3ad466c8ba

CB Insights (February 2018). *The Race for AI: Google, Intel, Apple in a Rush To Grab Artificial Intelligence Startups*. https://www.cbinsights.com/research/top-acquirers-ai-startups-ma-timeline/

Center for Devices and Radiological Health (December 2017). *Clinical and Patient Decision Support Software: Draft Guidance for Industry and Food and Drug Administration Staff* (Washington, D.C.: U.S. Food & Drug Administration, December 8, 2017), https://www.fda.gov/MedicalDevices/DigitalHealth/ucm562577.htm.

CFPB (July 2011). *The impact of differences between consumer- and creditor-purchased credit scores,* p. 7. https://s3.amazonaws.com/files.consumerfinance.gov/f/2011/07/Report_20110719_CreditScores.pdf.

CFBP (September 2012). *Analysis of Differences between Consumer- and Creditor-Purchased Credit Scores*, https://files.consumerfinance.gov/f/201209_Analysis_Differences_Consumer_Credit.pdf.

CFPB (December 2012). *Key Dimensions and Processes in the U.S. Credit Reporting System*. p. 22 https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf.

CFPB (September 2013). *CFPB Puts Companies on Notice About Duty to Investigate Consumer Credit Report Disputes* (Sep. 4, 2013), https://www.consumerfinance.gov/about-us/newsroom/cfpb-puts-companies-on-notice-about-duty-to-investigate-consumer-credit-report-disputes/.

CFPB (Sept. 14, 2017).Press Release, CFPB Announces First No-Action Letter to Upstart Network

Certificate in Finance and Technology (2018). *Home*. https://www.certfintech.org/#home-about

Chen, A. (July 2018). *IBM's Watson gave unsafe recommendations for treating cancer.* https://www.theverge.com/2018/7/26/17619382/ibms-watson-cancer-ai-healthcare-science

Cheng, F. & Zhao, Z. (October 2014). *Machine Learning-Based Prediction of Drug–drug Interactions by Integrating Drug Phenotypic, Therapeutic, Chemical, and Genomic Properties*. Journal of the American Medical Informatics Association: JAMIA 21, no. e2 (October 2014): e278–86. https://doi.org/10/f6hpts

Christl, W. (June 2017). *Corporate Surveillance in Everyday Life, How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions.* A Report by Cracked Labs, Vienna, June 2017, http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Christl, W. (October 2017). *How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information.* Working paper by Cracked Labs, October 2017. Author: Wolfie Christl. Contributors: Katharina Kopp, Patrick Urs Riechert. http://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

City of New York (May 2018). *Mayor de Blasio Announces First-In-Nation Task Force to Examine Automated Decision Systems Used by the City.* https://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by

Class Action Complaint, Communications Workers of America v. T-Mobile US and similarly situated employers and employment agencies, No. 5:17-cv-07232 (N.D. Cal. Dec. 20, 2017) https://cwa-union.org/sites/default/files/20171220-facebook-ads-age-discrimination-complaint.pdf

Clinton, W. J. & Gore, A. Jr., (1997). *A framework for global electronic commerce*. Washington D.C. p. 4. http://www.w3.org/TR/NOTE-framework-970706

Collins, K. (November 2017). *Google collects Android users' locations even when location services are disabled*. https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/

Complaint, U.S. v. Spokeo, Inc., No. 12-05001 (C.D. Cal. June 7, 2012) at para. 11 & 12.

Complaint, National Fair housing Alliance et al. v. Facebook INC. No. 1:18-cv-02689 (S.D. N.Y. Mar. 27, 2018) https://nationalfairhousing.org/wp-content/uploads/2018/03/NFHA-v.-Facebook.-Complaint-w-Exhibits-March-27-Final-pdf.pdf

Consent Decree, US v. Experian Info. Solutions, Inc., No. CA 3-00CV0056-L (N.D. Tex. Jan. 12, 2000)

CoreLogic CREDCO (2011). *Understanding Credit & Credit Risk Scores.* pp.17–25. www.credco.com.

Corelogic. (2017). *2017 Annual Report. Powering the Global Real Estate Economy.* https://investor.corelogic.com/sites/default/files/2018-03/corelogic-2017-annual-report.pdf

Council of Europe (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, Art. 2, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

Council of Europe (23 November 2010) *The protection of individuals with regard to automatic processing of personal data in the context of profiling.* Recommendation CM/Rec(2010)13 and explanatory memorandum. https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf

Cybergenetics (2018). *Casework*. https://www.cybgen.com/products/casework.shtml

D'Angelo, C.M. (September 14, 2017), CFPB No-Action Letter https://files.consumerfinance.gov/f/documents/201709_cfpb_upstart-no-action-letter.pdf

DARPA (2017). *Explainable Artificial Intelligence (XAI).* https://www.darpa.mil/program/explainable-artificial-intelligence

Davis v. N. Carolina Dep't of Correction, 48 F.3d 134, 136–37 (4th Cir. 1995).

Determann, L. (2017). *California Privacy Law 2017: Practical Guide and Commentary U.S. Federal and State Law*, The Recorder.

DalleMule, L. and Davenport, T.H (May–June 2017) What's Your Data Strategy? in Harvard Business Review, May–June 2017 Issue, https://hbr.org/2017/05/whats-your-data-strategy

Data Transfer Project (2018). *Data Transfer Project Overview and Fundamentals,* p. 4, https://datatransferproject.dev/dtp-overview.pdf

Dixon, P. and Gellman, R. (2 April 2014) The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future. World Privacy Forum https://www.ftc.gov/system/files/documents/public_comments/2014/08/00014-92369.pdf

Dobber, T., Trilling, D., Helberger, D. & de Vreese, C. H. (2017). *Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques*, Internet Policy Review, [online] 6(4). https://policyreview.info/articles/analysis/two-

crates-beer-and-40-pizzas-adoption-innovative-political-behavioural-targeting [Accessed: 21 Sep. 2018]. https://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-political-behavioural-targeting

Domingos, P. (2015). The Master Algorithm. Basic Books, New York

Duhigg, C. (May 2009). *What Does Your Credit-Card Company Know About You?*, New York Times, May 12, 2009, https://www.nytimes.com/2009/05/17/magazine/17credit-t.html.

Dwoskin, E. (August 2018). *Facebook is Rating the Trustworthiness of its Users on a Scale from Zero to 1*, Washington Post (August 21, 2018), https://www.washingtonpost.com/technology/2018/08/21/facebook-is-rating-trustworthiness-its-users-scale-zero-one/?noredirect=on&utm_term=.f4953b509e27.

EDPS (19 March 2018), *Opinion 3/2018 on online manipulation and personal data,* p. 19, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

Edwards, L. & Veale, M. (2017). *Slave to the Algorithm? Why a 'right to an Explanation' is Probably not the Remedy you are Looking for*, 16 DUKE L.& TECH. REV. 17, 44, (2017)

EEOC, (Meeting of October 13, 2016). *Big Data in the Workplace: Examining Implications for Equal Employment Opportunity Law*, https://www.eeoc.gov/eeoc/meetings/10-13-16/

Electronic Frontier Foundation. (August 2017). *hiQ v. LinkedIn – Order Granting hiQ's Preliminary Injunction Motion Against LinkedIn*. https://www.eff.org/document/hiq-v-linkedin-order-granting-hiqs-preliminary-injunction-motion-against-linkedin

EPIC (August 2018). *Following EPIC Complaint, FTC Acknowledges Review of Google Consent Order* https://epic.org/2018/08/following-epic-complaint-ftc-a.html

EPIC (August 2018). *Letter FTC to EPIC*. https://epic.org/privacy/ftc/2018-08-20-FTC-EPIC-Ltr-re-Google.pdf

Esteva, A., Kuprel, B., Novoa, Ko, J., Swetter, S. M., Blau, H. M. & Thrun, S. (February 2017). *Dermatologist-Level Classification of Skin Cancer with Deep Neural Networks*. Nature 542, no. 7639 (February 2017): 115–18. https://doi.org/10/bxwn

European Commission (2001) *Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries*, under Directive 95/46/EC [2001] OJ L181/19

European Commission (2004) *Decision 2004/915/EC of 27 December 2004 amending decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries* (notified under document number C(2004)5271) [2004] OJ L385/74

European Commission (2010), *Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council* (notified under document C (2010) 593) (Text with EEA relevance) [2010] OJ L39/5

European Commission (2013). *Communication From The Commission To The European Parliament And The Council Rebuilding Trust in EU-US Data Flows*

(COM(2013)0846), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013DC0846

European Commission (2015). *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the E.U. to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems),* COM/2015/0566 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0566

European Commission (2016). *Communication from the Commission to the European Parliament and the Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards,* COM/2016/0117 final, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52016DC0117

European Commission (July 2016). *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield,* C/2016/4176. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG

European Commission. (July 2016). *EU-U.S. Privacy Shield factsheet*. http://collections.internetmemory.org/haeu/20171122154227/http:/ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf

European Commission (18 October 2017*) Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield of 18 October 2017, COM (2017) 611 final.* Brussels,

European Commission (18 October 2017) *A Commission Staff Working Document accompanying the Document Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield* {COM(2017) 611 final}, Brussels, file:///C:/Users/bodeag/Downloads/StaffWorkingDocumentpdf.pdf

European Commission (18 October 2017) *Document Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield* {SWD(2017) 344 final}, Brussels, http://ec.europa.eu/newsroom/document.cfm?doc_id=47798

European Commission (25 April 2018) *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe*. COM(2018) 237 final, Brussels, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625

European Commission (June 2018). *The Article 29 Working Party Ceased to Exist as of 25 May 2018.* http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492.

European Court of Justice (2015). *The judgment of 6 October 2015 in Case C-362/14 Maximillian Schrems v Data Protection Commissioner* (EU:C:2015:650), Case C-362/14. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362

European Court of Justice (October 2016). *La Quadrature du Net and Others v Commission (Case T-738/16)*. https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2017.006.01.0039.01.ENG

European Parliament *Rules of Procedure*, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+RULES-EP+20180731+TOC+DOC+XML+V0//EN&language=EN

European Parliament, the Council and the Commission (2012), *Charter of Fundamental Rights of the European Union*, esp. Articles 6, 7, 8, 11, 16, 47 and 52, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

European Parliament and the Council (2011). *Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights,* amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance. Full text https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32011L0083 ; summary https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:0904_4

European Parliament and the Council (27 April 2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*General Data Protection Regulation) (GDPR) http://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament (26 June 2018) *Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Privacy Shield* (2018/2645(RSP)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2018-0305+0+DOC+PDF+V0//EN

European Parliament (5 July 2018) *Resolution on the adequacy of the protection afforded by the EU-US Privacy Shield,* Provisional edition P8_TA-PROV(2018)0315, Strasbourg, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2018-0315

European Union (2016) *Agreement Between the United States of America and the European Union of December 12, 2016, on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences,* 2016 O.J. (L 336/3), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.336.01.0003.01.ENG

Experian. (2018). *The Art of Customer Profiling*. http://www.experian.co.uk/marketing-services/knowledge/white-papers/white-paper-the-art-of-customer-profiling.html

Experian Marketing Solutions, Inc. v. Lehman et al, https://cases.justia.com/federal/district-courts/michigan/miwdce/1:2015cv00476/80902/61/0.pdf?ts=1462448698

Facebook (2018). *Offline conversions*. https://www.facebook.com/business/help/1782327938668950

Facebook. (2018). *Ad Targeting*. https://www.facebook.com/business/products/ads/ad-targeting

Facebook. (2018). *Look-alike audiences*. https://www.facebook.com/business/a/lookalike-audiences

Facebook. (March 2018). *Shutting Down Partner Categories*. https://newsroom.fb.com/news/h/shutting-down-partner-categories/

Fair Housing Act, 42 USC § x3601 et seq. (same)

Fair Housing Legal Support Center and Clinic (2014*). A Primer on Fair Housing Law*, The John Marshall Law School, at 16.

Fair, L. (June 2012). *Speaking of Spokeo: Part 1*, FTC Business Blog, https://www.ftc.gov/news-events/blogs/business-blog/2012/06/speaking-spokeo-part-1

Federal Trade Commission, *Fair Credit Reporting Act*, https://www.ftc.gov/system/files/fcra_2016.pdf and https://www.ecfr.gov/cgi-bin/text-idx?SID=2b1fab8de5438fc52f2a326fc6592874&mc=true&tpl=/ecfrbrowse/Title16/16CIsubchapF.tpl

Federal Trade Commission & Board of Governors of the Federal Reserve System (August 2006), *Report to Congress on the Fair Credit Reporting Act Dispute Process,* p. 15 https://www.ftc.gov/reports/federal-trade-commission-board-governors-federal-reserve-system-report-congress-fair-credit .

Federal Trade Commission (July 2011). *Forty Years of Experience With the Fair Credit Reporting Act*, pp. 50-86, https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf

Federal Trade Commission (May 2014) *Data Brokers, A Call for Transparency and Accountability.* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Federal Trade Commission (January 2016). *Big Data: A Tool for Inclusion or Exclusion?,* pp.18-19. https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

Federal Trade Commission (March 2018). *Consumer Reports: What Insurers Need to Know.* https://www.ftc.gov/tips-advice/business-center/guidance/consumer-reports-what-insurers-need-know

Federal Trade Commission (March 2018). *Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices*. https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection?utm_source=govdelivery

Federal Trade Commission (2018). *#760: The consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics*. https://www.ftc.gov/policy/public-comments/2018/07/initiative-760

FICO (May 2015). *Understanding Fico Scores*, https://www.myfico.com/Downloads/Files/myFICO_UYFS_Booklet.pdf.

Flaherty, D.H. (1989). *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (1989), 373-74.

Fuentes v. Shevin, 407 U.S. 67, 80–81 (1972).

Gartner (April 2018). *Gartner Says Global Artificial Intelligence Business Value to Reach $1.2 Trillion in 2018*. https://www.gartner.com/newsroom/id/3872933

Gellert, R., & Gutwirth, S. (2013). *The legal construction of privacy and data protection*. *Computer Law & Security Review* 29.5 (2013): 522-530.

Gillespie v. Equifax Info. Servs., 2008 WL 4316950, at *7 (N.D. Ill. Sept. 15, 2008) (quoting S. Rep. No. 104-185, at 42-43 (1995)).

Gillespie v. Trans Union Corp., 482 F.3d 907 (7th Cir. 2007)

Gladstone Realtors v. Vill. of Bellwood, 441 U.S. 91 (1979).

Goddard, K., & Roudsari, A. & Wyatt, J.C. (2011). *Automation bias: a systematic review of frequency, effect mediators, and mitigators*. Journal of the American Medical Informatics Association 19.1 (2011): 121-127.

Google. (May 2017). *Powering ads and analytics innovations with machine learning*. https://adwords.googleblog.com/2017/05/powering-ads-and-analytics-innovations.html

Grant, R. (2006). *Joint drug formularies: are they worth developing?,* 17 Prescriber 28.

Greene, R. (May 2018). *How Cities Are Reining in Out-of-Control Policing Tech*, Slate May 18, 2018, available at https://slate.com/technology/2018/05/oakland-california-and-other-cities-are-reining-in-out-of-control-police-

Habermann, H. (2006). *Ethics, confidentiality, and data dissemination*. Journal of Official Statistics 22.4: 599, p. 600.

Helfand, R. D. (2017). *Big Data and Insurance: What Lawyers Need to Know and Understand*, 21 J. Internet L. 1, 10 (2017).

Helveston, M. N. (2016). *Consumer Protection in the Age of Big Data*, 93 Wash. U.L. Rev. 859, 902 (2016)

Hoffman, S. (2017). *Big Data and the Americans with Disabilities Act*, 68 Hastings L.J. 777, 779 (2017).

Honest Ads Act, H.R. 4077, 115th Cong. (1st Sess. 2017); Honest Ads Act, S.1989 115th Cong. (1st Sess. 2017).

Hoofnagle, C. (2005). *Privacy Self-Regulation: A Decade of Disappointmen*t, Electronic Privacy Information Center (2005), p. 2. https://www.epic.org/reports/decadedisappoint.html

Hoofnagle, C. (2013). *How the Fair Credit Reporting Act Regulates Big Data, Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet*. https://ssrn.com/abstract=2432955.

Horvitz, E. & Mulligan, D.K. (2015). *Data, Privacy, and the Greater Good*, 349 Science 6245, 253-54.

Houston Fed'n of Teachers v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1171, 1176 , 1178 – 1180 (S.D. Tex. 2017).

Hurley, M. & Adebayo, J. (2016). *Credit Scoring in the Era of Big Data*, 18 Yale J. L. & Tech. pp. 148, 185, 190.

IAB (2008). *Interactive Advertising Privacy Principles.* https://archive.iab.com/iab.atlasworks.com/guidelines/508676/1464.html.

IAPP & EY (2017). *Annual Privacy Governance Report 2017.* https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf

IEEE Computer Society (2018). *IEEE Computer Society Certification and Credential Program*. https://www.computer.org/web/education/certifications;jsessionid=d2c7cb85f238b82e5386d44e9579

IFI Claims (2018). *Largest and Fastest Growing Technologies*. https://www.ificlaims.com/rankings-growing-tech.htm

Information-Sharing Disclosure, "Shine the Light," California Civil Code sections 1798.83-1798.84
innovative political behavioural targeting techniques, Internet Policy Review. Id. pp. 12-18.

Jones, M.L. (2017). *The right to a human in the loop: Political constructions of computer automation and personhood*, Social Studies of Science Vol. 47(2) (2017), at 220.

Judicial Redress Act of 2015, 5 U.S.C. § 552a note; Attorney General Designations, 82 Fed. Reg. 7860-01 (Jan. 23, 2017). For more information see https://www.justice.gov/opcl/judicial-redress-act-2015.

Kaminski, M. E. (2018). *The Right to Explanation, Explained*, U of Colorado Law Legal Studies Research Paper No. 18-24 (2018).

Kidd v. Thomson Reuters Corp., 299 F. Supp. 3d 400, 402 (S.D.N.Y. 2017).

Kidd v. Thomson Reuters Corp., 299 F. Supp. 3d 400, 405 (S.D.N.Y. 2017) (quoting Tony Rodriguez & Jessica Lyon, Background Screening Reports and the FCRA: Just Saying You're Not a Consumer Reporting Agency Isn't Enough, FTC BUSINESS BLOG (Jan. 10, 2013, 2:00 p.m.), https://www.ftc.gov/news-events/blogs/business-blog/2013/01/background-screening-reports-fcra-just-saying-youre-not). quoting

Kim, P. (2017). *Data-Driven Discrimination at Work*, 58 Wm. & Mary L. Rev. 857, 861-62.

Kincannon, C. L. (2009). *Comment on Article by Anderson and Seltzer*. Journal of Privacy and Confidentiality 1 (1). pp. 53-54 https://doi.org/10.29012/jpc.v1i1.564.

Kroll, J. A., Kohli, N. & Mulligan, D. K. (2018). *A Shared Lexicon for Research and Practice in Human Centered Software Systems*, Draft on file with author.

Larson, J., Mattu, S., Kirchner, L. & Angwin, J. (May 2016). *How We Analyzed the Compas Recidivism Algorithm*. https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

Lauer, J. (2017). *Creditworthy: A History of Consumer Surveillance and Financial Identity in America*.

Lee J.D., & Seppelt B.D. (2009). *Human Factors in Automation Design*. In Nof S. (eds) Springer Handbook of Automation. Berlin: Springer.

Letter from Upstart Network, Inc. to Consumer Financial Protection Bureau, Request for No-Action Letter (undated), https://files.consumerfinance.gov/f/documents/201709_cfpb_upstart-no-action-letter-request.pdf.

Levitin, A. (August 2018). *Facebook: The New Credit Reporting Agency?*, Creditslips (August 21, 2018), http://www.creditslips.org/creditslips/2018/08/facebook-the-new-credit-reporting-agency.html.

Lewis Mayers, The American Legal System (1964).

Libert, T., Graves, L. & Kleis Nielsen, R. (August 2018). *Changes in Third-Party Content on European News Websites after GDPR*. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf

Light, J. (August 2017). *There's One Mortgage Monopoly the U.S. Government Wants to Keep*, Bloomberg, August 25, 2017, https://www.bloomberg.com/news/articles/2017-08-25/there-s-a-mortgage-monopoly-the-u-s-government-wants-to-keep.

Malgieri, G. & Comandé, G. (2017). *Why a right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*.

Mckee, G. (2014). *Injury Without Relief: The Increasing Reluctance of Courts to Allow Negligence Per Se Claims Based on Violations of Fda Regulations*, 83 UMKC L. Rev. 161, 164.

Mendoza, I. & Bygrave, L.A. (2017). *The Right not to be Subject to Automated Decisions based on Profiling*, University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20.

Mesropyan, E. (June 2018). *Alternative Data & Financial Access: The Good, the Bad, and the Ugly.* https://gomedici.com/alternative-data-financial-access-good-bad-ugly/

Meyer, D. (November 2017). *Did the WP29 misinterpret the GDPR on automated decision-making?*, IAPP https://iapp.org/news/a/did-the-wp29-misinterpret-the-gdpr-on-automated-decision-making/.

Middleton, B., Sittig, D. F. & Wright. A. (2016). *Clinical Decision Support: A 25 Year Retrospective and a 25 Year Vision*. Yearbook of Medical Informatics Suppl 1 (2016): S103-16.

Miller, T. (2017). *Explanation in artificial intelligence: Insights from the social sciences*. arXiv preprint arXiv:1706.07269, 2017.

Mosier, K. L., & Fischer, U.M. (2010). *Judgment and decision making by individuals and teams: issues, models, and applications*. Reviews of human factors and ergonomics 6.1 (2010): 198-256. pp. 232-233.

Mulligan, D. K., Koopman, C. & Doty, N. (2016). *Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. Phil. Trans. R. Soc. A* 374.2083 (2016): 20160118.

myFICO (2018). *One Time Credit Reports*. https://www1.myfico.com/products/onetimereports.

National Association of Insurance Commissioners. (2018). *Big Data (Ex) Working Group.* https://naic.org/cmte_ex_bdwg.htm

National Conference of State Legislation (2018). *Privacy and Security*. http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-and-security.aspx

National Conference of State Legislatures (2018). Security Breach Notification Laws. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

National Conference of State Legislatures (2018) *Overview of State Laws Related to Internet Privacy* http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#CollectPI

National Consumer Law Center (NCLC) (January 2009). *Automated Injustice: How a Mechanized Dispute System Frustrates Consumers Seeking to Fix Errors in their Credit Reports*.

National Consumer Law Center (2018) *Credit Discrimination,* 7th ed. 2018. § 1.3.2.1, § 10.5.4.2.3 and § 10.5.4.2.1 https://library.nclc.org/cd

National Consumer Law Center (2018), *Fair Credit Reporting, 9th ed. 2018*, https://library.nclc.org/fcr

Nevada Department of Business and Industry, Division of Insurance (January 2017). *Bulletin 17-001* (Jan. 26, 2017).

Newman, A. (2008). *Protectors of Privacy: Regulating Personal Data in the Global Economy*. 74-75.

New York Times (03 June 2018). *Facebook Gave Device Makers Deep Access to Data on Users and Friends.* https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html

Nissenbaum, H. (1994). *Computing and accountability*. Communications of the ACM 37.1 (1994): 72-81

Ocak, H. (April 2013). *A Medical Decision Support System Based on Support Vector Machines and the Genetic Algorithm for the Evaluation of Fetal Well-Being*. Journal of Medical Systems 37, no. 2 (April 1, 2013): 9913. https://doi.org/10/gbcwv4

Office of the Comptroller of the Currency (OCC). (27 November 2000). *Advisory Letter No. 2000-10*. https://www.occ.treas.gov/news-issuances/advisory-letters/2000/advisory-letter-2000-11.pdf

Official Interpretations of Reg. B, 12 C.F.R. pt. 1002, supp. I, § 1002.9(b)(3).

Official Interpretations of Reg. B, 12 C.F.R. pt. 1002, supp. I, § 1002.9(b)(2) paras. 4-5.

OpenAI. (n.d.). About OpenAI. https://openai.com/about/

Partnership on AI (September 2016). *Industry Leaders Establish Partnership on AI Best Practices*. https://www.partnershiponai.org/industry-leaders-establish-partnership-on-ai-best-practices/

Passmore, W. & Sparks, R. (April 1997). *The Effect of Automated Underwriting on the Profitability of Mortgage Securitization* (Draft, April 8, 1997), pp. 4-5, https://ssrn.com/abstract=36643 or http://dx.doi.org/10.2139/ssrn.36643.

Poon, M. A. (2013). *What Lenders See—A History of the Fair Isaac Scorecard*, (unpublished Ph.D. dissertation, University of California, San Diego), http://search.proquest.com/docview/1520318884.

Post, R.C. (2001). Three concepts of privacy. *Faculty Scholarship Series.* Paper 185. http://digitalcommons.law.yale.edu/fss_papers/185

Privacy Rights for California Minors in the Digital World, California Business and Professions Code sections 22580-22582, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=22580&lawCode=BPC

Rachlinski, J.J., Johnson, S. L., Wistrich, A. J. & Guthrie, C. (2008). *Does unconscious racial bias affect trial judges*. Notre Dame L. Rev. 84 (2008): 1195.

Restatement (Second) of Torts § 652A (1977)

Reuters (March 2018). *Acxiom shares tank after Facebook cuts ties with data brokers.* https://www.reuters.com/article/us-acxiom-stocks/acxiom-shares-tank-after-facebook-cuts-ties-with-data-brokers-idUSKBN1H520U

Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017).

Robins v. Spokeo, Inc., 867 F.3d 1108, 1117 (9th Cir. 2017).

Rodriguez, T. & Lyon, J. (10 January 2013) *Background Screening Reports and the FCRA: Just Saying You're Not a Consumer Reporting Agency Isn't Enough*, FTC BUSINESS BLOG (Jan. 10, 2013, 2:00 p.m.), https://www.ftc.gov/news-events/blogs/business-blog/2013/01/background-screening-reports-fcra-just-saying-youre-not).

Rothstein, M. (2008). *Is GINA Worth the Wait?,* 36 J. Law, Medicine & Ethics 174, 177.

RTE (July 2018). *Supreme Court to hear Facebook data transfer appeal.* https://www.rte.ie/news/courts/2018/0731/982240-facebook-data-transfer/

Ruffin-Thompkins v. Experian Info. Sols., Inc., 422 F.3d 603, 610 (7th Cir. 2005).

Schwartz, P. M. (2015). *The value of privacy federalism*. In *Social dimensions of privacy: Interdisciplinary perspectives*, Roessler, Beate, and Dorota Mokrosinska, eds. Cambridge University Press.

Selbst, A D. and Barocas, S. (19 February 2018). *The Intuitive Appeal of Explainable Machines.* Fordham Law Review, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3126971 or http://dx.doi.org/10.2139/ssrn.3126971

Selbst, A. D. & Powles, J. (2017). *Meaningful Information and the Right to Explanation*, 7 INT'L DATA PRIVACY L. 233, 236 (2017)

Sennaar, K. (15 January 2018) *Artificial Intelligence Applications for Treating Heart Disease - 6 Current Use Cases.*" TechEmergence. https://www.techemergence.com/artificial-intelligence-applications-treating-heart-disease-5-current-use-cases/

Shickel, B., Tighe, P., Bihorac, A. & Rashidi, P. (2018). *Deep EHR: A Survey of Recent Advances in Deep Learning Techniques for Electronic Health Record (EHR) Analysis*. IEEE Journal of Biomedical and Health Informatics (forthcoming 2018). https://doi.org/10/gddkw8

Simon, J. (2015). *Distributed epistemic responsibility in a hyperconnected era*. The Onlife Manifesto. Springer, Cham, 2015. 145-159.

Software Certifications. (2018). *Software Certifications Overview*. http://www.softwarecertifications.org/process/software-certifications-overview/

Solove D.J. (2008) *Understanding privacy*. Cambridge, MA: Harvard University Press

Solove, D. J. & Hartzog, W. (2014). *The FTC and the new common law of privacy*. *Colum. L. Rev.* 114: 583.

Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544, 1547, 1548 (2016)

State of California Department of Justice. (2018). *Privacy Laws*. https://oag.ca.gov/privacy/privacy-laws.

State v. Loomis Case Note, Harvard Law Review, Vol. 130, No. 5, March 2017. https://harvardlawreview.org/2017/03/state-v-loomis/ (Note 55).

Stone, P., Brooks, R. Brynjolfsson, E. Calo, R. Etzioni, O. Hager, G. Hirschberg, J. Kalyanakrishnan, S. Kamar, E. Kraus, S. Leyton-Brown, K. Parkes, D. Press, W. Saxenian, A. Shah, J. Tambe, M. and Teller, A. (2016) *Artificial Intelligence and Life in 2030*. *One Hundred Year Study on Artificial Intelligence*: Report of the 2015-2016 Study Panel, Stanford University, Stanford, CA, September 2016. Doc: http://ai100.stanford.edu/2016-report. Accessed: August, 2018.

Susman, T. (1988). *The Privacy Act and the Freedom of Information Act: Conflict and Resolution*, 21 J. Marshall L. Rev. 703, 705 (1988).

Treadway v. Gateway Chevrolet Oldsmobile Inc., 362 F.3d 971, 982 (7th Cir. 2004) (quoting H.R.Rep. No. 103–486 p. 26 (1994)).

Treaty on the Functioning of the European Union (TFEU), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

UK ICO (11 July 2018) *Democracy Disrupted?: Personal information and political Influence*, https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

UK ICO (11 July 2018). *Investigation into the use of data analytics in political campaigns - update*. pp. 35-40, https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf

UK ICO (2018). *What else do we need to consider if Article 22 applies?* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-else-do-we-need-to-consider-if-article-22-applies/

UK ICO (2018). *What is automated individual decision-making and profiling?* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/

U.S. Civil Rights Act (1964) Section 704(b) of Title VII of the of 1964, codified at 42 USC x2000e-3(b)

U.S. Constitution, Amendment X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people."). https://www.law.cornell.edu/constitution-conan

U.S. Constitution. Article VI - [Legal Status of the Constitution], https://www.law.cornell.edu/constitution-conan

U.S. Copyright Office (December 1998). *The Digital Millennium Copyright Act of 1998. U.S. Copyright Office Summary.* https://www.copyright.gov/legislation/dmca.pdf

U.S. District Court, Southern District of New York. (March 2018). *National Fair housing Alliance; Fair Housing Justice Center, inc; Housing opportunities project for excellence inc.; Fair Housing Council of Greater San Antonio v. Facebook INC.* https://nationalfairhousing.org/wp-content/uploads/2018/03/NFHA-v.-Facebook.-Complaint-w-Exhibits-March-27-Final-pdf.pdf

U.S. v. Experian Info. Solutions, Inc., CA 3-00CV0056-L (N.D. Tex. Jan. 12, 2000) (consent decree)
Upstart Request for No-Action Letter (undated), https://files.consumerfinance.gov/f/documents/201709_cfpb_upstart-no-action-letter-request.pdf.

U.S. Department of Commerce (2018). *Privacy Shield List*, https://www.privacyshield.gov/list

U.S. Department of Commerce (n.d.). *Privacy Shield Framework,* https://www.privacyshield.gov/EU-US-Framework

U.S. Department of Health, Education & Welfare (1973). *Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems* pp.89-243, https://www.justice.gov/opcl/docs/rec-com-rights.pdf

U.S. Department of Health and Human Services, *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*. 45 C.F.R. § 164.502 (2010), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

U.S. Department of Housing and Urban Development (April 2016). *Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions*, Office of General Counsel Guidance , https://www.hud.gov/sites/documents/HUD_OGCGUIDAPPFHASTANDCR.PDF.

U.S. Food and Drug Administration (FDA) (2016). *The 21st Century Cures Act, Pub. L. No. 114-255*. Section 3060(a).

U.S. Food and Drug Administration (FDA) (December 2017). *Draft Guidance for Industry and Food and Drug Administration Staff.* https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM587820.pdf

U.S. Food and Drug Administration (FDA) (December 2017). *Statement from FDA Commissioner Scott Gottlieb, M.D., on advancing new digital health policies to encourage innovation, bring efficiency and modernization to regulation.* https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm587890.htm

U.S. Food and Drug Administration (FDA) (February 2018). *FDA permits marketing of clinical decision support software for alerting providers of a potential stroke in patients*. https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm596575.htm

U.S. Food and Drug Administration (FDA) (April 2018). *FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems*. https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm604357.htm

U.S. Food and Drug Administration (FDA) (May 2018). *FDA permits marketing of artificial intelligences algorithm for aiding providers in detecting wrist fractures*. https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm608833.htm

U.S. Securities and Exchange Commission. (2017). *Annual Report Adobe Systems Incorporated.* https://wwwimages2.adobe.com/content/dam/acom/en/investor-relations/pdfs/ADBE-10K-FY17-FINAL-CERTIFIED.pdf

U.S. Securities and Exchange Commission, Division of Investment Management (February 2017). *Guidance Update: Robo-Advisors*, No. 2017-02, p. 3 February 2017.

U.S. Securities and Exchange Commission. (January 2018). *Annual Report Salesforce.com*. https://s1.q4cdn.com/454432842/files/doc_financials/2018/Q4/Salesforce-Q4Y18-10K.pdf

U.S. Senate, Commerce, Science, and Transportation (2017) *S.J.Res.34 - A Joint Resolution Providing for Congressional Disapproval under Chapter 8 of Title 5, United States Code, of the Rule Submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,'"* 115th Congress, 2d. sess., 2017, https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34.

U.S. Senate, Senator Tim Scott (1 August 2017). *Senators Scott, Warner Champion Homeownership for the "Credit Invisible",* https://www.scott.senate.gov/media-center/press-releases/senators-scott-warner-champion-homeownership-for-the-credit-invisible.

Wachter, S., Mittelstadt, B. & Floridi, L. (28 December 2016). *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulatio*n, International Data Privacy Law, 2017, https://ssrn.com/abstract=2903469 or http://dx.doi.org/10.2139/ssrn.2903469

Wang, X., Sontag, D. & Wang, F. (2014). *Unsupervised Learning of Disease Progression Models*. In KDD 2014 - Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. Association for Computing Machinery. https://doi.org/10.1145/2623330.2623754

Webb, M. Short, N. Bloom, N. ad Lerner, J. (July 2018) *Some Facts of High-Tech Patenting*, the National Bureau of Economic Research (NBER) Working Paper No. 24793, Issued in July 2018, https://www.nber.org/papers/w24793

White House (February 2012). *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

White House (May 2014). *Big Data: Seizing Opportunities, Preserving Values*, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

White House, Executive Office of the President. President's Council of Advisors on Science and Technology (May 2014) *Report to the President: Big Data and Privacy: A Technological Perspective*, https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf

White House (February 2015). *Big Data: Seizing Opportunities and Preserving Values: Interim Progress Report.* https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf

White House, Executive Office of the President (December 2016). *Artificial Intelligence, Automation, and the Economy*. https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.pdf

White House, Executive Office of the President (May 2016). *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

White House (2017). *FY 2019 Administration Research and Development Budget Priorities.* https://www.whitehouse.gov/sites/whitehouse.gov/files/ostp/fy2019-administration-research-development-budget-priorities.pdf

White House, Office of Science and Technology Policy (May 2018). *Summary of the 2018 White House Summit on Artificial Intelligence for American Industry*. https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf

Wiggin, T. (April 2014). *Steering 2.0? Data may undermine fair housing laws*, Inman News https://www.inman.com/2014/04/29/steering-2-0-data-may-undermine-fair-housing-laws/.

13 Annex 1 List of relevant U.S. laws, other instruments and case law

13.1 A. U.S. Laws

Credit

1. Fair Credit Reporting Act (15 USC § 1681 et seq)
    - 12 CFR Part 1022 (implements the requirements of the Fair Credit Reporting Act and includes the amendment that implements the FACTA (Fair and Accurate Credit Transactions Act) which primarily protects consumers from identity theft.)

Equal Opportunity Laws

1. Equal Credit Opportunity Act (15 U.S.C. §§ 1691-1691f)
    - 12 CFR 1002 (implements requirements of ECOA)

2. Title VII of the Civil Rights Act (42 USC § 2000e)
    - 29 CFR 1607 (Uniform guidelines on employee selection procedures)

3. Fair Housing Act (42 U.S.C. 3601 et seq.)

4. Americans with Disabilities Act (42 USC 12101, 47 USC 610)

Laws Applying to U.S. Government

1. Federal agency data mining reporting (42 USC § 2000ee-3)
    - requires federal departments or agencies to report to Congress when they engage in data mining

2. Privacy Act (5 USC § 552a)

Vehicle Information

49 C.F.R. § 563.1 (event data recorders)

13.2 B. Other Instruments (certification mechanisms, codes of conduct)

1. Partnership on AI

2. Recommendations made in U.S. Government reports:

   • "Preparing for the Future of Artificial Intelligence," Executive Office of the President, October 2016

   • “The National Artificial Intelligence Research and Development Strategic Plan, National Science and Technology Council, Subcommittee on Networking and Information Technology Research and Development. (October 2016).

13.3 C. Case Law

1. Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017).
2. Berry v. Schulman, 807 F.3d 600, 605 (4th Cir. 2015).

14 Annex 2 Information Held by the U.S. Government

14.1 Privacy Act

The Privacy Act of 1974 (Privacy Act) protects the privacy of personal information held by the U.S. government.[381] It sets limits on the authority of federal agencies to collect information about individuals, restricts disclosure of records to third parties without consent, and provides access and correction rights to records about individuals.[382] As originally enacted the Privacy Act applied only to U.S. citizens or lawful permanent residents,[383] and therefore would not be directly relevant to E.U. data subjects. However, recent amendments make it applicable to E.U. citizens in some contexts. Therefore, we briefly mention the Privacy Act because it is now specifically applicable to E.U. citizens in the context of criminal investigations. While law enforcement investigations are beyond the scope of this report, given the direct relevance to E.U. citizens of the federal amendments to the Privacy Act, we address it here in order to be as comprehensive as possible.

In 2015, Congress passed an amendment to the Privacy Act known as the Judicial Redress Act (JRA). The JRA extends rights of judicial redress under the Privacy Act to "covered person[s]" and authorizes the U.S. Attorney General (AG) to designate foreign countries whose citizens become entitled to status as a covered person.[384] In February 2017, the U.S. AG designated the European Union as a "covered country" under the JRA.[385] This action was taken as part of the two regions' negotiations of what is known in the U.S. as the Data Protection and Privacy Agreement (DPPA).[386]

Although the Privacy Act prohibits the disclosure of individual records, this limitation is subject to several exceptions. The disclosure is generally limited unless it would be:

[381] 5 USC § 552a.
[382] Thomas Susman, The Privacy Act and the Freedom of Information Act: Conflict and Resolution, 21 J. Marshall L. Rev. 703, 705 (1988).
[383] 5 USC § 552a(a)(2).
[384] 5 USC § 552a Note.
[385] Judicial Redress Act of 2015; Attorney General Designations, 82 Fed. Reg. 7860-01 (Jan. 23, 2017). For more information see https://www.justice.gov/opcl/judicial-redress-act-2015.
[386] Commission Agreement Between the United States of America and the European Union of December 12, 2016, on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, 2016 O.J. (L 336/3).

- To those officers and employees of the agency which maintains the record, who have a need for the record in the performance of their duties.
- When the disclosure is made under the Freedom of Information Act (5 U.S.C. § 552).
- For an established routine use (routine use must be published as part of the system of records notice).
- To the Census Bureau for the purposes of planning or carrying out a census or survey.
- To someone who has adequately notified the agency in advance that the record is to be used for statistical research or reporting and the record is transferred without individually identifying data.
- To the National Archives and Records Administration as a record of historical value.
- To another agency or to an instrumentality of any governmental jurisdiction, within or under the control of the United States for a civil or criminal law enforcement activity, if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.
- To a person under compelling circumstances affecting someone's health or safety, and the person whose health or safety is affected is sent a notification of the disclosure.
- To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee.
- To the Comptroller General in the course of the duties of the General Accountability Office.
- Pursuant to the order of a court of competent jurisdiction.
- To a consumer reporting agency in accordance with section 31 U.S.C. §3711(f).[387]

[387] 5 U.S.C. § 552a(b).

14.2 Federal Agency Data Mining Reporting Act (FADMRA)

The Federal Agency Data Mining Reporting Act (FADMRA) specifically applies to automated processing but offers few if any legal protections.[388] Enacted in 2007, it requires federal agencies that are engaged in any "pattern-based" data mining activity to submit reports to Congress on these activities. The statute requires the report to be produced in coordination with the privacy officer of the relevant agency (if there is one), and to be made available to the public. However, classified information, law enforcement sensitive information, proprietary business information and trade secrets are exempted from the need for disclosure.[389]

Conclusion

The Privacy Act and the FADMRA put some constraints and requirements on personal information held and data mining conducted by the U.S. Government. However, the Privacy Act has many exceptions, and the FADMRA, while it seeks to promote transparency, puts no substantive requirements on data mining by government agencies. Overall these statutes are likely not as relevant to the Privacy Shield as those discussed above, but we mention them here in the interest of completeness.

[388] 42 U.S.C. § 2000ee-3.
[389] 42 U.S.C. § 2000ee-3(3).

15 Annex 3 Comparison of "Right to Explanation" In GDPR and U.S. Credit Statutes

These tables set forth the notices required under the Fair Credit Reporting Act and the Equal Credit Opportunity Act as they compare to the following categories of information required by the GDPR:

1. Information about the system: generalized meaningful information of the system and its logic;
2. Information about the decision: specific meaningful information about the logic and data that contributed to a particular, rendered decision about an individual

Fair Credit Reporting Act

1. Information about the system

Type of required disclosure	Triggered by	Description	Rationale for inclusion in this category
Consumer file disclosure	Consumer request	Consumer is provided with their information (bills paid, debts, etc.), as well as the sources of the information in the file, identification of recipients of their information, such as lenders, and a Summary of Consumer Rights.	The information is not about a particular decision, but it gives consumers a sense of how the system works and informs them of their rights under the system.
Credit score	Consumer request	Consumer is provided with a score, often an "educational" score, and information about the score: the range of scores, the factors that influenced the score.	This information is not about a particular decision, but it gives the consumer a sense of how the system works.
Prescreening notices	Lender action	Notice that accompanies firm offers of credit, and a statement that the consumer can opt out. Notice states that the consumer received the offer because he satisfied certain criteria.	Although the notice is triggered by a "decision" (the consumer qualifies for a certain credit rate), the information provided is very general. Notice informs consumer that information in their consumer report was used. Notice does not

			have to state what criteria the consumer met.

2. Information about the decision

Type of Disclosure	Triggered by	Description	Rationale for inclusion in this category
Mortgage notices	Mortgage lender uses a credit score to make a loan	Consumer's actual credit score obtained by mortgage lender, along with information about the credit score, and the notice to home loan applicants.	Consumer receives the actual score used by the mortgage lender to make a decision about them.
Adverse action notices	Lender takes adverse action, such as denial of credit or employment	Statement of the adverse action, actual credit score used, information about the score: the range of scores, the factors that influenced the score, disclosure of the consumer's right to dispute the accuracy or completeness of the report	Consumer receives the actual credit score used. However, there is no requirement that the user disclose the reasons for the adverse action itself.
Risk-based pricing notices	Provision of credit where lender makes adjustment to credit price that is materially less favorable than most other consumers receive	Statement that terms offered may be less favorable, actual credit score used (if a score was used), identity of the CRA that furnished the consumer report	Consumer receives the actual credit score used in making the decision and notice that credit terms were based on a credit report.
Notices related to employment	Employer seeks to use consumer report for employment purposes	Employer must provide notice that it will obtain a consumer report and obtain consent from the employee before doing so. Before taking an adverse action, consumer must receive a copy of their consumer report and Summary of consumer	Consent required before consumer report used, actual credit score (if credit score was used).

		rights. If an adverse action is taken, the consumer is entitled to the same information as required for other adverse actions	

Equal Credit Opportunity Act

1. Information about the system

Unlike the FCRA, the ECOA does not provide a right for individuals on their own initiative to obtain general information about the credit system, such as through requesting the consumer's file or a credit score. Thus, the disclosures required by the ECOA usually relate to information about a specific decision.

2. Information about the decision

Type of required disclosure	Triggered by	Description	Rationale for inclusion in this category
Adverse action notice	Lender's refusal to grant credit in amount or terms requested, termination of account	Statement of adverse action, statement of specific reasons for the action taken, actual credit score used	The statement of specific reasons for the action taken is related to the particular decision about an applicant's credit.

16 Annex 4 Complaints overview

Complaints received by the independent complaint resolution bodies

Introduction

As per 04 August 2018, 3,447 active organizations were listed as self-certified under the Privacy Shield framework. 327 additional organizations were listed as inactive.
The actual number of entities covered by the Privacy Shield exceeds 3,447, as organizations can choose to list several of their entities (for example, their fully owned subsidiaries).
Each of the 3447 listed organizations' adhere to one or two of the available frameworks, namely:

- the EU-U.S. Privacy Shield and/or
- the Swiss-U.S. Privacy Shield

The data covered can be either HR or non-HR, or both.
According to the Privacy Shield framework, complaints sent by eligible individuals to participating organizations must be answered within 45 days. In the absence of a timely or satisfactory response, eligible individuals can contact the independent recourse mechanisms chosen by the organizations.
In many cases, organizations select different recourse mechanisms to handle non-HR-related requests from HR-related requests (for the latter only DPAs can be selected).
At the time of the analysis, there were 11 (groups) of resolution providers, beside the DPAs. Each listed organization may choose one or several resolution providers to handle their complaints.

Complaints overview

The table below provides an overview of the 11 (groups) of resolution providers, the number of organizations that selected them to handle their Privacy Shield-related complaints, the most recent reporting information available (N.B. all but one had not published the 2017-2018 reports at the time of the analysis), the number of total claims received, the number of eligible claims, and the claims pertaining to ADM and/or profiling.

No.	Resolution provider	No of organization selecting a particular independent recourse mechanism in 2018	Most recent period for which a claims report is available	Total claims received during the reporting time	Number of eligible claims	Number of resolved claims	Profiling or ADM claims as part of the total number of claims reported as received or eligible or resolved
1	Insights Association Privacy Shield Program (N.B. their complaints are actually handled by ICDR/AAA Privacy Shield Program – see 7 below.)	33	15 April 2017 – 31 July 2017	0	0	0	0
2	PrivacyTrust Privacy Shield Program	47	1 Aug. 2016 – 31 July 2017	15	0	0	0
3	Whistic	8	No report available	No report available	No report available	No report available	No report available
4	BBB EU Privacy Shield Program	870	1 Aug. 2016 – 31 July 2017	180 (53 of which by EU nationals)	0 (1 was still pending at the end of the reporting period)	N.A.	0?
5	DMA Privacy Shield Program	44	Aug. 2016 – Aug 2017	5	5	4 processed at staff-to-staff level; 1 pending	0?
6	EU Data Protection Authorities (DPAs)	1531	Only general activity annual reports available for the year 2016/2017. No separate PS reports available.	-	-	-	No PS-related complaint information available in the annual reports of the sample DPAs included (i.e. the UK, Ireland, the Netherlands, France, Belgium and Romania)
7	ICDR/AAA Privacy Shield Program	282	01 Aug. 2016 – 31 July 2017	0	0	0	0
8	JAMS Privacy Shield Program	881	1 Aug. 2017 – 31 July 2018	No information provided	2	2	No information provided

9	TRUSTe (now TrustArc)	572	01 Aug. 2016 - 31 July 2017	788	About 55%	- 285 were resolved by consumer education -1 required issue-specific changes by the Participant (e.g. unsubscribe the user, close the account). -115 fell into other categories such as that fall outside the scope of TRUSTe 's authority under our privacy program, (e.g. billing/transactional issues, requests for feature enhancements). TRUSTe typically suggests that the consumer contact the site directly in these instances. -4 Complaints were pending resolution as of the close of this reporting period.	14 cases of Unauthorized Profile With Personal Information
10	VeraSafe Privacy Shield Program	40	Not available	Not available	Not available	Not available	Not available
11	Privacy Dispute Resolution Services (PDRS)	0	01 Aug. 2016 – 31 July 2017	0	0	0	0

1. Insights Association is a marketing research trade association. It offers, as of the 15th of April 2017, a Privacy Shield Program[390] to its members. The programme includes an independent recourse mechanism for which the services are provided by the International Centre for Dispute

[390] http://www.insightsassociation.org/sites/default/files/misc_files/insights_privacy_shield_program_2017_report.pdf

resolution(ICDR)[391],[392], the international division of the American Arbitration Association. ICDR reports[393] that during the period between the 1st of August 2016 and the 31st of July 2017 no complaints were received.

2. PrivacyTrust[394] is International Charter Ltd, and provides services related to data privacy. During the 1st of August and the 31st of July 2017, they received[395] 15 complaints, none of which was considered valid.

3. Whistic is a security risk assessment and analytics platform providing services to the industry[396]. In addition, it provides an independent recourse mechanism. No annual reporting on Privacy Shield-related complaints available on the website.

4. BBB EU Privacy Shield Program (BBB EUPS) is an independent recourse mechanism created by the Council of Better Business Bureaus (CBBB) specifically for the Privacy Shield. Next to the independent recourse mechanism, BBB EU also provides "compliance assistance for U.S. companies preparing for Privacy Shield self-certification"[397]. CBBB is an umbrella organization of a network of businesses across the U.S. and Canada. During the reporting period, 1 Aug. 2016 – 31 July 2017, BBB EUPS received 180 complaints, 53 of which from individuals from the EU. All complaints but one were considered out of the scope of the programme. One complaint was still pending at the end of the reporting period.

5. The DMA Privacy Shield programme is available to members of the Data & Marketing Association (DMA) and provides dispute resolution services. DMA has recently (July 2018) been acquired[398] by ANA (Association of National

[391] http://go.adr.org/privacyshield.html
[392] Since 2017, ICDR also administers the "Annex I Binding Arbitration Program" on behalf of the U.S. Department of Commerce. "ICDR, in consultation with the U.S. Department of Commerce and its EU counterparts, developed an expedited set of international arbitration rules and arbitrator code of conduct for the (Privacy Shield) program."
https://www.adr.org/sites/default/files/document_repository/AAA_AnnualReport_Financials_2018.pdf
[393] http://go.adr.org/rs/294-SFS-516/images/PrivacyShield_ProgramReport.pdf
[394] https://www.privacytrust.com/about/
[395]
https://www.privacytrust.com/privacyshield/disputeresolution/PrivacyTrust_Dispute_Resolution_Report%20_2016_2017.pdf
[396] https://blog.whistic.com/the-vendor-security-alliance-chooses-whistic-as-its-exclusive-vendor-assessment-platform-9b2365d29be0
[397] https://www.bbb.org/globalassets/local-bbbs/council-113/media/eu-safe-harbor/eups-mini-annual-report-final.pdf
[398] https://thedma.org/blog/data-driven-marketing/stronger-unified-ana-voice-advertising-marketing-growth/

Advertisers) forming the largest trade organization for marketers. The DMA Privacy Shield programme provided a detailed complaints annual report[399] for the period Aug. 2016 – Aug 2017.

6. The International Centre for Dispute resolution (ICDR)[400],[401] is the international division of the American Arbitration Association. ICDR reports[402] that during the period between the 1st of August 2016 and the 31st of July 2017 no complaints were received. ICDR/AAA might be the only recourse body providing multilingual information to potential PS claimants.

7. JAMS[403] describes itself as "the largest private alternative dispute resolution (ADR) provider in the world". "With its prestigious panel of neutrals, JAMS specializes in mediating and arbitrating complex, multi-party, business/commercial cases – those in which the choice of neutral is crucial." JAMS is the only body making available online the 2018 Annual report[404] covering complaints in the period between the 1st of August 2017 and the 31st of July 2018. However, it provides no information about the number or the nature of the complaints received. It mentions only that two cases were eligible and that both eligible complaints were resolved satisfactory within one month. No further details are provided.

8. TRUSTe (renamed TrustArc) is an organization providing privacy and risk assessments, verification and certification for online businesses, as well as a privacy seal. In addition, TRUSTe provides a dispute resolution procedure. The annual report[405] covering the period 01 Aug. 2016 - 31 July 2017 is the most detailed amongst all recourse mechanism providers and the only one mentioning complaints regarding profiling.

9. VeraSafe Privacy Shield Program is a dispute resolution procedure (including facilitation, mediation, and arbitration) for Privacy Shield-related

[399] https://thedma.org/wp-content/uploads/Privacy-Shield-Report-August-2017.pdf
[400] http://go.adr.org/privacyshield.html
[401] Since 2017, ICDR also administers the "Annex I Binding Arbitration Program" on behalf of the U.S. Department of Commerce. "ICDR, in consultation with the U.S. Department of Commerce and its EU counterparts, developed an expedited set of international arbitration rules and arbitrator code of conduct for the (Privacy Shield) program."
https://www.adr.org/sites/default/files/document_repository/AAA_AnnualReport_Financials_2018.pdf
[402] http://go.adr.org/rs/294-SFS-516/images/PrivacyShield_ProgramReport.pdf
[403] https://www.jamsadr.com/about-jams/
[404] https://www.jamsadr.com/files/uploads/documents/annual-report-privacy-shield-cases-2018-08-01.pdf
[405] https://download.trustarc.com/dload.php/?f=FYYE02VY-678

complaints and is administered by Advanced Partnerships LLC ("VeraSafe").[406] Additional services offered by VeraSafe include compliance assessments, privacy certification and privacy seals. No annual report re Privacy Shield-related complaints was available on the programme's website. According to the information on the website, the "Annual Procedure Reports will not be published when no Complaints have been filed with the Procedure."[407]

10. The Privacy Dispute Resolution Services (PDRS)[408] is featured on the list of independent dispute resolution providers although, currently, it appears to have not been selected by any company on the Privacy Shield list. During the reporting[409] period 1st August 2016 - 31st of July 2017 it reports to have received no complaints.

[406] https://www.verasafe.com/privacy-services/dispute-resolution/privacy-shield-dispute-procedure/
[407] https://www.verasafe.com/privacy-services/dispute-resolution/dispute-resolution-procedure/#pub-href
[408] http://www.beyondthecourthouse.com/subject-areas/privacy-dispute-resolution-services/
[409] http://www.beyondthecourthouse.com/wp-content/uploads/2016-17-PDRS-Annual-IRM-Report.pdf

17 Annex 5 Interview protocol

The scope of the interview could be summarize in the following 2 main questions:

1. To what extent is automated individual decision-making (ADM) one of the purposes for which data of EU data subjects are transferred to the U.S. by Privacy Shield-certified companies?

And, if that should be the case,

2. Is the protection afforded to EU data subjects by current U.S. federal- or state-level (legal) mechanisms sufficient/adequate?

General outline of the interview protocol

A.1. Interview duration

- Depending on the interviewee's availability and willingness to engage, the interview is intended to last between 45 min and 1 hour.

A.2. Interview format

- The interview will be semi-structured.
- The issues below reflect the project's research questions and interests and will be used either as direct or indirect questions during the interview.
- Given the limited duration of the interview, as well as the specific expertise of individual interviewees, not all issues are likely to be addressed.
- The expert interviewee should be allowed sufficient room to share new and relevant knowledge not captured by the pre-determined list of issues below.

A.3. Interview output

- Depending on the interviewees' request: interview notes or a summary of the main issues discussed during the interview.

(**Acronym** used below: ADM = automated decision-making.)

B.1. Interview questions - General information regarding the expert

1. Choice and consent regarding the participation in the interview and use of the outcome (e.g. named or anonymous; confidential or on-the-record; interview notes or summary of the conversation; to be shared only with the EC or to be included in a publicly accessible report; direct quotes or not, etc.)
2. Affiliation of the interviewee: government / industry / academic or research / non-profit civil rights
3. Declaration of interest (if applicable)
4. Main area of expertise of the interviewee: legal / technical / commercial / policymaking / regulatory / advocacy etc.
5. Familiarity with profiling & ADM / privacy & data protection. Level of expertise/confidence.
6. Familiarity with the EU privacy and data protection regime.

B.2 Interview questions - Specific questions

7. Opinion on current and near-future use of profiling and ADM
    a. incidence
    b. main application domains
    c. specific domains deserving attention from a privacy & data protection perspective
    d. general public's awareness of profiling & ADM
8. Specific examples of profiling & ADM, if available
9. Assessment of concrete practices of companies employing profiling & ADM – relating to:
    a. data processing in general and at each individual stage
    b. processing of special categories of personal data
    c. technology employed
    d. data business ecosystem
    e. concrete means of observing the rights of data subjects
    f. data subject awareness of the practices
    g. likelihood of impact on EU data subjects

10. Assessment of the applicable federal legal framework – including but not limited to:
    a. availability
    b. adequacy re privacy and data protection
    c. enforceability and oversight
    d. protections afforded to data subjects in general
    e. likelihood of impact on EU data subjects specifically
    f. new and relevant initiatives or developments
11. Relevant case law, if available
12. Assessment of alternative protection mechanisms (e.g. best practices, codes of conduct, standardization, etc.)
    a. availability
    b. accessibility
    c. maturity
    d. quality
    e. likelihood of relevance for EU data subjects
13. Other relevant initiatives (e.g. algorithmic transparency etc.), if available
14. Any further suggestions, opinions, relevant documents, etc. the expert might want to share with the EC.

18 Annex 6 List of expert interviewees

Non-profit / Public interest research group	Ms Pam Dixon, Executive Director, World Privacy Forum
Not-for-profit / non-advocacy information privacy membership association	Ms Rita Heimes, CIPP/E, CIPP/US, CIPM, Research Director & DPO, International Association of Privacy Professionals (IAPP) Ms Müge Fazlioglu, CIPP/E, CIPP/US, International Association of Privacy Professionals (IAPP)
Academic, journalist, author	Mr Adam Tanner, Associate, Institute for Quantitative Social Science, Harvard
Policy think tank	Mr Martin Abrams, Executive Director, Information Accountability Foundation
Non-profit / consumer protection and privacy	Mr Jeff Chester, Executive Director, Center for Digital Democracy (CDD)
Investigative journalist	Mr Jeff Larson, independent, ex-ProPublica, ex-NYT
Industry representatives	anonymous
Industry representative	anonymous
Industry representative	anonymous