Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 96

Adjudication of Artificial Intelligence and Automated Decision-Making Cases in Europe and the United States

Elif Kiesow Cortez & Nestor Maslej

2022

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Authors

Dr. Elif Kiesow Cortez is a TTLF Fellow at Stanford Law School and collaborates with the Stanford Institute for Human-Centered AI. Elif works in designing governance mechanisms for responsible and ethical deployment of technology. Elif has worked in policy advisory, project management, and academic roles on the governance of emerging technologies. Previously, Elif was a John M. Olin Fellow in Law and Economics at Harvard Law School. Her doctoral research at the Institute of Law and Economics, University of Hamburg, Germany, was fully funded by the German Research Association (DFG). During her doctoral studies, she was a visiting researcher at Harvard Business School and at UC Berkeley School of Law. Elif supports organizations by offering guidance on achieving effective policy dialogue across domains and jurisdictions regarding responsible deployment of technology.

Nestor Maslej is a Research Manager at Stanford's Institute for Human-Centered Artificial Intelligence (HAI). In this position, he manages the AI Index and Global AI Vibrancy Tool. Nestor also leads research projects that study AI in the context of technical advancement, ethical concerns and policymaking. In developing tools that track the advancement of AI, Nestor hopes to make the AI space more accessible to policymakers. Nestor also speaks frequently about trends in AI. Prior to joining HAI, Nestor worked in Toronto as an analyst in several startups. He graduated from the University of Oxford in 2021 with an MPhil in Comparative Government, where he used machine learning methodologies to study the Canadian Indian Residential schooling system, and Harvard College in 2017 with an A.B. in Social Studies.

General Note about the Content

The opinions expressed in this paper are those of the authors and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Elif Kiesow Cortez & Nestor Maslej, Adjudication of Artificial Intelligence and Automated Decision-Making Cases in Europe and the United States, Stanford-Vienna TTLF Working Paper No. 96, http://ttlf.stanford.edu.

Copyright

Abstract

Artificial Intelligence (AI) started to impact many facets of the economy and of citizens' routine activities. This article contributes to our understanding of how the legal system is reacting to the ongoing uptake of AI and the disputes or right infringements this might create. Select legal cases regarding the use of AI technology for automated decisions are reviewed, with a focus on filings in Europe and the United States. This exercise reveals which type of legal challenges can be expected when it comes to deploying automated systems in these jurisdictions. Additionally, incipient regulatory efforts targeting AI on both sides of the North Atlantic are introduced and briefly discussed. The paper sheds light on how different legal systems accommodate an emerging technology with disruptive potential and offers a mapping of exemplary legal risks for prospective actors or organizations seeking to develop and deploy AI.

Keywords

Artificial intelligence, court cases, adjudication of artificial intelligence, administrative decisions on artificial intelligence, privacy, bias, artificial intelligence regulation

Table of Contents

1. Introduction

Artificial Intelligence (AI) technology is becoming more prevalent and is increasingly deployed by economic actors in various domains for informing an ever larger number of decisions and practices at many levels. There is a continuous decrease in cost per achieved computing performance and an immense amount of data that is being produced by the ubiquity of digital devices in daily life and across the economy. These two elements combined provide fertile ground for the dissemination and uptake of AI, with the accumulated effects on the shape of economic activity and society overall being difficult to anticipate.

This article offers insights on how rule of law institutions are reacting to the increasing deployment of AI systems and in doing so provides an idea of the various collective responses to AI adoption, the guardrails being developed to contain abuses, and in general the attempt to strike the right balance in achieving benefits while minimizing the risks of this powerful technology. This paper will offer a legal analysis of select legal cases regarding the use of AI technology for automated decisions, oftentimes involving the (mis)use of personal data. The focus lies on exemplary disputes drawn from the US and the EU, and these jurisdictions make for interesting cases in light of the proposed EU Artificial Intelligence Act[1], the US Algorithmic

[1] 'Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 21 April 2021, COM2021/0206 - C9-0146/2021 - 2021/0106(COD)' (2021).

Accountability Act which was reintroduced in 2022[2] and the US AI Bill of Rights of the same year.[3] This paper aims to provide a comparative analysis of regulatory frameworks that affect this breakthrough technology in the US and the EU and will bring to light which type of legal challenges can be expected when it comes to deploying AI based automated decision-making in these jurisdictions by also highlighting the role of pursuing a risk-based approach.

More specifically, the paper presents an overview and analysis of selected cases: from the EU judiciary and administrative authorities and from US courts on a range of artificial intelligence and automated decision-making subjects including automated web scraping, facial recognition, voice recognition for detecting emotions, and government use of digital welfare fraud detection systems, algorithms assisting judicial decisions, computerized rules to process personal injury protection claims, automated recommender systems in social network leading to harmful content, AI's eligibility to obtain patent rights, use of facial recognition technology during exam sessions, use of digital fraud detection systems in the insurance sector, and discriminatory social media algorithms. The information from the US and EU case studies offered in this paper will improve our understanding of legal hurdles for AI deployment, widen our knowledge on jurisdictional heterogeneity in legal treatment, and therefore contribute to reducing legal uncertainty around making AI work in practice.

[2] S.3572 - Algorithmic Accountability Act of 2022, 'S.3572 - 117th Congress (2021-2022): Algorithmic Accountability Act of 2022' (3 February 2022) <http://www.congress.gov/> accessed 20 December 2022.

[3] 'Blueprint for an AI Bill of Rights | OSTP' (*The White House*) <https://www.whitehouse.gov/ostp/ai-bill-of-rights/> accessed 20 December 2022.

The paper will further analyze the trade-offs and legal reasoning that potentially lay behind rulings in AI cases on each side of the Atlantic. Additionally, the legal reasoning behind the rulings that are part of the analysis will be compared to the principles set out in the draft EU regulation – which incidentally is intended to be extraterritorially applicable. The article analyzes the way that regulatory and legal systems are de facto accommodating AI system deployment primarily by summarizing and breaking down essential elements of select judicial and administrative case examples from the European Union and the Unites States where the use of algorithmic systems was brought to court. In order to better capture the current status quo judicial reasoning on AI as reflected in the rulings, the article focuses on the select cases from the time period between 2017 and 2022. Additionally, the article briefly discusses incipient regulatory initiatives on both sides of the Atlantic targeting AI and automated decision-making.

The EU-US 'Joint Roadmap for Trustworthy AI and Risk Management' was announced on the 1st of December 2022, with the aim of advancing shared terminologies and taxonomies and inciting transatlantic communication on metrics for measuring AI trustworthiness and risk management methods in order to promote common values, to safeguard human rights, to support the planet, and to bolster market innovation.[4]

According to the draft EU Artificial Intelligence Regulation, an AI system is defined as follows: "'artificial intelligence system' (AI system) means software that is developed

[4] 'TTC Joint Roadmap for Trustworthy AI and Risk Management | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management> accessed 19 December 2022.

with one or more of the techniques and approaches listed in Annex I[5] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with." Throughout the paper we will be using the definition broadly to cover existing automated systems and how the existing case law and enforcement decisions handle these systems in order to contribute to the further understanding of the status quo view of the judiciary on automated systems across the Atlantic with an aim to inform the current and future debates on how AI systems are likely to be treated by the judiciary. We will be providing an overview and analysis of selected cases, including six cases from the EU judiciary and administrative authorities and seven cases from US courts from the time period between 2017 and 2022.

2. Emerging AI rules

This section will cover the current regulatory frameworks existing or being developed that are applicable to artificial intelligence and automated decision-making systems in the EU and in the US.

[5] The techniques underlying AI systems as per the EU AI Act are listed under Annex I and are the following: "(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods."

2.1. EU AI Act

The EU Commission proposed the Artificial Intelligence (AI) Act in April 2021 and stated that the proposed regulation will serve the goal of enabling the EU to build strategic leadership in high-impact sectors, facilitating the development and uptake of AI in the EU, making the EU the place where AI thrives from the lab to the market and ensuring that AI works for people and is a force for good in society.[6] Possible amendments to the regulation have been proposed both by the European Union Council and the European Parliament, which could have a broad impact on the regulation's overall scope and content. As reported by CEPS, the co-legislators are likely to reach an agreement by mid-2023, but it depends on whether they can agree on key issues such as the definition of AI, risk classification and associated regulatory remedies, governance arrangements, and enforcement policies.[7]

According to the draft EU Artificial Intelligence Regulation, an AI system is defined as follows "'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".

[6] 'A European Approach to Artificial Intelligence | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 19 December 2022.

[7] 'CEPS-In-Depth-Analysis-2022-02_The-AI-Act-and-Emerging-EU-Digital-Acquis.Pdf' <https://www.ceps.eu/wp-content/uploads/2022/09/CEPS-In-depth-analysis-2022-02_The-AI-Act-and-emerging-EU-digital-acquis.pdf> accessed 19 December 2022.

Annex I brings further clarity to this definition regarding the techniques and approaches such as:

"(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods."

In comparison, the US AAA 2022 works with a definition that focuses less on the specific techniques underlying AI but rather emphasizes the process of decisions having been reached in an automated way.

In the EU this prospective AI regulation is making its way through the legislative process. In December 2022 the Council, reflecting the collective position of EU member state governments, agreed on a version of the text for the EU AI Act. Parallel to that the European Parliament is on its way to defining their own commonly agreed position acceptable to different political groupings, and thereafter trilateral negotiations involving Council, European Parliament and European Commission will be held before a final version can become law.

The negotiations are ongoing, however cornerstones and main features of the overall regulatory approach taken are already determined. First, the EU AI Act is set out to be

a horizontal regulation, which means that it formulates a common set of rules on AI applicable horizontally across the different sectors of the economy.[8] In contrast, even if this hard to predict at this point, it is conceivable that the regulatory framework for AI and automated systems emerging in the US evolves more in the direction of a sector-based approach, at least when compared to the European regime.

Second, the approach taken intends to be risk-based in the sense that application domains in which AI will be deployed are categorized according to the risk that is deemed to be posed by utilizing AI in that specific domain. The European Commission as drafter of the Act expects most uses of AI to pose 'low risk' and, following the EU AI Act's risk-based approach, exempts this vast majority of applications of AI from any binding obligations. An example of a use case deemed low risk is an AI system used in spam filter. At the other extreme the Commission identified and listed a select number of uses cases in which the use of AI is forbidden due to 'unacceptable risk'. Among these completely banned practices are using AI for social scoring or using AI systems that exploit the vulnerabilities of a specific group of persons. The use cases falling within the 'high risk' category might be most interesting to the reader because for this category the EU AI Act requires concrete and binding measures, i.e., an ex-ante conformity assessment before the AI system is put on the market accompanied by an ongoing risk management system for when it has entered the market. Examples of use cases in this category are systems that assess the creditworthiness of consumers, systems used for recruitment and management of employees, or systems

[8] This stands in contrast to, for instance, one of the discarded alternative regulatory approaches that were considered, an approach which would consist of various sector specific rules and obligations.

used in the administration of justice. And lastly, there is the 'limited risk' category, ranking just above the low risk one, and chatbots can be mentioned as an example falling under this limited risk category. The EU AI Act demands a limited set of transparency obligations to be met for AI systems in this category. One can think for instance that consumers should be made aware that they are interacting with an AI-operated chatbot.

A crucial issue for successfully implementing the risk-based approach is the question of how use cases are assigned a risk category and the procedure to review or update the classification. The legitimacy and success of the regulation hinges to a considerable degree on the quality of this classification process.

Next, a third notable feature of the incipient European AI regulation, it relies on the standard EU product legislation approach with its technical procedural style but adds to it by introducing the fundamental rights of the EU as a crucial set of principles for the EU AI Act.[9]

The product legislation approach is concerned with ensuring the safety of mostly physical products such as children's toys or medical equipment, and it often relies on, e.g., pre-market conformity assessments. Products then get CE marking, which is an administrative marking that can be affixed by the manufacturers themselves indicating conformity of a product with the relevant EC Directives.

[9] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 Computer Law Review International 97.

This is also of vital importance with respect to the EU internal market, also referred to as the single market, since marked products can then be freely traded across European countries. This is helped by the existence of applicable 'harmonised standards' across Europe for a range of products, which support the free trade of the relevant products across the participating jurisdictions. The EU AI Act aims to create an equivalent regime for AI systems with harmonized rules that allow them to be commercialized across Europe, with the goal being that this happens in a lawful, safe and trustworthy manner.[10]

Another feature of European product regulation approach is that the formulation of specific technical rules is to a significant extent delegated to private standardization organizations such as CEN (European Committee for Standardisation) and CENELEC (European Committee for Electrotechnical Standardisation). These precise organizations will also play a role in AI standard specification in connection to the forthcoming AI regulation as evidenced by the European Commission's standardization request from December 2022.[11] However, in the case of regulating AI systems, the fundamental rights protections enshrined in the draft EU AI Act might pose a challenge to these organizations whose expertise is oriented rather towards strictly technical matters.

[10] Also, the AI Act can be seen in conjunction with other regulations and initiatives aiming to boost the digital sector Europe-wide, such as the AI Liability Directive, the Digital Services Act, the the Digital Markets Act and the Data Governance Act, all of which are linked to the EU Digital Single Market Strategy.

[11] https://ec.europa.eu/docsroom/documents/52376?locale=en

Another aspect of the draft EU AI Act is its extraterritorial application which means that it has the potential to influence practices beyond Europe's borders. Regarding its sanctioning regime, the draft Act foresees three levels of severity of fines. The most significant fines are levied for violating the prohibition of specific AI systems, and they can go up to 30 million Euros or 6% of the violating company's turnover. A considerable part of the fine regime concerns the rules for high-risk systems, and it targets the different actors along an AI system's life cycle, i.e., not only 'providers' but also 'users'[12], importers, distributors, and notified bodies can be subject to high sanctions. However, the draft Act also determines that SMEs and start-ups would face relatively lower fines for infringements.

2.2. US Algorithmic Accountability Act 2022

In February 2022 the Algorithmic Accountability Act of 2022 (AAA) was presented to the US Congress.[13] In light of uneasiness with the use of automated systems to reach decisions in domains such as housing, education, employment, healthcare, lending, or healthcare, the AAA is supposed to enhance transparency of algorithm in various contexts in order to minimize discriminatory, biased or harmful decisions.

[12] For clarification, 'users' as defined in the EU AI Act are basically organizations deploying the AI system.

[13] An earlier version of this Act was introduced in April of 2019 but did not garner sufficient backing for ultimately getting enacted. Major revisions were made in the 2022 version, for instance when compared to the earlier 2019 version, the new one contains stricter impact assessment requirements. However, it is also still unclear whether or when the 2022 version could become law.

In general, the goal of the AAA is to be able to hold organization to account when they deploy algorithms or automated systems for generating decisions in a manner that significantly affects individuals in the US. In this line the AAA proposes government-mandated "impact assessments" for organizations that use automated decision systems, and impact assessments follow a two-pronged approach as they should be conducted both before deployment and after deployment in form of augmented decision-making processes.[14]

Going forward the FTC would need to determine the content, form, and other details of the impact assessments. Also, the precise requirements of impact assessments can evolve overtime in reaction to, for example, judicial decisions, civil society demands, or technological advances.[15]

The AAA in its current form already contains indications of what should be included in the impact assessments, which will have to be conducted by 'covered entities' for their ADS (automated decision systems) and ACDP (augmented critical decision processes) with inputs from relevant stakeholders.[16] The AAA determines that impact assessments should at least include the following steps (Sec. 4(a)):

- describe the existing decision process and compare with the augmented process outlining the intended benefits, need, and purpose;

[14] Jakob Mökander and others, 'The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: What Can They Learn from Each Other?' (2022) 32 Minds and Machines 751.
[15] Jacob Metcalf, Brittany Smith and Emanuel Moss, 'A New Proposed Law Could Actually Hold Big Tech Accountable for Its Algorithms' [2022] *Slate* <https://slate.com/technology/2022/02/algorithmic-accountability-act-wyden.html> accessed 14 December 2022.
[16] Covered entities

- identify and describe consultations with stakeholders, as well as their recommendations, explaining the decision of whether these were incorporated;
- ongoing testing for privacy risks;
- ongoing testing for performance, including a description of methods and criteria used, additionally test for differential performance according to demographic groups;
- continuously review industry best practices and risk mitigation and train relevant agents;
- assess the need for limitations and limitations on the use of ADS and integrate these into the product or its terms of use;
- keep data and other input information used to develop, test, update, or maintain the ADS as well as the reasons for the choice of data;
- assess the rights of consumers, paying attention to transparency, explainability, and mechanisms for contesting, recourse, and opting out;
- identify likely negative impacts in a structured way and evaluate mitigation strategies;
- describe ongoing documentation of the development, testing, and deployment processes;
- identify stakeholder engagement processes that could prove beneficial, identify capabilities, tools, protocols, and standards to improve the ADS or impact assessment with regard to performance (i.e., accuracy, robustness, reliability), fairness (i.e., bias, nondiscrimination), transparency, explainability,

contestability, an opportunity for recourse, privacy and security, personal and public safety, among others;

- include a reasoning in case any of the requirements above were not followed.

Commenters have pointed out what they think are shortcomings of the AAA.[17] First, they have pointed out that the Act applies only to large private companies, exempting SMEs and government agencies from regulatory scrutiny. Second, the AAA is blamed for lacking detail and specificity at times. For one, a number of relevant policy choices are left to be determined by the Federal Trade Commission. Next, the language criticized for being vague besides reliance on qualifiers such as 'to the extent possible' potentially rendering the Act weakly enforceable. Also, commenters criticize the AAA for not taking into account some potential tradeoffs involved, for instance with regard to safeguarding equal treatment of protected groups while simultaneously aiming for accuracy, efficiency and privacy. Further it is pointed out that the AAA aims to more narrowly protect consumers from AI-related risks instead of protecting citizens as a broader category.

It is not immediately clear how strong of a priority it will be for the US administration to get the AAA passed in the near future, with approval pending in the House of Representatives and the Senate. While aware of risks from decisions relying on automated systems, the US seems to deem innovation and the vibrancy of its

[17] Jakob Mökander and Luciano Floridi, 'From Algorithmic Accountability to Digital Governance' (2022) 4 Nature Machine Intelligence 508.

technology sector of significant importance, including of a geopolitical nature, and might consider following a relatively measured or gradual regulatory approach.

However, given US's federal structure, regulation of AI systems can already start at subnational level, as exemplified with New York City's Law on Automated Employment Decision Tools, which determines that automated systems used for hiring decisions used January 2023 onwards was on track to require to get an audit for bias conducted by an independent auditor and that assesses potential disparate impact on certain groups.[18] On the 12th december 2022, The Department of Consumer and Worker Protection (DCWP) announced it would postpone enforcement until April 15, 2023.[19] According to the agency's statement, a second public hearing is being planned due to the high volume of public comments.[20]

2.3. US AI Bill of Rights

The White House's 'blueprint' for an AI Bill of Rights (AIBoR) was published in October 2022. It does not constitute hard law, however it provides a relevant framework that will potentially guide and inform AI laws and policymaking in the US. This is the latest and major initiative by the Biden administration showcasing its approach to the

[18] Benjamin Cedric Larsen, 'The Geopolitics of AI and the Rise of Digital Sovereignty' (*Brookings*, 8 December 2022) <https://www.brookings.edu/research/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/> accessed 14 December 2022.

[19] 'AI Bias Law Postponed until April 15 as Unanswered Questions Remain' (*VentureBeat*, 12 December 2022) <https://venturebeat.com/ai/for-nycs-new-ai-bias-law-unanswered-questions-remain/> accessed 19 December 2022.

[20] 'New Laws & Rules - DCA' <https://www.nyc.gov/site/dca/about/new-laws-rules.page#:~:text=December%202022%20Update%3A%20The%20Department,144%20until%20April%2015%2C%202023.> accessed 19 December 2022.

regulation of AI algorithms. The AIBoR lays out AI-related potential civil rights harms and presents five principles to be observed as well as a more detailed companion containing guidance on how to implement the principles.

The first principle demands AI systems to be 'safe and effective', which calls for pre-deployment testing for risks and harm mitigation. Second, 'notice and explanation' should be provided, a principle that emphasizes both making persons aware that they are facing an AI system and being to some degree transparent by way of proving information on how the AI system generates decisions. Third, a 'right to data privacy' should be observed – this principle relates to persons retaining control over how their data is used and prescribes data minimization, but also calls for heightened oversight for AI in the context of surveillance systems. Fourth, the right to 'protection from algorithmic discrimination' demands assessments regarding equity and continuous alertness to and mitigation of disparities. The fifth and last principle asks for 'human alternatives, consideration, and fallback', providing persons a way to opt out or access a human with the means to review and override decisions generated by algorithm.

The AIBoR focuses on AI system use in human services, for example in education, health services, lending, hiring, commercial surveillance, among others. Hence it is not a comprehensive AI guidance as it lacks emphasis on utilization of algorithms

within most consumer products, online information ecosystems, or critical infrastructure.[21]

2.4. EU-US Roadmap

In order to promote responsible artificial intelligence in both sides of the Atlantic, the United States and the European Union published a "joint roadmap on evaluation and measurement tools for trustworthy AI and risk management" on December 2022.[22] The roadmap is issued as an output of the EU-US Trade and Technology Council and it states as its aim to commit to OECD's recommendation on AI.[23]

In May 2022, the U.S.-EU Joint Statement of the Trade and Technology Council declared that that the parties confirm their "commitment to collaboration in developing and implementing trustworthy AI through a human-centered approach that reinforces shared democratic values and respects human rights".[24] The report also declared that the intentions to develop a joint road map on AI risk management. It was stated that the parties are dedicated "to develop a shared hub/repository of metrics and methodologies for measuring AI trustworthiness and AI risks" so that this

[21] Alex Engler, 'The AI Bill of Rights Makes Uneven Progress on Algorithmic Protections' (*Brookings*, 21 November 2022) <https://www.brookings.edu/2022/11/21/the-ai-bill-of-rights-makes-uneven-progress-on-algorithmic-protections/> accessed 14 December 2022.
[22] https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management
[23] https://oecd.ai/en/ai-principles
[24] US-EU Trade and Technology Council, 'U.S.-EU Joint Statement of the Trade and Technology Council' (2022) <https://www.commerce.gov/sites/default/files/2022-05/US-EU-Joint-Statement-Trade-Technology-Council.pdf> accessed 18 December 2022.

could be used to evaluate the technical requirements for trustworthy AI and bias mitigation as well as facilitating interoperable approaches to manage AI risks.[25]

In December 2022 the EU-US 'Joint Roadmap for Trustworthy AI and Risk Management' was made public, with the aim of advancing shared terminologies and taxonomies and fomenting transatlantic communication on metrics for measuring AI trustworthiness and risk management methods.[26] In this report, both parties reaffirmed that "a risk-based approach and a focus on trustworthy AI systems can provide people with confidence in AI-based solutions, while inspiring enterprises to develop trustworthy AI technologies".[27] The report emphasizes the importance of using a risk-based approach to AI which may be the key to developing trustworthy AI systems that enhance innovation, reduce trade barriers, boost market competition, operationalize common values, and protect human rights.

3. Case law selection – A transatlantic perspective

When a revolutionary technological innovation starts being utilized by economic actors, the legal systems start to process its potential ramifications and understand its operating principles to in turn offer a legal response. Naturally, how actors in the legal system in different jurisdictions perceive the risks and benefits from the use of

[25] ibid.
[26] 'TTC Joint Roadmap for Trustworthy AI and Risk Management | Shaping Europe's Digital Future' (n 6).
[27] EU-US TTC, 'TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management' (2022).

AI will affect judicial decisions concerning this expanding new technology. In short, the paper will be aiming to analyze the selection of cases by focusing on which legal definitions were used by the judiciary in their decisions. The paper would conclude with a forward-looking exercise on what the current application of a rule in a given case might mean for future applications of this rule for emerging technologies and also discuss the shape EU's (draft) regulation is starting to take. Moreover, the research project will offer a breakdown of the nature of legal responses in different domains to assess to what extent sectoral differences exist, e.g. carve outs for strategic R&D projects, but also sectors with user-contact where AI technology is already being rolled out or beginning to be scaled up. We will be providing an overview and analysis of selected cases: six cases from the EU judiciary and administrative authorities and seven cases from US courts, including cases from the time period ranging from 2017 until 2022.

3.1. Case law examples: Europe

The following section presents selected cases from the EU, that involve disputes on issues such automated web scraping, facial recognition, voice-recognition for detecting emotions, and government use of digital welfare fraud detection systems.

3.1.1. Childcare Benefits & SyRI Cases – Netherlands (11/25/2021) & (2/5/2020)

A December 2022 report on the bias in algorithms, artificial intelligence and discrimination prepared by the European Union Fundamental Rights Agency states in its foreword that AI based algorithms are increasingly more important as they are used for essential decision-making systems such as "determining who will receive state benefits".[28] [29] In 2021, the Dutch government resigned due to what was called "childcare scandal" as it was discovered that the algorithm used for risk assessment to detect welfare fraud was biased towards foreigners. [30] [31] It was reported that around 1115 children were taken away from their family homes due to their caregivers being wrongly assessed as involved in fraudulent activities as a result of the biased algorithm.[32] An Amnesty International report described that algorithm reinforced the existing institutional bias of a racial/ethnic link between crime and race and ethnicity and with no meaningful human oversight, the self-learning mechanism reproduced discriminatory design flaws by adapting the algorithm to

[28] EFRA., *Bias in Algorithms: Artificial Intelligence and Discrimination.* (Publications Office 2022) <https://data.europa.eu/doi/10.2811/25847> accessed 20 December 2022.
[29] Sandra Wachter, 'Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR' (2018) 34 Computer Law & Security Review 436.
[30] Silvia Amaro, 'Dutch Government Resigns after Childcare Benefits Scandal' (*CNBC*, 15 January 2021) <https://www.cnbc.com/2021/01/15/dutch-government-resigns-after-childcare-benefits-scandal-.html> accessed 20 December 2022.
[31] 'Dutch Childcare Benefit Scandal an Urgent Wake-up Call to Ban Racist Algorithms' (*Amnesty International*, 25 October 2021) <https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/> accessed 20 December 2022.
[32] 'Meer dan duizend kinderen gedupeerden toeslagenaffaire uit huis geplaatst' (19 October 2021) <https://nos.nl/artikel/2402299-meer-dan-duizend-kinderen-gedupeerden-toeslagenaffaire-uit-huis-geplaatst> accessed 20 December 2022.

experience over time.[33] The report defines this as a discriminatory loop in which non-Dutch nationals were flagged more frequently for fraud than Dutch nationals.[34]

On 25th November 2021, the Dutch Data Protection Authority fined the Minister of Finance 2,75 million EUR as the Tax and Customs Administration automatically categorized certain applications as risky while the algorithm used the nationality of applicants as an indicator (Dutch/non-Dutch).[35] Using a self-learning algorithm, the risk classification model tests all applications within a month, and this algorithm automatically selected requests for which human resources are available is deployed. In that month, based on the algorithm's risk assessment, the 100 applications with the highest risk score were presented to an employee for manual review. It was noticed that March 2016 to October 2018, the model included an indicator "Dutch nationality/non-Dutch nationality

The Amnesty International reported that the Dutch Government had knowledge on the risk of the human rights impacts of using algorithmic decision-making systems such as SyRI.[36] The Hague District Court ruled on the 5th February 2020 that the Dutch government can no longer use the digital welfare fraud detection system SyRI (system risk indication – systeem risico indicatie) on the basis that it violated the European

[33] Amnesty International, 'Xenophobic Machines: Discrimination Through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal' (2021).
[34] ibid.
[35] 'Boete Belastingdienst voor discriminerende en onrechtmatige werkwijze' <https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-discriminerende-en-onrechtmatige-werkwijze> accessed 20 December 2022. The decision can be accessed at the Dutch Data Protection Authority website: <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_belastingdienst.pdf> accessed 19 December 2022.
[36] Amnesty International (n 33).

Convention on Human Rights (ECHR) Article 8 which protects the right to respect for private and family life.[37] SyRI was a system used for its ability to assist the government in identifying individuals at risk of engaging in fraud when it comes to social security, taxation, and employment laws.[38] The Article 8 reads "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.".

The case also has a special importance as it is one of the world's first court decisions to stop the use of digital welfare technologies on human rights grounds as observed by the UN Special Rapporteur on extreme poverty and human rights in this case.[39] In its analysis of the SyRI case, the court expressed similar concerns as the Special Rapporteur, and warned that SyRI could discriminate on the basis of socio-economic status and migrant status without additional information regarding how the automated system works.[40]

[37] 'SyRI legislation in breach of European Convention on Human Rights' <https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Den-Haag/Nieuws/Paginas/SyRI-legislation-in-breach-of-European-Convention-on-Human-Rights.aspx> accessed 20 December 2022. The decision can be accessed at the Hungarian Data Protection Authority website: < https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:865> accessed 19 December 2022.

[38] EFRA. (n 30).

[39] 'Landmark Ruling by Dutch Court Stops Government Attempts to Spy on the Poor – UN Expert' (*OHCHR*) <https://www.ohchr.org/en/press-releases/2020/02/landmark-ruling-dutch-court-stops-government-attempts-spy-poor-un-expert> accessed 20 December 2022.

[40] ibid.

These proceedings were initiated against the Netherlands State by a number of civil society interest groups, including the Dutch Section of the International Commission of Jurists (NJCM) and two private individuals. As a party to the claimants' proceedings, the Dutch Trade Union Confederation (FNV) joined as a party. The claimants asked for stopping the use of SyRI while claiming that Dutch government should be accused of violating human rights unlawfully by using this automated system.[41]

The decision of the court states that NJCM et al. who were being joined in this procedure by the FNV and the Special Rapporteur on extreme poverty and human rights, have provided detailed explanations of their view that SyRI is discriminatory and stigmatizing. It was argued by the parties that SyRI would facilitate further investigation of neighborhoods that were currently recognized as problematic areas. Thus, they suggested that there would be a greater likelihood that irregularities would be found in those than in other neighbourhoods. It was argued that this would reinforce the negative perception that the relevant neighbourhood and of its residents, and strengthen stereotyping even though no risk notifications have been issued.[42]

[41] Rechtbank Den Haag, 'ECLI:NL:RBDHA:2020:865' (2020) <https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:865>.
[42] ibid.

3.1.2. Budapest Bank Case – Hungary (2/8/2022)

Budapest Bank has been fined EUR 634,000 by the Hungarian Data Protection Authority (NAIH) on the basis that the bank automated the evaluation of customers' emotional states using an artificial intelligence-driven software solution.[43] Using the speech evaluation system, the bank determined which customers needed to be recalled based on their mood. This application was used to prevent complaints as well as to retain customers.[44]

Reporting phone calls of customers is common practice among many companies. In a former case brought to the attention of French Data Protection Authority, recording customer phone calls only led to a fine when other GDPR requirements such as implementing data minimization was not achieved.[45] In other words, solely the recording of customer calls is not prohibited under the GDPR as long as the other requirements of the regulation are complied with. However at the case of the Budapest Bank, in addition to recording all customer service telephone calls, the data controller automatically analyzed all new audio recordings every night using artificial intelligence. The software can also predict the emotional state of the client at the time of the call based on the keywords that are detected. In conjunction with the

[43] 'Data Protection Issues Arising in Connection with the Use of Artificial Intelligence | European Data Protection Board' <https://edpb.europa.eu/news/national-news/2022/data-protection-issues-arising-connection-use-artificial-intelligence_en> accessed 19 December 2022.
[44] ibid. The decision can be accessed at the Hungarian Data Protection Authority website: <https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei> accessed 19 December 2022.
[45] CNIL, 'Délibération SAN-2020-003 Du 28 Juillet 2020' (2020) <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042203965/>.

voice call, the emotional analysis result of the data subjects were also stored within the system for 45 days.[46]

The key findings of the decision reported by the European Data Protection Board (EDPB) states that based on the audio recording of the customer service telephone call, a list of people is compiled based on the likelihood of dissatisfaction and anger. The results of the analysis are utilized to identify clients whose dissatisfaction can be assessed by customer service personnel. The data subjects were not informed about this particular data processing and they are not technically entitled to object, and the data processing was planned and carried out despite this. Additionally, the data controller's impact assessment confirmed that the reviewed data processing relies on artificial intelligence and poses a high risk to the fundamental rights of individuals.[47]

The decision text details the NAIH's analysis on the impact assessment that the assessment was deemed by the authority as formally correct, however its content did not correspond to reality. It was concluded that the assessment did not deal with the issue of the analysis of emotions in any meaningful way[48] and based on the company's statements it was decided that the company was clearly aware of these

[46] 'Data Protection Issues Arising in Connection with the Use of Artificial Intelligence | European Data Protection Board' (n 43).
[47] ibid.
[48] Peter Lewinski, Jan Trzaskowski and Joasia Luzak, 'Face and Emotion Recognition on Commercial Property under EU Data Protection Law' (2016) 33 Psychology & Marketing 729.

shortcomings when preparing the impact assessment, as well as during the mandatory regular checks during operational and GDPR compliance reviews.[49]

The fact that these shortcomings were known by the Budapest Bank was also seen from the NAIH decision which reports that in an internal memo related to a customer complaint emphasized that no profiles were created on customers. The NAIH decision quotes the internal memo as follows: "*the software analyzes the audio recording according to [...] - the developer's business secret - aspect. Among these, the developer described the speed, volume, pitch, and length of speech pauses as examples. As a result of the analysis, no profile is created, but the recordings are ranked daily by the system*."[50]

The key findings summarized by the EDPB report that it was clear from both the impact assessment and the legitimate interest assessment that no actual risk mitigation measures were provided, and only some insufficient measures such as information and right of objection were existing on paper. Given the complexity of artificial intelligence systems, in order to achieve transparent and safe deployment of this technology, additional safeguards are required as AI systems are prone to bias as it is difficult to verify the complete results of the processing of personal data by the algorithm. [51]

[49] NAIH, 'Case Number: NAIH-85-3/2022' (2022) <https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei>.
[50] ibid.
[51] 'Data Protection Issues Arising in Connection with the Use of Artificial Intelligence | European Data Protection Board' (n 43).

The proposed EU AI Act[52] addresses the issue of emotion recognition systems with defining these systems in Article 3.34. as "an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data". A report by the Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs published on April 2022 cites the amendments suggested by the Parliament regarding the definition of the emotion recognition system, and this amendment proposes to expand the relevant definition in the following manner "..inferring emotions, thoughts, states of mind or intentions of natural persons..". [53]

The explanatory memorandum of the EU AI Act attends this by indicating that the transparency obligations will be applicable to AI systems : "that (i) interact with humans, (ii) are used to detect emotions or determine association with (social) categories based on biometric data, or (iii) generate or manipulate content ('deep fakes')." The relevant section of the EU AIA also states that individuals must be informed when they interact with an AI system or when their emotions or characteristics are recognized through automated means and the Recital 70 of the current version of the proposed Act reads "… natural persons should be notified

[52] 'Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 21 April 2021, COM2021/0206 - C9-0146/2021 - 2021/0106(COD)' (n 3).

[53] Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs, 'DRAFT REPORT on the Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM2021/0206 – C9 0146/2021 – 2021/0106(COD))' (2022).

when they are exposed to an emotion recognition system or a biometric categorisation system".[54]

3.1.3. Clearview AI case – France, Italy & Greece (10/17/2022)

The last case in this section will be focusing on the decision regarding Clearview AI, a software company extracting publicly available images in significantly large amounts. On 17th October the French Data Protection Authority (CNIL) issued a penalty of 20 million Euro for Clearview AI. This was the third fine to the same amount issued to the company in 2022 by EU data protection authorities. The decision was aligned with the earlier decision of the Italian Data Protection Authority which issued another 20 million Euro fine to Clearview AI on the 10th of February. The company also faced the same amount of fine by the Greek Data Protection Authority on the 13th of July.[55] [56] Also on the 23rd of May 2022, the company was fined 7.5 million pounds by the UK Data Protection Authority (Information Commissioner's Office – ICO) and was ordered to delete the data belonging to UK residents.[57]

---

[54] 'Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 21 April 2021, COM2021/0206 - C9-0146/2021 - 2021/0106(COD)' (n 3).

[55] 'Facial Recognition: Italian SA Fines Clearview AI EUR 20 Million | European Data Protection Board' <https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en> accessed 19 December 2022. The decision can be accessed at the Greek Data Protection Authority website: <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362> accessed 19 December 2022.

[56] 'Hellenic DPA Fines Clearview AI 20 Million Euros | European Data Protection Board' <https://edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en> accessed 19 December 2022. The decision can be accessed at the Greek Data Protection Authority website: < https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-stin-etaireia-clearview-ai-inc> accessed 19 December 2022.

[57] 'Clearview AI Inc.' (26 May 2022) <https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/> accessed 19 December 2022.

CLEARVIEW AI extracts and collects images, photos and videos, from a variety of sources, including social media. This would refer to collecting all of the photos that are directly accessible without creating an account or logging in.[58] On its own website, Clearview AI promotes their product as an "investigative platform" that "allows law enforcement to rapidly generate leads to help identify suspects, witnesses and victims".[59] The company reportedly has amassed over 20 billion publicly available facial images.[60] Given this astonishingly large dataset that was created, the company sells law enforcement agencies access to its database which promotes an image search engine to facilitate the identification of suspects and victims.[61] [62]

In their analysis of the case, CNIL decision states that an extensive amount of photographic data is collected by the company in the present case[63], which are associated with other personal data likely to reveal a variety of aspects of a person's private life, which constitutes an extremely intrusive form of processing. This data is used to create a biometric template, i.e. biometric data, if it is reliable, allowing to

[58] 'Facial Recognition: 20 Million Euros Penalty against CLEARVIEW AI | CNIL' <https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai> accessed 19 December 2022.

[59] 'Clearview AI | Facial Recognition' (*Clearview AI*) <https://www.clearview.ai> accessed 19 December 2022.

[60] 'Clearview AI Now Features 20B Facial Images' <https://iapp.org/news/a/clearview-ai-now-features-20-billion-facial-images/> accessed 19 December 2022.

[61] 'Facial Recognition: 20 Million Euros Penalty against CLEARVIEW AI | CNIL' (n 58).

[62] See also: Elif Kiesow Cortez, 'Data Protection Around the World: Future Challenges' in Elif Kiesow Cortez (ed), Data Protection Around the World: Privacy Laws in Action (Springer - TMC Asser Press 2021); Katelyn Ringrose, 'Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns Essay' (2019) 105 Virginia Law Review Online 57; Yana Welinder, 'A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks' (2012) 26 Harvard Journal of Law & Technology 165.

[63] Reportedly 20 billion images, see w AI Now Features 20B Facial Images' <https://iapp.org/news/a/clearview-ai-now-features-20-billion-facial-images/> accessed 19 December 2022.

identify a person uniquely from a photograph of the individual. The authority declares that the detention of such data by a third party also constitutes a significant privacy invasion.

According to the Article 83.5. of the GDPR, the data protection supervisory authority can impose administrative fines in respect of infringements of the GDPR "up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher".[64] Clearview AI was fined 20.000.000 EUR by the French Data Protection Authority (CNIL) on the 17 October 2022. CNIL explained the amount of the fine stating that the company did not provide any information relating to its turnover despite the CNIL's requests. Conducting own research CNIL found that journalistic sources report that the company was valued at 130 million euros at the start of 2021. The authority stated that the final amount was deemed appropriate considering that a substantial administrative fine must be imposed in order to be effective, dissuasive and proportionate, given the extent of the processing, the seriousness of the breaches, and the biometric nature of the personal data involved.[65]

The decision details that it is necessary to determine whether the persons concerned were reasonably expected to be subject to such processing at the time and within the context of the collection of the personal data. In this respect, Clearview AI had no

[64] '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).

[65] CNIL, 'Délibération SAN-2022-019 Du 17 Octobre 2022 - Légifrance' <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046444859> accessed 19 December 2022.

relationship with the data subjects. This may be understood in the context of the GDPR where the collection of user's data is strictly regulated by imposing several obligations to the collecting party, such as informing the user of their rights or collecting their consent.

CNIL also refers to the reasonable expectation of individuals regarding the privacy of their photos. The ruling highlights that it is reasonable for the data subjects to expect that third parties will be able to access the photographs from time to time, the public nature of these photographs cannot be considered sufficient to conclude that the subjects can reasonably expect their images to be used in data processing. It is also pointed out in this justification that the software used by the company is not publicly available, and the vast majority of those concerned are unaware of its existence. This section of CNIL's decision may draw parallels to a common US privacy concept: the reasonable expectation of privacy. In the well-known decision Katz v. United States, 389 U.S. 347 (1967), a two-prong test was developed to assess whether the individual's rights under the Fourth Amendment were infringed. The test looked at whether the individual's subjective expectation of privacy was violated and whether this expectation of privacy was reasonable. CNIL declares that the fact that an individual making their photo public, does not override their reasonable expectation that this photo is not going to be used by a company to create a biometric profile on them.

In fact, CNIL's decision is aligned with a recent report of an individual who filed a complaint with his local data protection authority in Germany against Clearview AI. Matthias Marx reported that he filed this complaint as he found out that his face was mapped and monetized by three companies.[66] According to the article, Marx states that he read about Clearview AI which reported that it scraped billions of photos from the internet to create a huge database of faces in 2020. With Clearview's facial recognition technology, law enforcement agencies can find other online photos of the same face by uploading a single photo.[67] He emailed Clearview to see if the company had any photos of his face. In response, Marx received two screenshots from a Google engineering competition that he attended around a decade ago. He reports that he knew that the pictures existed, but he didn't know that a photographer was selling them without his permission on stock photo site Alamy.[68]

As the CNIL decision focused on posting a photo public does not mean that the user should expect that it will be processed by a large software company serving law enforcement's needs, Marx's story shows evidence that it might even be the case that these images might also be used by other third parties for commercial profit. In accordance with Recital 47 of the GDPR, when data subjects do not reasonably expect their personal information will be processed, it is likely that the interests and fundamental rights of the data subject will prevail over the interests of the

[66] Morgan Meaker, 'Clearview Stole My Face and the EU Can't Do Anything About It' [2022] *Wired* <https://www.wired.com/story/clearview-face-search-engine-gdpr/> accessed 19 December 2022.
[67] ibid.
[68] ibid.

controller.[69] What adds more to the discussion on Clearview AI, is the company's reported mission being assisting law enforcement agencies. Recently, it was reported that in the US the company is also considering authorizing access to its product to public defenders.[70] The news article states that a lawyer benefited from the facial recognition software to prove his innocence in a vehicular homicide case. Although the software was not allowing access to lawyers, the company's CEO reported this was a one-off case where they asked the lawyer to make the use of their software public if their search resulted in proving the innocence.[71]

The CNIL decision was taken under the GDPR which has been designed by the EU as a regulation with exterritoriality. However it can be quite difficult to operationalize extraterritoriality given the limitations of national jurisdictions and international enforcement. As reported by Meaker, at the time of the article was written in November 2022, Clearview has not deleted the photographs belonging to EU data subjects and it was stated that the fines by the Italian and Greek data protection authorities were not paid and the French data protection authority did not disclose whether the fine was paid.[72] This might show the importance of the potential benefits of further transatlantic alignment via the EU-US common roadmap for assessing AI risks and interoperable approaches to manage these risks as covered in Section 2.4.

[69] '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)' (n 64).
[70] Kashmir Hill, 'Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands' *The New York Times* (18 September 2022) <https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html> accessed 19 December 2022.
[71] ibid.
[72] Meaker (n 66).

3.2. Case law examples: United States

The selected US cases cover a range of subjects, including algorithms assisting judicial decisions, computerized rules to process personal injury protection claims, automated recommender systems in social network leading to harmful content, AI's eligibility to obtain patent rights, use of facial recognition technology during exam sessions, use of digital fraud detection systems for insurance sector, and discriminatory social media algorithms.

3.2.1. Flores v. Stanford (9/28/2021)

This case concerned an application made by Northpointe Inc. to prevent the disclosure of materials produced by Northpointe to one of the Plaintiff's experts, Dr. Rubin. Ultimately, Northpointe's request was denied and the Compelled Materials were ordered to be released under a supplemental protective order. The court ruled that the Compelled Materials were relevant to the Plaintiff's constitutional claims, had little risk of competitive injury and an elevated risk of prejudice to Plaintiffs if not admitted.

This particular decision stemmed from a previous court order, dated February 12, 2021 which ordered Northpointe to produce for Plaintiffs a variety of proprietary information on the topic of Northpointe's Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool. More specifically, COMPAS is a

secret algorithm that was used by the defendants (more broadly the New York State Board of Parole) to decide whether to grant offenders that were sentenced to life in prison discretionary parole. In the former dispute, the Plaintiffs contended that the Defendants' use of an algorithm, which they did not fully understand, took away the individualized parole assessment that juvenile offenders sentenced to life are entitled to under the 8th and 14th amendments.

In the previous decision, the Court ordered that Northpointe release a variety of proprietary data on the operation of their algorithm to the Plaintiffs. However, in order to respect Northpointe's concern that the Compelled Materials contained trade secrets and other proprietary info, the Court mandated that the Compelled Materials be released under a protective order. Although Northpointe and the Plaintiffs entered into a Second Supplemental Stipulation of Confidentiality and Proposed Protective Order on February 26, 2021, Northpointe would not agree to permitting Dr. Rudin, one of the Plaintiff's expert witnesses, access to the Compelled Materials. Northpointe contended that the Compelled Materials contain highly proprietary information and that releasing this information to Dr. Rudin, a highly outspoken critic of Northpointe, would jeopardize Northpointe's existence. Northpointe has argued that in order to prevent competitive injury to Northpointe, the Court should a) not allow the Compelled Materials to be disclosed to Dr. Rudin and b) delay any ruling relating to such a disclosure until certification of the putative class. The Plaintiffs have responded by arguing that releasing the Compelled Materials to Dr. Rudin is necessary to prosecute their case effectively. Moreover they claim that a risk of

competitive injury does not exist because Dr. Rudin has not worked for a competitor nor intends to in the future. Dr. Rudin, they note, has also agreed to be bound by the existing Protective Orders. Finally, the Plaintiff's claim that the alternative request would delay litigation unnecessarily.

In adjudicating the case, the Court noted that they treat Northpointe's request as a motion for a protective order. According to Rule 26(c) of the Federal Rule of Civil Procedure, a protective order can be issued so that trade secrets or other confidential research not be revealed or only be revealed in a specific way. Ultimately, the party that seeks a protective order has to establish that a good cause for the order exists[73] and the establishment of this cause often exists when the party can demonstrate a clearly defined, specific and serious injury.[74] The Court noted as well that there is no absolute privilege against disclosing trade secrets.[75] In such matters, the court must balance the relevance of commercially sensitive materials to a party's claim (in this case having its chosen expert review the materials) against the interest of the opposing party in maintaining trade secrets.[76] The relevant issues that figure in this consideration are: (1) whether the person receiving the confidential information is involved in competitive decision-making relating to subject of the materials, (2) whether there is a risk of inadvertent disclosure of the information, (3) the hardship

[73] Duling v. Gristede's Operating Corp., 266 F.R.D. 66, 71 (S.D.N.Y. 2010)
[74] re. Terrorist Attacks on Sept. 11, 2011, 454 F. Supp. 2d 220, 222 (S.D.N.Y, 2006)
[75] Federal Open Mkt. Comm. of Fed. Reserve Sys. v. Merrill, 443 U.S. 340, 362, 99 S. Ct. 2800, 61 L. Ed. 2d 587 (1987)
[76] Grand River Enters. Six Nations, Ltd v. King, No. 02 Civ. 5068 (JFK), 2009 U.S. Dist LEXIS 11504, 2009 WL 222160, at *5 (S.D.N.Y Jan. 30, 2009 also Uniroyal Chem. Co. Inc. v. Syngenta Crop prot., 224 F.R.D 53, 57 (D. Conn. 2004)

imposed by the restriction, (4) the time of the remedy and (5) the scope of the remedy.[77]

The Court ruled that the disclosure of the Compelled Materials were relevant, posed little risk of competitive injury and would prevent prejudice against the Plaintiff. First, the Defendants claimed that the Compelled Materials were irrelevant to the issue of class certification and only minimally relevant to the lawsuit in its entirety, because only one of the named Plaintiffs was denied parole as a result of a high COMPAS risk score. The Plaintiffs conversely contended that the Compelled Materials were highly relevant to class certification and merits as they showed how the algorithm factors youth into its risk scores across the proposed class and for the Individual Plaintiff. The Court contend that the class issue does in factor overlap quite significantly with merits discovery[78] and held the issue to be relevant given that Courts are typically unwilling to separate class-related discovery from discovery of the merits.[79] Moreover, the Court said that the Compelled Materials were highly relevant to the Plaintiff's constitutional claims. The Plaintiff's in their previous motions contended that COMPAS treats youth as an aggravating factor in their model, which fails to account for juvenile rehabilitative capabilities and ultimately violates the right to individualized parole assessment implied in the 8th and 14th amendments. Northpointe has suggested that age is a datapoint, but has failed to reveal how significantly the algorithm weights age. Therefore, the Court ruled that more information was needed to understand how the algorithm weights age of offense. In

[77] (Uniroyal Chem. Corp., 224 F.R.D at 57)
[78] Bodner v. Paribas, 202 F.R.D. 370, 373 (E.D.N.Y. 2000)
[79] Chen-Oster v. Goldman, Sachs & Co., 285 F.R.D. 294, 299 (S.D.N.Y. 2012)

addition, this information needs to be adjudicated by an expert witness like Dr. Rudin, a witness that would understand how the algorithm operates. The Court finds the materials to be relevant and contends that any further delay of discovery would be wasteful and duplicative, so it denies Northpointe's request to consider the issue only after a class certification.

Second, the Court, while sensitive to Northpointe's concern about the dissemination of trade secrets, feels the risk of intentional or inadvertent disclosure of this information to competitors is low. The Court reasoned that the Protective Orders already in place prevent the disclosure of the Compelled Materials except for individuals involved in issues relating to the litigation of the case. Moreover, Dr. Rudin has agreed to be bound by the Orders, has promised to take further measures to prevent inadvertent disclosure and has a history of lawfully dealing with confidential information in the past. Moreover, the Court contended that it is imprudent to assume that parties will violate their protective order obligations.[80] The potential to injure Northpointe does exist, but it involves issues of money and can be dealt with money or injunction damages.[81] Finally, there is a history of other courts permitting disclosure of sensitive commercial information to an expert on the grounds that this expert is bound to a protection order.[82] The Defendants have made claims that the strong negative opinion that Dr. Rudin holds of Northpointe are so pervasive, that no level of protection could prevent injury to Northpointe if she is given access to the

[80] CSL Silicones Inc. v. Midsun Grp. Inc., 3:14-CV-01897 (CSH), 2016 U.S. Dist. LEXIS 82923, 2016 WL 3568173, at *5 (D. Conn. June 27, 2016)
[81] n re The City of New York, 607 F.3d at 936; see also CSL Silicones Inc., 2016 U.S. Dist. LEXIS 82923, 2016 WL 3568173, at *5
[82] CSL Silicones Inc., 2016 U.S. Dist. LEXIS 82923, 2016 WL 3568173, at *4-5.

Compelled Materials. The Court ruled these justifications to be insufficient grounds for preventing release of the information. There is no evidence that Dr. Rubin dislikes COMPAS for reasons tied to business competition. Dr. Rubin criticizes COMPAS because its workings are private while it is used by government agencies. Moreover, Dr. Rubin has no control over the competitor's decision to use one algorithm over another because Dr. Rudin has never been involved with a Northpointe competitor and does not intend to work for one in the future.[83] The Court feels as well that Dr. Rudin's work poses limited risk of inadvertent disclosure. However the Court is sensitive to the fact that Dr. Rudin has formerly been publicly critical of Northpointe and would caution her not to disclose the content contained in the Compelled Materials beyond the scope of the litigation. In order to further safeguard the information, the Court directs the parties and Northpointe to propose an additional protective order governing disclosure of the Compelled Materials to Dr. Rudin.

Third, the Court contends that there is a risk of prejudice to the Plaintiff's if Dr. Rudin is unable to testify. Dr. Rudin is highly qualified in the field of machine learning and has unique experience of understanding how machine learning technologies interact with social problems. Her unique skillset is essential in this case, because this particular case requires a thorough analysis of the workings of the algorithm and how these workings relate to protections guaranteed by the Constitution. The Court feels that it is not clear that other experts possess the same degree of expertise. Moreover, the Court holds that it would be prejudicial to further prevent Dr. Rudin

[83] Santella, 2012 U.S. Dist. LEXIS 158349, 2012 WL 5399970, at *5-6

from reviewing the Compelled materials. At present, Dr. Rudin lacks information necessary for her to make the assessment on COMPAS that she requires. The information that is being withheld is highly relevant to the assessment Dr. Rubin needs to deliver. The case has been pending since 2018 and requiring the Plaintiff's to find an additional expert and bring them up to speed on the litigation would unnecessarily delay the proceedings.

This case seemed relevant for inclusion because it illustrates a tension between algorithm deploying companies that aim to maintain their trade secrets and opposing parties that want more clarity on how algorithms operate. It is highly likely that these kinds of tensions will increase in the near future as artificial intelligence systems improve in their capability and are more and more likely to be deployed in the real world. Companies that use these systems will desire to keep their operation secret for competitive reasons, while individuals that are unfairly affected by these systems will attempt to understand how they operate. This case is illustrative because it paints a picture of the particular legal issues that Courts consider in resolving these tensions. The two most salient issues seem to be the relevance of proprietary information to the issue at hand and the possibility of competitive injury. The decision in this case suggests that should an algorithm make a decision that affects an individual in a particularly unlawful way, it is acceptable that information on the workings of such algorithms be released in a court setting for the resolution of disputes. A more complex question concerns the operation of more complex neural network based algorithms that learn weights that themselves are sometimes not

completely understood by the algorithm developers. These algorithms can sometimes be “black boxes” so the question of how their operation relates to law might be challenging to judge. The second issue on risk of competitive injury, seems to be taken seriously by Courts. The Court acknowledges the right companies have to keep information proprietary but seem to believe that the risk of disclosure can be prevented with Protective Orders. Moreover, there seems to be a ground to prevent the release of information to parties involved in litigation that could be in competition with the opposing parties.

3.2.2. Yvonne Green, WPRC, and RA, P.A. v. GEICO (3/24/21)

This case was a class action lawsuit in which Yvonne Green from the Wilmington Pain & Rehabilitation Center (WPRC) and Rehabilitation Associates (RA) sued Geico General Insurance Company (GEICO). The plaintiffs alleged that GEICO's use of two computerized rules, the Geographic Reduction Rule (GRR) and the Passive Modality Rule (PMR) in their assessment of insurance claims was improper. Moreover, they claim that in using such rules GEICO was unable to properly evaluate facts that were unique to each insurance claim. The plaintiffs advanced three charges: first, a breach of contract, second a bad faith breach of contract and third, a declaratory judgment. Both parties also submitted motions of summary judgment: the core issue in the cross-motions for summary judgment was whether GEICO’s use of computerized rules to process personal injury protection claims violated their contract and

Delaware Law. Ultimately, the Court denied the plaintiffs motions on the first and second counts, but granted them on the third.

Before diving into the specifics of the jurisprudence, it is necessary to consider how GEICO's computerized rules actually worked. The first, the Geographic Reduction Rule (GRR), was a computer rule that would limit the full payment of claims based on an 80th percentile cap. GEICO had a database where it sorted all its claims from the lowest to highest. The amount that was the 80th percentile is the maximum amount that GEICO would pay for any particular CPT code (a universal code that is assigned to each treatment procedure). The Passive Modality rule was used to assess claims for passive modality treatments that are issued more than eight weeks after an accident. If a claim is filed for a passive modality treatment that occurs eight weeks after an accident, the PMR issued a recommendation that had the effect of denying the claim without human review. Both of these rules were not disclosed in GEICO's policies however they were disclosed in various portions of GEICO's Message Modifier code. When GEICO processed its PIP claims it would use both of these computerized rules and then make a decision whether to pay, limit or deny the claims. The claims that GEICO processed with the use of such rules were ultimately not reviewed by humans.

The amended complaint filed by the plaintiffs contained four specific counts. The first was that GEICO breached its own policies. The plaintiffs asserted that GEICO has a contractual duty to its assignees and insureds under its own policies to provide personal injury protection (PIP). The first count further held that GEICO breached its

policy by using the computerized rules to limit or deny PIP benefit claims. The second count was that GEICO committed a bad faith breach of Section 2188(d) of the Delaware Code and is therefore responsible for covering the fees associated with the litigatory actions. The plaintiffs argued that because of the use of computerized rules, the PIP benefits that were owed to them were not paid within 30 days. The third count aims to have the court issue a declaratory judgment that GEICO's deployment of the computerized rules is unlawful and in violation of Section 2118. This argument held that Delaware law required that GEICO pay covered PIP benefits, and that GEICO violated those laws by using the computerized rules to determine the amount and possibility of receiving PIP benefits. The fourth and final count contended that GEICO participated in deceptive and unfair practices. GEICO did not disclose its use of the computerized rules and did not perform a thorough investigation of PIP benefit claims: therefore the Plaintiffs held, GEICO violated 6 Del. C. §2532(a)(5) and (12).

GEICO countered with several responses. First and most fundamentally, they argued that their own policies only obligated them to pay reasonable expenses for necessary treatment. GEICO asserted that they were not contractually prevented from using any particular approach in assessing the payments. Second, GEICO challenged some of the factual inferences raised by the plaintiffs but claims that none of the facts in question hinder the Court from granting relief as the case purely concerns legal issues.

The Court began approaching these questions by first, establishing the standard through which motions for summary are reviewed. They noted that this standard is well-settled: the court must study the record in order to judge whether legitimate issues of material fact exist. However the Court does not need to decide the issues. The Court will review the record in a way that is most favorable to the nonmoving party and should no genuine issues of material fact exist, then a summary judgment will be granted. Conversely, if the factual record is not developed enough for the Court to apply the law to the record or if the record suggests that the facts are in dispute, then the summary judgment will not be granted.

Concerning the first question of breach of contract, the Court issued a summary judgment in favor of GEICO. The Court began by noting that there are three requirements for proving a breach of contract: (1) existence of a contract, (2) breach of the contract's imposed obligations and (3) claim of damages suffered by virtue of the breach. At issue here was the question of whether GEICO had an obligation under either contract, common law, statutory law or Delaware law to investigate the PIP claims in a specific fashion and whether this duty was breached by GEICO. Next the Court rejected the Plaintiffs' claim that the Delaware Unfair Trade Practices Act (UTPA) (18 Del. C. § 2304) implies a breach of contract. Although this law stipulates that the Delaware Commissioner of Insurance can "deal with unfair trade practices within the insurance industry," there is nothing explicitly cited in the GEICO policies that obligates it to use a particular method in PIP claim assessment. The only obligation GEICO had was to pay reasonable medical expenses.

The Court also agrees with GEICO's assertion that there is no common law duty to investigate. More specifically, the Court cites *Mt. Hawley Ins. Co. v. Jenny Craig, Inc.* as prior jurisprudence that demonstrates the absence of a common law duty to investigate. The Court also asserts that the use of the computerized rules is consistent with the Delaware Insurance Regulation 603. Concerning PIP, those regulations stipulate that "any insurer, in accordance with fillings made with the Insurance Department, may provide for certain deductibles, waiting periods, sublimits, percentage reductions, excess provisions or similar reductions…the owner's election of any reduced benefits described must be made in writing and signed by the owner." While the Court does agree that GEICO never openly disclosed the use of the rules, these rules were functionally incorporated into their policies under GEICO's interpretation of reasonableness. The Court also agrees with the plaintiffs' claim that these rules operate like sublimits; however, crucially notes that these rules are not applied to all GEICO policyholders. For example, the GRR only applies to claimants that live within certain geographies. Therefore, the contention that there is a breach of contract theory under Delaware Insurance Regulation 603 fails. Similarly, the plaintiffs have not sufficiently shown that there is a breach due to non-disclosure rather than application.

The Court concludes its analysis on the breach of contract issue by noting that it would be prepared to grant summary judgment to the plaintiffs' on Count II, were it not for a previous Supreme Court ruling, notably *State Farm Mutual Automobile Insurance Company v. Spine Care Delaware, LLC*. The Court does agree with the

plaintiffs that under GEICO policies as well as sections 2118 and 2118B of Delaware law, GEICO is obligated to process PIP claims within 30 days and pay all reasonable and necessary claims. Moreover, it holds that GEICO's use of the computerized rules failed to determine the reasonableness of the claims, at least in terms of their accordance with the law. Given that GEICO has no other review mechanism, failure to pay as a result of the usage of rules would constitute a contractual breach. However, in the aforementioned case, *State Farm v. Spine Care*, the Supreme Court ruled that a breach of contract claim under Section 2118B(d) cannot be pursued without a factual presentation on behalf of the plaintiffs' that their claims were reasonable and necessary. The State Farm case likewise involved an insurance provider, State Farm, using a computerized rule to assess insurance claims. In their ruling, the Supreme Court held that PIP claimants have the initial responsibility of showing that their claims are reasonable and necessary. Because in this particular case concerning GEICO, the Plaintiffs did not opt for an individualized claim approach, the Court cannot rule on the reasonableness of their claims and therefore, cannot enter summary judgment on the first count in their favor.

The Court likewise denies summary judgment for the second count, bad faith breach of contract. In order to prove a bad faith contractual breach, the plaintiffs must demonstrate that the insurer did not have "reasonable justification" to deny coverage for the insured. The Court holds that the plaintiffs have not sufficiently shown that GEICO's usage of the computerized rules was without any reasonable justification.

However, the Court does issue declaratory relief on count III, and asserts that GEICO's usage of the computer rules is in violation of Section 2118B(c) and 2118(a)(2). The Court begins its argument regarding the appropriateness of issuing declaratory relief by noting that in previous cases, most notably the State Farm v. Spine Care case in front of the Supreme Court, it was ruled that State Farm's use of computerized rules in assessing insurance claims violated 21 Del. C. § 2118(a)(2) and would warrant the issuance of relief. Second, the Court agrees with the plaintiffs that section 2118B(c) has been violated because this section requires that GEICO process claims. Assuming that the word process takes the meaning that is invoked by the statute, process necessitates a full investigation of all available information. However, in deploying a computerized rule whose underlying justification was arbitrary and inflexible, GEICO failed to take into account the full slate of information that underlay the insurance claims. Regarding the GRR, GEICO contended that the 80th percentile was industry standard but the Court ruled that it does not sufficiently justify why this particular level is a justifiable standard. GEICO cites peer reviewed medical literature to validate the standard but in previous rulings such as *Lundberg v. State Farm Mut. Ins. Co.,* the Court of Common Pleas held that insurance companies cannot reject claims as unnecessary by merely relying on medical journal articles. Moreover, in testimony, a GEICO representative admitted that passive modalities may in fact be appropriate after 8 weeks which challenges the logic of GEICO's PMR which prohibits the coverage of modalities after an 8 week period. In sum, the Court finds that GEICO has not sufficiently shown their rules to be reasonable.

In terms of what in fact constitutes a reasonable medical expense, the Court follows the lead of the Supreme Court which has reaffirmed the application of the *Anticaglia and Watson* standards.[84] The Court ultimately agrees with the plaintiffs that there is no factual record that GEICO employs analysis that relies on these factors in assessing the reasonableness of PIP claims: GEICO merely applies the computerized rules. In its defense, GEICO cites *St. Louis Park Chiropractic, P.A. V. Federal Ins. Co.* as a case where it was ruled that a computerized auditing system is not in violation of insurance laws. The Court dismisses this argument as it finds that the case over which it is presently ruling occurs in Delaware and Delaware law necessitates that all information be assessed before a claim is considered. However in this instance, GEICO's use of automated computer rules which did not process all available information violated the aforementioned requirement. The Court noted that using automated systems per se does not directly violate Delaware law, however using systems that fail to consider all necessary information does violate. Should insurance providers desire to use automated systems to make the processing of claims more efficient, they must do so in a manner that accounts for all the Anticaglia and Watson factors.

GEICO further raises twelve issues of disputed facts but the Court notes that such issues are immaterial or flawed, given that there is no way to factually disagree with

[84] These standards in full are: ordinary and reasonable charges usually made by members of the same profession of similar standing, nature and difficulty of case, time devoted to it, amount of services rendered, number of visits, inconvenience and expense to which the physician was subjected, size of the city or town where services were rendered, physician's education and training, physician's experience, skill or capacity, physician's professional standing or reputation, extent of the physician's business or practice and ability of the defendant to pay.

the fact that GEICO uses the computerized rules and engages in no further investigation of claims. The majority of these issues are unrelated to technical questions surrounding the jurisprudence of artificial intelligence, so a more detailed analysis of their specifics will not be considered in this paper.

This particular legal case is interesting because it highlights the consideration courts might weigh in adjudicating the appropriateness of automated-based insurance systems or automated based systems in general. Particularly, the jurisprudence in this case suggests that while courts are willing to take guidance from outside sources on the appropriateness of rules, their decisions will ultimately be based on written law. For example, the Court acknowledged that it considered the perspective of law professors such as Danielle Citron that have argued that insurance decisions are best addressed by non-automated systems[85], as well as arguments that automated systems have the potential to eliminate persistent and pernicious errors in the administration of insurance claims. However, the Court, acknowledging that there is no "per se rule on whether automated rules can be employed in handling insurance claims," noted in the end that "Delaware law, not law review articles, will govern the resolution of…claims." Ultimately as AI technologies become more ubiquitous, it is likely that administrative responsibilities once handled by humans will be delegated to computers. In such a world, it would seem to be prudent for policymakers to consider the institution of new laws that impose more precise standards on when, where and how such computerized systems can be used.

[85] Danielle Keats Citron, 'Technological Due Process' (2007) 85 Washington University Law Review 1249.

In the absence of new legislation, it is also interesting to consider what current legal provisions permit in terms of the usage of computerized rules. This case only offers a perspective regarding Delaware law, and the jurisprudence seems to claim that the adjudication of medical expenses must be reasonable which implies that it must consider the Anticaglia and Watson factors. In this case, the computerized rules considered none of those factors. However with current advances in AI, it is not inconceivable to imagine that many of these factors could theoretically be imputed into a computerized system such as a physician's education and training, or number of visits. Some of these factors are more challenging to quantify and perhaps more open to subjective interpretation such as the physician's professional standing or reputation, or the inconvenience and expense to which the physician was subjected. If these factors are one day included in computerized models that adjudicate insurance claims, it will be interesting to see how courts and legal scholars judge the degree to which their quantification is in fact reasonable. Moreover, if more complex AI systems could be built that consider all such factors, at what point do their decisions become more reasonable than the ones issued by humans? In this case, the Court takes issue with GEICO's computerized rules largely because of their inflexibility: human review is preferable to the use of the rules because such reviews permits a more flexible consideration of claims. If however, computerized systems can be built to be more flexible and are able to consistently deliver reasonable insurance outcomes, should their use therefore be preferred? Presently it appears that using computerized rules without some kind of human oversight, is sufficient to support the legal challenge that insurance claims were not reasonably assessed.

GEICO ultimately deployed no human oversight, so the question of reasonableness was not a difficult one for the Court to assess: a more plausibly complex issue would be if GEICO had deployed some degree of human oversight. In that case, exactly how much oversight would be appropriate. All of these aforementioned questions are not ones the Court was asked to currently consider, but ones that possibly loom on the horizon.

3.2.3. Dyroff v. Ultimate Software Grp., Inc. (11/26/17)

This case pits the plaintiff Kristanalea Dyroff against the defendant Ultimate Software. The plaintiff sued Ultimate Software after her adult son Wesley Greer, died from an overdose of fentanyl-laced heroin bought from a drug dealer that he had met through Ultimate Software's now discontinued social-networking website, Experience Project.

The plaintiff advanced seven charges: (1) negligence, (2) wrongful death, (3) premise liability, (4) failure to warn, (5) civil conspiracy, (6) unjust enrichment and (7) violation of the Drug Dealer Liability Act. The crux of the plaintiff's claim is that Ultimate Software is responsible because it mines data from its users' activity on Experience Project, deploys algorithms to glean insights from the posts and uses those insights to make actionable recommendations for users, which in this case channeled her son towards the heroin-related discussion groups that enabled the purchase of tainted drugs. Ultimate Software removed the action from state court citing diversity jurisdiction and petitioned to dismiss all claims under Federal Rule of Civil Procedure

12(b)6. Moreover, for all claims advanced by the plaintiff, with the exception of the fourth, Ultimate Software asserted immunity under the Communications Decency Act, 47 U.S.C. § 230(c)(1). This section of the act allows websites to have immunity for third-party content on their platforms unless they are wholly or partially responsible for the creation and development of such content. The plaintiff responded to Ultimate Software's immunity claim by contending that websites need not co-author posts to technically develop content. More specifically, she asserted that content creation can mean materially manipulating such content, for example guiding the content's generation or generating novel insights from data and using such insights to guide and signal users. The Court ruled that the defendants did in fact have immunity for all claims with the exception of the fourth under the CDA given that they did not develop the content that led the plaintiff's son to purchase the drug. The Court likewise held that the website is unlike a brick and mortar business that has a duty to warn, and therefore was not obligated to warn Mr. Geer of fentanyl laced drugs.

To begin, it is useful to consider some background on how Ultimate Software's Experience Project website actually worked. On this particular social media platform, users could register with anonymous user names and join or start groups related to their interest, such as dogs or drugs. Ultimate Software then deployed advanced data-mining algorithms in order to analyze their users' posts and activity. Such information was further used for two purposes: first, it was commercially sold to third parties and second, it was fed into recommendation engines which then directed users to other relevant groups of interests. Finally, Experience Project also deployed

emails and other notifications to notify users of activity in some of the groups that they had belonged to.

As such, the first and most essential question that the court faced was whether Ultimate Software was in fact eligible for immunity. The Court ended up ruling that Ultimate Software was immune because its tools were content neutral: they facilitated communication but did not in and of themselves represent novel content. In reaching its decision, the Court cited jurisprudence in Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1167-69 (9th Cir. 2008). In this case, Roommates.com asserted immunity against claims that it had violated the federal Fair Housing Act and California housing-discrimination laws. In that case, it was ruled that Roomates.com did not qualify for immunity. Roomates.com, by requiring that its users provide information in the form of a limited set of pre-populated answers, became, in part, a developer of content or information. Conversely Roomates.com had immunity for content that its users voluntarily displayed in a section where users were asked to: “personalize [their] profiles by writing a paragraph or two describing yourself and what you are looking for in a roommate.” For this section, Roomates.com did not guide users to submit particular answers nor did it facilitate the addition of discriminatory preferences. With this decision in mind, the Court ruled that the mere provision of content-neutral tools is sufficient for the granting of immunity: Ultimate Software did not use unlawful criteria to limit the scope of search, it did not tailor its platform to specifically achieve illegal ends and it did not directly develop any kinds of unlawful searches. Moreover

in the end it was Ultimate Software's users and their voluntary inputs that created the content on the platform, not the algorithms. The mere provision of a framework of communication that could then be misappropriated is not sufficient for demonstrating liability.[86] The Court therefore granted Ultimate Software immunity for all of the Plaintiff's charges except for the fourth, on duty to warn.

Next the Court addressed the validity of the fourth claim: did Ultimate Software have a duty to warn its users of criminal activity that occurred on its platform? The plaintiff contended that Ultimate Software had a duty to inform her son that there was a criminal selling fentanyl-laced heroin on its platform. In the eyes of the plaintiff, this duty stemmed from the fact that Ultimate Software is like any brick and mortar business that has a special relationship with its clients and thereby an obligation to inform them of associated risks. More specifically, the plaintiff articulated that website operators are like "restaurants, bars…amusement parks and all businesses open to the public" and have the same duty that all businesses open to the public have to their invitees. Moreover this duty, the plaintiff noted, involves taking affirmative action to control the wrongful act of various third parties which could plausibly threaten invitees, in cases where the occupants have reasonable cause to anticipate such acts and the injury that might result from them. Ultimate Software in turn contended that websites have no duty to warn their users of the criminal activity of other users and that the plaintiff's son should have assumed the obvious risk of purchasing drugs from an anonymous Internet drug dealer.

[86] Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1195 (N.D. Cal. 2009

On this question, the Court began by acknowledging that the California Supreme Court has not yet answered the question of whether or not websites have special relationships with their users and whether this relationship creates a duty to warn. Next the Court observed that a duty to warn can arise from the special relationship that businesses have with their customers or from the creation of their own risk.[87] California law likewise stipulates that if a person has not created a danger then they typically have no responsibility to come to the aid of another individual, unless there is a relationship that requires a duty to protect.[88] The special relationship that gives rise to a duty to protect comes from the distinction that the common law draws between nonfeasance, a failure to act and misfeasance, a defendant being responsible for actively making the plaintiff's position worse, by for example, creating risk. The Court disqualified the possibility of an obligation to warn arising from misfeasance creating risk, contending that Ultimate Software used neutral tools and functionalities which did not create a risk of harm that imposed some kind of ordinary duty of care. Next, the Court ruled that Ultimate Software could be liable for nonfeasance under two conditions: (1) it had some kind of special relationship with a third party actor and therefore held a duty to control this actor or (2) had a special relationship with the defendant and therefore had a duty to protect him. Citing previous jurisprudence, the Court noted that special-relationship doctrines have typically been invoked in "cases involving the relationship between business proprietors such as [landlords], shopping centers, restaurants and bars and their

[87] McGarry v. Sax, 158 Cal. App. 4th 983, 995, 70 Cal. Rptr. 3d 519 (2008

[88] Zelig v. County of Los Angeles, 27 Cal. 4th 1112, 119 Cal. Rptr. 2d 709, 45 P.3d 1171, 1182 (Cal. 2002)

tenants, patrons or invitees."[89] More recently however, the deployment of special relationships to justify duty has been eclipsed by the more modern balancing policy factors listed in Rowland v. Christian.[90] [91] The Court deferred to two recent cases, both of which concluded that websites do not have special relationships with users that require them to warn the users of known risks on their websites.[92]

However the Court took a further step and elucidated its own reasons why social-network websites are not liable. First, the imposition of a duty would impose an ineffective general warning to all users.[93] Second, it would have a chilling effect on the Internet by opening the possibility of further litigation.[94] Third, the contention that brick and mortar businesses like bars are similar to social-networking websites is not persuasive. The allocation of risk partially depends on the degree to which harm is foreseeable and the court contended that risk can be substantially more apparent in the real world than the virtual social-network world. Moreover, even if Ultimate Software possessed superior knowledge of the sale of fentanyl-laced heroin, the possession of such knowledge only creates a special relationship if there is dependency or detrimental reliance by users.[95] The Court therefore rejected the

[89] McGarry, 158 Cal. App. 4th at 995.
[90] Rowland v. Christian, 69 Cal. 2d 108, 70 Cal. Rptr. 97, 443 P.2d 561, 564 (Cal. 1968))
[91] The Rowland factors in greater length, are: (1) foreseeability of harm to the plaintiff, (2) degree of certainty that the plaintiff suffered injury, (3) closeness of the connection between the defendant's conduct and injury suffered, (4) moral blame attached to the defendant's conduct, (5) policy of preventing future harm, (6) extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach and the availability, cost and prevalence of insurance for the risk involved.
[92] Jane Doe No. 14 v. Internet Brands, Inc., No. 2:12-CV-3626-JFW (PJW), 2016 U.S. Dist. LEXIS 192144, ECF No. 51 (C.D. Cal. Nov. 14, 2016) and Beckman v. Match.com, LLC, No. 2:13-CV-97 JCM (NJK), 2017 U.S. Dist. LEXIS 35562, 2017 WL 1304288, at *4 (D. Nev. Mar. 10, 2017).
[93] Internet Brands, No. 2:12-cv-3626-JFW (PJW), 2016 U.S. Dist. LEXIS 192144, ECF No. 51 at 6.
[94] 2016 U.S. Dist. LEXIS 192144 at *14
[95] Internet Brands, No. 2:12-cv-3626-JFW (PJW), 2016 U.S. Dist. LEXIS 192144, ECF No. 51 at 6.

plaintiff's argument that Ultimate Software should be liable because it owed a duty to her son.

This particular case was elected for inclusion as it concerns litigation around an issue that is only likely to continue increasing in salience: social media platforms using AI-informed tools to facilitate behavior that can be potentially harmful for their users. This Court's decision suggests that for a plethora of charges such social media platforms are eligible for immunity, unless they create and develop information or content that then facilitates harmful behavior. Naturally, the question then becomes what actually constitutes the creation of content and in this case the Court ruled that mining insights from algorithms and then using those insights to steer users does not necessarily constitute information creation. Conversely, framing the creation of content in a way that for instance requires the submission of unlawful answers and steers users based on that information, as Roomates.com did, constitutes content creation. There seems to be well-established jurisprudence that argues that providing neutral tools for navigating websites is fully protected by CDA immunity, unless the website creators use such tools for unlawful purposes. For example, in Gonzalez, 2017 U.S. Dist. LEXIS 175327, 2017 WL 4773366, at *11 the Court rejected the claim that Google was liable because YouTube's website supposedly aided ISIS's communication of its message. In Cohen v. Facebook, Inc., 252 F. Supp. 3d 140, 158 (E.D.N.Y. May 18, 2017) the Court likewise rejected the argument that Facebook should be liable for providing a tool to support terrorist organizations. Moreover, in Fields, 217 F. Supp. 3d at 1120-23 courts rejected the claim that Twitter provided

material support to ISIS by allowing its members to sign up for accounts. While jurisprudence in this domain seems to be well-established, this question might plausibly become more thorny in the future with the rise of generative AI that creates content like text, photos and videos. If such content is deployed on social media platforms and leads to situations of harm, when does it become no longer neutral? This case hints at how Courts might think about this question.

Moreover the Court ruled fairly decisively that Ultimate Software had no duty to warn its users of potential danger because it owed no special obligation to that user. The Court drew a distinction between brick and mortar businesses which it argued possessed such a duty. One of the motivating factors in this distinction was that such businesses could more accurately foresee risks, than social media websites. One could imagine that as AI becomes increasingly advanced and websites continue mining more information from users, they may in fact be able to quite accurately foresee user risks. Disregarding arguments concerning ineffective warning and chilling effects, if such platforms become more advanced in their assessment of risk, do they then possess some kind of duty to warn? Moreover, if an increasingly larger portion of activity is conducted on such social media platforms which carry with them the potential of user harm, should lawmakers perhaps not start thinking about ways in which conceptions of duty of harm ought to be reconceptualized?

3.2.4. Thaler v. Hirschfeld (9/2/21)

This case concerned the question of whether an AI machine could be an inventor under the Patent Act. Ultimately the Court ruled that under the plain statutory language of the Patent Act and Federal Circuit Act, AI-generated inventions cannot be patentable. More specifically in this case, Stephen Thaler filed two patent applications with the United States Patent and Trademark Office (USPTO). The patent applications were rejected. Thaler held that the decision of the defendant Andrew Hirshfield and the USPTO was arbitrary, an abuse of discretion, capricious, not in accordance with the law, unsupported by evidence and in excess of the defendant's statutory authority. The plaintiff not only sought for the patents to be reinstated but a declaration that AI-generated patents should stand.

The background of the case is as follows. The plaintiff claimed that he used AI to generate patentable output. He created an AI system called DABUS, which was then listed as the inventor of 350 different applications, for instance Neural Flame, a light beacon that flashes in a new and inventive manner. The plaintiff submitted applications for a plethora of these AI-generated patents. The USPTO then returned a notice to file missing parts of the application because the submitted application sheets did not identify the inventors by their legal names. Later in the year, on August 19th 2019, the plaintiff filed a petition with the USPTO director in which he requested that the USPTO vacate its request for missing parts in the application on the grounds that DABUS, his AI system, was the true inventor. On December 17th, 2019 the

USPTO submitted a written declaration in which it dismissed the plaintiff's petition arguing that the explicit Statutory Language in the congressional patent act designates the term "inventor" as a human individual. The USPTO also cited previous Federal Circuit rulings which twice held that an inventor could only be a natural person.[96] [97] On January 20, 2020 the plaintiff sought reconsideration of the USPTO's decision by filing a further petition, which the USPTO once again denied on April 22, 2020. In this final rejection, the USPTO frequently referenced Title 35 of the US Code which precludes the possibility of the term inventor being interpreted in a way to cover machines. Moreover, the USPTO held that the essence of inventorship is the formation in the mind of an inventor of an idea, which according to current legal standards can only be performed by a natural person.[98] In this decision, the USPTO did acknowledge the policy concerns brought up by the plaintiff but ultimately ruled that "they do not overcome the plain language of the patent laws as passed by Congress and as interpreted by the courts."[99] The plaintiff then filed a civil suit to review the USPTO's most recent decision.

The Court began by first, establishing the standard of review, noting that it can only set aside a final agency decision if it is "arbitrary, capricious, an abuse of discretion or otherwise not in accordance with law."[100] Moreover, a decision is deemed to be arbitrary if the agency "relied on factors which Congress has not intended it to considered, entirely failed to consider an important aspect of the problem, offered an

[96] Univ. of Utah v. Max-Planck-Gesellschaft, 734 F.3d 1315, 1323 (Fed. Cir. 2013)
[97] Beech Aircraft Corp. v. Edo Corp., 990 F.2d 1237, 1248 (Fed. Cir. 1993)
[98] Max-Planck, 734 F.3d at 1323; Beech Aircraft, 990 F.2d at 1248
[99] Glaxo Ops. UK Ltd. v. Quigg, 894 F.2d 392, 399-400 (Fed. Cir. 1990)
[100] 5 U.S.C. § 706(2)(A)

explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise."[101] The Court must also consider "whether the decision was based on a consideration of the relevant factors and whether there has been a clear error of judgment."[102] Ultimately, the clear legal focus of the review should "be the administrative record that is already in existence."[103]

The Court observed that an important prior case to weigh in this issue was the Supreme Court decision in Skidmore v. Swift & Co., where the court ruled that deference should be given to agency interpretations of statutory provisions that "constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance to the extent that those decisions have the power to persuade."[104] The validity of an agency's judgment, the Supreme Court ruled, will further depend on the thoroughness of the evidence it considered and the degree to which the reasoning is valid and consistent with earlier and later pronouncements. In the case at hand, the plaintiff contended that the defendants are not entitled to Skidmore deference because they did not consider alternative interpretations of statutory construction and did not sufficiently show that Congress sought to exclude AI generated inventions from patentability. The Court rejected these arguments because they held that these arguments imposed standards for the Skidmore deference that rise above those outlined by the Supreme Court.

[101] Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43, 103 S. Ct. 2856, 77 L. Ed. 2d 443 (1983).
[102] Burandt v. Dudas, 528 F.3d 1329, 1332 (Fed. Cir. 2008)
[103] SourceAmerica v. United States Dep't of Educ., 368 F. Supp. 3d 974, 986 (E.D. Va. 2019)
[104] 323 U.S. 134, 140, 65 S. Ct. 161, 89 L. Ed. 124 (1944)

More fundamentally the Court held that the USPTO correctly interpreted the Patent Act's language. This contention further undermined the plaintiff's challenge of deference and crucially undermined his contention that AI-generated inventions ought to be patentable. The Court began noting that the question of how the Patent Act's language applies to this case is a question of statutory consideration, and as demonstrated in previous cases that were similar, the "preeminent canon of statutory interpretation requires us to presume that [the] legislature says in a statue what it means and means in a statue what it says there."[105] [106]

In reading the language of the Patent Act, the Court determines that the terms inventor and joint inventor reference an individual or individuals, so the question of whether an AI machine can be an inventor, turns on the meaning of the term individual. The Court held that an individual is understood to mean a natural person. A similar decision was reached when the Supreme Court conducted a statutory construction analysis of how Congress used the term individual in the Torture Victim Protection Act, and found that "the ordinary meaning of the word, fortified by its statutory context referenced a natural person."[107] Moreover, the idea that the ordinary meaning of the word individual is in fact a natural person is fortified by the Oxford English Dictionary which holds that "as a noun, individual ordinarily means a human being, a person." The Patent Act employs the term "individual" as a noun and given that individual ordinarily means [a] human being, a person, it can be presumed that individual is taken to mean a natural person not a machine. The Court also notes

[105] Shoshone Indian Tribe v. United States, 364 F.3d 1339, 1345 (Fed. Cir. 2004)
[106] BedRoc Ltd., LLC v. United States, 541 U.S. 176, 183, 124 S. Ct. 1587, 158 L. Ed. 2d 338 (2004)
[107] Mohamad v. Palestinian Auth., 566 U.S. 449, 453-54, 132 S. Ct. 1702, 182 L. Ed. 2d 720 (2012)

that there are other federal cases which further suggest that inventors can only be natural persons. For example in Max-Planck, the Federal Circuit ruled that "conception is the touchstone of inventorship" and that "to perform this mental act of [conception], inventors must be natural persons and cannot be corporations or sovereigns."[108] In Beech Aircraft, the Federal Circuit contended that corporations "could never have been declared an 'inventor' as [the corporation] was merely a corporate assignee and only natural persons can be 'inventors."[109]

The plaintiff attempted to challenge these assertions by suggesting that even if the statutory and judicial language do refer to inventors as individuals, none of this language has been established in the context of AI-generated inventions. Moreover, the Plaintiff held that there were a plethora of policy considerations that ought to be weighted that might override the literal statutory meaning of the Patent Act. For example, allowing AI systems to qualify for patents could lead to more innovation and would be more true to the moral rights of human inventors (as in, allowing humans to take credit for inventions they have not created ultimately devalues the act of human inventorship). Regarding the first claim, the Court was unconvinced with the plaintiff's argument that the term "inventor" should be more flexibly interpreted given that Congress passed the Patent Act long before AI-generated inventions were a reality. The plaintiff held that had Congress known about this possibility, it would have accounted for it in the Patent Act. The Court ruled that the most recent iteration of the Patent Act was passed in 2011, which defined an inventor as an individual, at a

[108] Max-Planck, 734 F.3d at 1323
[109] Beech Aircraft, 990 F.2d at 1248

time when AI already existed as a concept. Therefore there is strong evidence that Congress limited the scope of inventor to refer to natural persons. For all the reasons enumerated above, the Court denied the plaintiff's motion for Summary Judgement. Regarding the second claim, the Court responded by asserting that policy considerations should not override the plain statutory interpretation of the act, citing a plethora of previous Supreme and Federal Circuit decisions that have argued that policy considerations cannot overcome a statue's plain language and that in the end, questions of policy are for Congress and not the Courts.[110] [111] [112]

This particular legal decision is important as it suggests that presently, AI-generated inventions cannot qualify for patent protection. The decision also makes clear that while there may plausibly be valid policy arguments for AI-generated inventions qualifying for patent protection, such decisions ultimately rest with policymakers and not courts. As noted more explicitly in the decision: "as technology evolves, there may come a time when artificial intelligence reaches a level of sophistication such that it might satisfy accepted meanings of inventorship. But that time has not yet arrived, and if it does, it will be up to Congress to decide how, if at all, it wants to expand the scope of patent law." Naturally a further question to pose is when will this time come and perhaps more appropriately given the stunning advances of AI capabilities, if this time has perhaps not already arrived. The last few years have been especially notable in the AI community for the development of systems like GPT-3, DALL-E and PaLM, models that are capable of generating novel and functional

[110] Fisons PLC v. Quigg, 876 F.2d 99, 101 (Fed. Cir. 1989)
[111] Sandoz Inc. v. Amgen Inc., 137 S. Ct. 1664, 1678, 198 L. Ed. 2d 114 (2017)
[112] Kimble v. Marvel Entm't, LLC, 576 U.S. 446, 463-64, 135 S. Ct. 2401, 192 L. Ed. 2d 463 (2015)

content, such as text or images. It is not inconceivable to imagine that already, these models might be capable of generating certain ideas that could qualify for patent protection. At what point then do policymakers judge that AI-generated inventions should be patentable?

Jurisprudence in the Max Planck case, which likewise held that only natural persons can be inventors, argued that conception is at the heart of inventorship. Moreover, the USPTO noted that it continues to study the impact of AI on patent regulations. The consensus from a recent conference held by the USPTO in January of 2019, suggests that presently AI systems are too narrow to engage in the mental cognition required for innovation.[113] As in, the USPTO noted that as of January 2019, AI systems are only really capable of performing individual tasks in well-defined domains: only when they have more general capabilities, akin to the ones actually possessed by humans, should the discussion of AI-invention patentability be more seriously discussed. However, this conference came at a time when there were really no other beings or systems in existence that were capable of the kind of conception required for invention. As of 2022 that might no longer be the case. When systems like GPT-3 think, are they engaging in the kind of cognition that is sufficient for inventorship? Are such systems even thinking? What does thinking actually mean? These questions were not that relevant in the domain of patent jurisprudence ten, even perhaps three years ago. However, they seem to be relevant now. The jurisprudence in this case at least confirms that as it presently stands, AI-generated

[113] USPTO, 'Public Views on Artificial Intelligence and Intellectual Property Policy' (2020) <https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf> accessed 19 December 2022.

inventions cannot be patentable. Moreover, Congress not courts, must take a leading role if that is to change.

3.2.5. Duerr v. Bradley University (03/10/2022)

This case pits plaintiffs Thomas Duerr and his associates against Bradley University. The plaintiffs are suing Bradley University, which is a private university in Illinois, for its use of a third-party protecting tool that they contend was in violation of the Illinois Biometric Information Privacy Act ("BIPA"). The defendant filed a motion to dismiss the charges and for a motion for leave to cite additional authority. The Court sided with the defendant.

The following background information is important to understand the case. In the fall of 2020, the defendant required that its students enroll in classes that used exams which were monitored by Respondus Monitor, a third-party protecting tool. An integral component of this tool was "a powerful artificial intelligence engine" that "performs a second-by-second analysis of the exam session" using facial detection, motion and lighting to analyze the student and examination environment." The plaintiffs brought the suit forward on behalf of all persons at the university that took an assessment monitored by the tool, and claim that in using the tool, the defendant violated the Illinois Biometric Information Privacy Act ("BIPA".) More specifically, the plaintiffs assert that the defendant: (1) failed to maintain or comply with biometric information collection guidelines in violation of 740 ILCS 14/15(a), (2) collected

students' biometric information in violation of 740 ILCS 14/15(b), (3) profited from biometric information in violation of 640 ILCS 14/15(c) and (4) disclosed biometric information in violation of 740 ILCS 14/15(d).

When the suit was initially raised, the defendants filed an instant motion to dismiss on April 21, 2021. A few months later, on June 16, 2021 defendants moved for leave in order to submit a reply to the plaintiff's response, ECF No. 13, which the Court ultimately granted. On July 20, 2021 the plaintiffs next moved for leave to file a sur-reply. Then on January 19, 2022 the defendants filed a motion to cite additional authority and finally on February 28, 2022 the defendants filed a section motion for leave citing additional authority.

There were several important legal questions that were brought before the Court. The first was whether the plaintiffs' were able to file a sur-reply. The Court noted that previous cases have ruled that sur-replies should "generally be allowed only for valid reasons, such as…new arguments in a reply brief."[114] [115] In reviewing the plaintiffs' proposed sur-reply, the Court does not find a response to arguments introduced in the defendant's brief. Instead, the plaintiff's advanced arguments that could have been previously issued. The Court therefore, defined the plaintiffs' motion for leave to file a sur-reply. The second issue was whether the defendant's motions for leave to cite additional authority should be considered. The Court notes that such leaves can

[114] Meraz-Camacho v. United States, 417 F. App'x 558, 559 (7th Cir. 2011).
[115] Hanson Eng'rs Inc. v. UNECO, Inc., 64 F. Supp. 2d 797, 798 (C.D. Ill. 1999).

be granted when recent case law illuminates issues relevant to the motion at hand.[116] Given that the defendants sought leave to cite recent state and federal court decisions relating to DIPA claims, the Court grants additional authority.

Next the Court considered whether it had standing over the issue at hand, and noted that this process of inquiry requires evaluating whether plaintiffs have Article III standing regarding the issues they advance.[117] Article III standing "requires allegations of a concrete and particularized injury that is traceable to the defendant's conduct and redressable by judicial relief."[118] The Court noted that it does have subject-matter jurisdiction over the Plaintiffs' Section 15(b) and Section 15(d) claims, given that previous cases have ruled that violations of those sections inflicts Article III injuries.[119] [120] However the Court finds that it does not have standing regarding Section 15(c) given that the plaintiffs have not sufficiently shown that the defendant has committed some kind of particularized and concrete harm to the plaintiffs. The competitive advantage that the defendants earned from collecting the information, which the plaintiffs cite as an example of a Section 15(c) violation, is not an injury particular to the plaintiff.[121]

Conversely the Court ruled that it did have standing concerning Section 15(a). The plaintiffs assert that the defendant did not follow a data-retention schedule and kept

[116] Clinton Hill v. Sood, No. 18-4133, 2020 U.S. Dist. LEXIS 260554, 2020 WL 12697470, at *1 (C.D. Ill. Feb. 20, 2020)
[117] Cothron v. White Castle Sys., Inc., 20 F.4th 1156, 1160 (7th Cir. 2021)
[118] Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146, 1151 (7th Cir. 2020)
[119] Cothron, 20 F.4th at 1161
[120] Bryant, 958 F.3d at 619
[121] King v. PeopleNet Corp., No. 21 CV 2774, 2021 U.S. Dist. LEXIS 207694, 2021 WL 5006692, at *5 (N.D. Ill. Oct. 28, 2021)

"vast amount[s] of biometric information." Previous Courts have ruled that failing to comply with a data-retention schedule is sufficient to confer Article III injury.[122] [123] [124] Therefore, the Court ruled that the plaintiffs had standing. The Court ultimately severed the Section 15(c) claims to state court and then addressed the defendant's motion to dismiss in terms of the remaining BIPA claims.

The defendant's defense hinged on the argument that the BIPA claims do not apply to them given that they are a financial institution. Although the BIPA imposes a variety of restrictions on the collection, retention and disclosure of data, these restrictions do not "apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act (GLBA) of 1999 and the rules promulgated thereunder."[125] The plaintiffs in turn assert that because the BIPA does not explicitly define the term financial institution, nor does it borrow a definition from another statute, the term financial institution has to be given its popularly understood meaning, which ultimately does not include universities. The plaintiffs further contend that if the term "financial institution" is not assigned its typical meaning, then it would be rendered superfluous.

The Court argued that this case requires a statutory analysis to understand the meaning of the law. The Court's primary objective was ascertaining and giving effect to the legislature's intent. To do so, it argued that the plain language of the statute

[122] Kalb v. GardaWorld CashLink LLC, Case No. 1:21-cv-01092, 2021 U.S. Dist. LEXIS 81325, 2021 WL 1668036, at *3 (C.D. Ill. Apr. 28, 2021)
[123] Marsh v. CSL Plasma Inc., 503 F. Supp. 3d 677, 683 (N.D. Ill. 2020)
[124] Roberson v. Maestro Consulting Servs. LLC, 507 F. Supp. 3d 998, 1008 (S.D. Ill. 2020)
[125] 40 ILCS 14/25(c)

was the best suggestion of legislative intent.[126] In other cases relating to the BIPA, when statutory terms were not well defined, their popularly understood meanings were regarded to be the most relevant ones.

The Court ultimately found the plaintiffs' arguments, that the defendant's were not to be considered a financial institution, unconvincing. The Court observed that arguments about the interpretability of the term financial institution overlook the specific meaning of the term "financial institution" to describe regulated entities within the broader context of the GLBA.[127] Moreover, the Court noted that if the financial institution exemption was intended to only apply to banks, as the plaintiff's suggested, then the legislature could have specifically excluded banks from the BIPA without referencing the GLBA in any way. There is also no issue of absurdity, as the plaintiffs claim, that results from embracing a broader understanding of the term financial institution. Absurdity can be applied when the literal construction of a statue leads to results which legislatures could not have necessarily contemplated. However the Court deemed that the application of such a standard in this particular case, does not demonstrate absurdity. The Court also made a further note that financial institutions were likely exempted in BIPA because they were already subject to further comprehensive federal privacy laws.[128] The Court concludes in the end that there is no ambiguity in the statutory language and finds that Section 25(c) in fact exempts financial institutions subject to the GLBA from the BIPA.

[126] Maksym v. Bd. of Election Comm'rs of City of Chi., 242 Ill. 2d 303, 950 N.E.2d 1051, 1060, 351 Ill. Dec. 223 (Ill. 2011)
[127] Kraft, Inc. v. Edgar, 138 Ill. 2d 178, 561 N.E.2d 656, 661, 149 Ill. Dec. 286 (Ill. 1990)
[128] Bryant v. Compass Grp. USA, Inc., 503 F. Supp. 3d 597, 601 (N.D. Ill. 2020)

The next question therefore that the Court had to answer, is whether the defendant, a private university, is in fact a GLBA-regulated financial institution. The Court considered that the definition of financial institution employed under the GLBA is broad and includes within it a plethora of entities many of whom are "not traditionally recognized as financial institutions."[129] Moreover, the FTC has ruled that colleges and universities are financial institutions in that such institutions are significantly involved in lending funds to consumers.[130] In addition, there have been other cases whether BIPA claims were made against university defendants and in such cases, Courts decided that universities did in fact qualify as financial institutions.[131] [132] Finally on this count, the Court finds that the defendants have sufficiently demonstrated that they are a financial institution because they do lend significant funds to consumers. Given then that the BIPA does not apply to financial institutions, the Court finds the defendant exempt and therefore argues that the BIPA claims that Plaintiff raises must be dismissed.

This case is an example of jurisprudence surrounding issues relating to the acquisition, storage and management of data through artificial intelligence related platforms. These types of legal issues are likely to only increase in prominence given that more artificial intelligence systems are being put into use that actively take data from users. Furthermore, as time goes on and the capabilities of such technologies improve, there are also significantly more points of data that can be sourced.

[129] F.T.C. v. AmeriDebt, Inc., 343 F. Supp. 2d 451, 457 (D. Md. 2004)
[130] Privacy of Consumer Financial Information, 65 Fed. Reg. 33646, 33,648 (May 24, 2000)
[131] Northwestern Univ., Case No. 21 C 1579
[132] Doe v. Elmhurst Univ., 2020 L 1400 (Ill. Cir. Ct. Nov. 18, 2021)

Although cases relating to the management of data have been rising, the degree to which lawsuits will be introduced is likely contingent on the existence of broader legislation that regulates the collection and storage of data. For example, Illinois is one of the few states that has such explicit guidelines in the form of the BIPA. Therefore, Illinois has seen a significantly higher number of data-related legal case actions than other states. There are likely many other instances of improper data management occurring in other states, but because those states do not have legislation akin to the BIPA, cases are ultimately not brought up in courts. If policymakers impose more regulations around data, cases of this nature will become increasingly common.

Ultimately, the jurisprudence in this case concerned the question of whether a private university was a financial institution. This legal question is not necessarily directly related to issues of AI jurisprudence. Disregarding that question however, the discussion in this case seems to suggest that regarding the BIPA, there are legitimate grounds for institutions to be sued when improper acquisition and storage of data occurs, given that such actions are sufficient to demonstrate that injury has been suffered. This case also suggests a defense that other institutions, that are in the position of being sued regarding the BIPA, might employ in order to win: claiming that they are an exempt financial institution.

3.2.6. Cahoo v. Fast Enters, LLC (12/20/2020)

Cahoo v. Fast Enters is a case that involved five plaintiffs which began putative class action cases to recover damages resulting from the State of Michigan's Unemployment Insurance Agency (UIA). MiDAS was a rudimentary AI system that operated using logic trees and was created to identify discrepancies in the records of various unemployment compensation records, automatically determine whether claimants had committed fraud and execute collection. The plaintiffs assert that the system has a plethora of failures: lack of human oversight, detection of fraud where none existed, provision of little or no notice to accused claimants, failure to allow administrative appeals and assessment of penalties against blameless individuals. Originally, the amended complaint listed 12 specific counts against the companies and individuals that the plaintiffs believed had contributed to the state's development of this flawed system. However, the case has been whittled down through motion practice and interlocutory appeal. At this point, only one procedural due process claim remains.

The defendants in this case were FAST Enterprises LLC and CSG Government Solutions, two companies that assisted the UIA in the development of MiDAS. The defendants petitioned for a second round of motion to dismiss on the grounds that the plaintiffs could not establish Article III standing because: (1) there was a failure to highlight an injury-in-fact because their claims were not completely adjudicated by MiDAS, (2) the alleged injuries were not traceable to the defendants and (3) that

several plaintiffs are precluded from bringing their claims because they did not disclose property interests in the cause of action during the respective bankruptcy proceedings. Therefore the key issue in this case concerned whether the Court had subject matter jurisdiction over the dispute.

Ultimately, the Court contended that the plaintiffs did have adequate standing and that the defendants, by virtue of their assistance in the development of MiDAS, were legally liable. Although it was true that the plaintiffs' fraud cases were not entirely auto-adjudicated by MiDAS, the UIA still employed the flawed system to determine the existence of fraud. Moreover, in several cases the system deemed that fraud was present when a plaintiff merely failed to properly respond to a question. In addition, the UIA did not provide sufficient notice to the plaintiffs of their fraud determination. Crucially, at least in this case, both FAST and CSG worked closely with the UIA in developing MiDAS so the injuries that the plaintiffs claim are actually traceable to them. The Court noted that more factual developments on the accrual dates for due process claims are required for several plaintiffs regarding their bankruptcy filings. On this point, the Court also asserted that there is not enough information to rule out ratification by a potential real party of interest under the Federal Rule of Civil Procedure 17(a)(3).

In order to fully understand this case, is it important to understand how MiDAS actually worked. When MiDAS logic-tree informed system observed a discrepancy between employer-paid wages and employee-claimed eligibility, it automatically generated a questionnaire to the claimant. If the questionnaire was then not

responded to in a timely manner, there was an automatic determination that the claimant knowingly misrepresented or concealed information. Once a fraud determination was made, MiDAS issued three separate notices. The first, was a Notice of Determination that observed there being an issue at hand. The second was another Notice of Determination which notified the claimants that their actions misled or concealed information alongside an announcement that any active claims would be terminated. These determinations did indicate that the claimants had a right to appeal a determination of fraud in court within 30 days. However, these notices oftentimes did not notify claimants of their ability to file late appeals for good cause. Moreover, because there were frequent errors in notifying claimants, many claimants did not become aware of assessment until after the appeal deadlines passed. If the claimants did not appeal the determination within 30 days, MiDAS automatically sent a letter in which it demanded payment of restitution, penalty and an accrued interest. Ultimately, the UIA deactivated MiDAS after another court found that the system was error-prone.[133]

Given that the defendants moved to dismiss the case for lack of subject matter jurisdiction, the Court had to first determine whether it had subject matter jurisdiction. In order to do so, the plaintiffs needed to demonstrate that they suffered an "injury in fact" that was caused by the defendant's conduct and that a favorable legal decision would ultimately redress that injury.[134] The injury the plaintiffs named was the deprivation of property interests in unemployment benefits and exposure to

[133] Zynda v. Arwood, 175 F. Supp. 3d 791 (E.D. Mich. 2016)
[134] Town of Chester v. Laroe Estates, Inc., U.S., 137 S. Ct. 1645, 1650, 198 L. Ed. 2d 64 (2017)

penalties without a sufficient pre- or post-deprivation procedure. According to federal law, unemployment benefits can only be denied if employers conduct sufficient fact finding, adjudicate issues and determine eligibility.

The Court ruled that the defendants misrepresented the claims of the plaintiffs and that the occurrence of a sufficient injury in fact was demonstrated. First the plaintiffs never contended that MiDAS deployed sophisticated AI tools. Rather, their contention was that fraud determinations were wrongfully made based on MiDAS's application of logic trees, which led to automated decisions that were unfair. Second, the core of the plaintiffs' complaints is that the automated system did not afford the kind of pre-deprivation process that state law required. Further, the plaintiffs held that post-deprivation remedies were inadequate because that decision-making process lacked transparency. Therefore, even if it is true, as the defendants claim that UIA employees participated in all the fraud adjudications, the plaintiffs can still demonstrate an injury of fact given that they were deprived of unemployment benefits without adequate pre- or post-deprivation processes.

The next issue concerned the question of traceability. To have standing, the injuries suffered by the plaintiff must have been fairly traceable to the defendant.[135] The defendants argued that no injury can be traced to them given that they never directly participated in any unemployment claim adjudication or collection effort, or established any of the procedures that the UIA directed to be included in MiDAS. The

[135] Lujan, 504 U.S. at 560-61

Court rejected these arguments. While it is true that the UIA had the final authority over MiDAS, both defendants were instrumentally involved in the development of MiDAS, a system that caused injury. FAST was contracted to build MiDAS and trained UIA employees on its use. Moreover, the Court ruled that FAST's claims that it deserved immunity because it was merely following the orders of the state in creating the system were insufficient; there is a long jurisprudential tradition in the United States that holds that 'just following orders' is not a sufficient legal defense.[136] CSG's case is more complex given that it was not directly involved in building MiDAS and merely played an advisory and administrative role.

The Court noted that providing advice to a third party that voluntarily injuries another is not constitutionally sufficient for liability exposure.[137] Therefore, CSG cannot be made liable by sole virtue of being an advisor. However the Court finds that CSG played a role that went beyond that of advice provision, for example it acted as the onsite project manager for MiDAS, mentored various UIA staff and served in an administrative role, working to ensure that the project was on budget and on time. These activities amounted to more than advising, should have alerted CSG to the unconstitutional practices of MiDAS and were sufficient for the fairly traceable requirement for injury causation and therefore the establishment of standing.[138]

The final legal issue concerned the fact that FAST and CSG argued that several of the individual plaintiffs did not own cause of action. More specifically, the defendants

[136] Kennedy v. City of Cincinnati, 595 F.3d 327, 337 (6th Cir. 2010)
[137] Crawford, 868 F.3d at 457
[138] Allen, 468 U.S. at 751; Parsons, 801 F.3d at 714

held that because these plaintiffs filed for bankruptcy before the cases began, their cases belonged to their respective bankruptcy estates. The defendants held that the plaintiffs lacked standing to sue given that they were not the real parties of interest. Courts have previously established that there are clear rules that actions "must be prosecuted in the names of the real party in interest."[139] In cases concerning bankruptcy, once a debtor files for a bankruptcy petition the debtor has no standing to pursue a pre-petition cause of action.[140] All pre-petition causes of action are property of the estate.[141] The issue in this case therefore came down to when the causes of action for each plaintiff accrued. The Court ruled that the factual record is not developed sufficiently to determine when the accrual of claims occurred. While the Court concedes that the circumstances surrounding some plaintiffs challenge the idea that the plaintiffs are in fact the true party of interest, these issues do not override the fact that the Court has appropriate subject matter jurisdiction.

This case is significant for many reasons. First, it is broadly indicative of the fact that companies and government agencies are often eager to deploy AI tools without first developing a complete understanding of how such tools will work and what their associated ethical problems may be. In this case, the UIA deployed a system that was error-prone, deployed the tool before these errors were fully understood and as a result, facilitated the inequitable handling of several unemployment benefit claims. As AI grows in technical sophistication, and more companies rush to develop AI

[139] Fed. R. Civ. P. 17(a)
[140] Bauer v. Commerce Union Bank, 859 F.2d 438, 440-41 (6th Cir. 1988)
[141] Bd. of Trustees of Teamsters Local 863 Pension Fund v. Foodtown, Inc., 296 F.3d 164, 169 n. 5 (3d Cir. 2002))

related tools, the possibility of those tools being misused along the lines of UIA and MiDAS likewise increases. Both courts and legislative bodies will have important roles to play in working to ensure that AI tools do not perpetuate inequitable outcomes: courts can work towards ensuring that justice is served when inequitable outcomes result and legislative bodies in imposing regulations to limit the occurrence of such outcomes.

This case also highlights what degree of involvement in the development of AI related technologies is sufficient for establishing traceability in instances when injury has been committed. Advising is not sufficient for liability however more direct involvement in the creation and management of a tool is, even if the tool in question is deployed by an additional agency. This fact should serve as a warning to private entities that assist in the development of AI-related tools deployed by other actors, whether they are private or state: if the tool ultimately causes injury or violates some law, your company might be legally liable even though it did not directly oversee the tool's use.

Finally, this case interestingly sheds light as to the types of adjudication processes that are deemed to be fair and legal in the case of unemployment insurance. The Court rules that it is essential that adequate pre- and post-deprivation processes are provided for. In this case specifically, it was shown that post-deprivation processes were inadequate because the decision-making process was not transparent. The AI-system deployed in this case was admittedly rudimentary: MiDAS only made use of

low-level logic trees. In the near future, it is possible to imagine systems that can be less prone to the types of errors that MiDAS committed and more able to flexibly consider the cases of unemployment insurance claimants. The possibility of their being superior systems gives rise to the question of what degree of transparency is sufficient for adequate post-deprivation? Some neural network based AI systems make decisions in a black-box fashion: with these systems it is sometimes not necessarily clear to the developers themselves, how the systems reached the decisions they did. This particular legal case does not reveal what level of transparency would be sufficient on the part of an AI system in order to deem that it adjudicated an unemployment insurance claim transparently. As AI systems become increasingly more advanced, this type of issue might be one for future courts to decide.

3.2.7. Divino Grp. LLC v. Google LLC (01/06/2021)

This case concerns a group of LGBTQ+ content creators that used YouTube. The content creators are the plaintiffs and they brought forward a variety of anti-discrimination claims against YouTube, holding that YouTube (owned by Google) unfairly discriminated against the plaintiffs based on their gender or sexual orientation. More specifically the plaintiffs, Divino Group LLC asserted the following claims: (1) violation of the plaintiffs' First Amendment rights under 42 U.S.C § 1983, (2) violation of Article I, Section 2 of the California Constitution, (3) violation of the Unruh Act, California Civil Code § 51, et seq., (4) unfair competition under the

California Business and Professions Code § 17200, et seq., (5) breach of the implied covenant of good faith and fair dealing, (6) false advertising and false association in violation of the Lanham Act, 15 U.S.C. § 1125, et seq. Moreover, the Plaintiffs sought a declaration that Section 230 of the Communications Decency Act (CDA), 47 U.S.C. § 230(c) was unconstitutional as well as an omnibus claim for declaratory relief. The defendants moved to dismiss the claims under the Federal Rule of Civil Procedure 12(b)(6) and as barred under Section 230 of the CDA. Dkt. No. 25. The Court denied the claims of the plaintiffs arguing that no first amendment violation occurred, it was not properly suited to judge issues of state law and the cited section of the CDA was not in fact unconstitutional.

The plaintiffs construct their case in the following fashion. First they point to statements YouTube made to assert that it views itself to be one of the most essential public forums for the expression of ideas and speech. Second, the plaintiffs suggest that despite such claims, YouTube has discriminatorily interfered with their uploading of certain videos through their Age Restriction and Restricted Mode settings. The plaintiffs highlight some further examples of discrimination: "use of discriminatory AI and algorithms, demonetizing channels, not showing videos in search results, deleting LGBTQ+ content from the recommended Up Next feature, playing anti-LGBTQ+ advertisements immediately before plaintiffs' videos and permitting anti-LGBTQ+ comments to appear on the plaintiffs' content." Lastly, the plaintiffs held that YouTube had motivations to behave in anti-competitive ways given that YouTube

produced and distributed content that directly competed with the content produced by the plaintiffs.

The first question that the Court considered is whether the plaintiffs had their first Amendment rights violated under 42 U.S.C. § 1983. To demonstrate a successful violation in this regard, the plaintiffs needed to demonstrate that a person acting under the color of state law caused a violation of constitutional or other federal rights.[142] The defendants dismissed this claim asserting that the defendants are private entities, not state actors. The plaintiffs concede that YouTube is a private entity but argued that it should be considered a state actor that is subject to First Amendment standards for two reasons. First, the defendants have designated YouTube to be a public forum of free expression with their language and therefore take on the exclusive government function of regulating free speech in that forum, as required by the First Amendment. Second, by invoking the protections of a federal statute in Section 230 of the CDA in order to unlawfully discriminate against plaintiffs and their content, the defendants' private conduct becomes state action endorsed by the federal government.

The Court strikes down the first subpoint noting that in previous decisions, such as the Ninth Circuit's *Prager University v. Google LLC*, it was ruled that YouTube's hosting of speech on a private platform is not a traditional and exclusive government function. Moreover, the Supreme Court has consistently held that there are very

[142] Crumpton v. Gates, 947 F.2d 1418, 1420 (9th Cir. 1991)

limited cases where private entities engage in state action.[143] Finally, there is no evidence that YouTube in any way declared itself to be a state actor.

The Court likewise struck down the second subpoint. It cannot be said that by virtue of the CDA statute the federal government endorses YouTube's alleged discrimination because the section the plaintiffs cited only applied to action taken under state law not federal law.[144] In addition, although a private actor may be considered a state actor when the government compels it to take a particular action, the plaintiffs fail to sufficiently show that there is government compulsion of any kind in this instance.[145] Section 230 does not require private entities to do anything in particular and there is no evidence that YouTube applied the Restricted Mode features to the Plaintiffs' videos or demonetized them by "compulsion of sovereign authority." The Court concludes the matter by referencing a relevant Supreme Court case, Moose Lodge No. 107 v. Irvis, in which it held that "where the impetus for discrimination is private, the State must have significantly involved itself with invidious discriminations in order for the discriminatory action to fall within the ambit of the constitutional prohibition."[146] There was no evidence that the state was significantly involved in any of YouTube's content decisions, so the First Amendment violation claim fails.

The next claim the Court turned its attention toward was the plaintiffs' claims that YouTube violated the Lanham Act, 15 U.S.C. § 1125(a)(1) because it falsely advertised.

[143] Manhattan Cmty. Access Corp. v. Halleck, 139 S. Ct. 1921, 1930, 204 L. Ed. 2d 405 (2019)
[144] Kali v. Bowen, 854 F.2d 329, 331 (9th Cir. 1988)
[145] Blum v. Yaretsky, 457 U.S. 991, 102 S. Ct. 2777, 73 L. Ed. 2d 534 (1982)
[146] Moose Lodge No. 107 v. Irvis

The Plaintiffs also previously made a false association claim, but because the plaintiffs withdrew this claim at a previous hearing, the Court did not focus its attention on this claim. The false advertisement claim charged that the application of Restricted Mode to certain videos degraded the content by inappropriately implying that it contained shocking, inappropriate, offensive or sexually explicit content that is somehow unfit for minors. This false advertising the plaintiffs further held, caused injury "in the form of diverted views, decreased subscriber numbers, and lost advertising revenues and other harm to channel and video reach, distribution and monetization." False advertisement requires that defendants make false or misleading representation of fact in commercial advertising or promotion about the plaintiffs' offerings.

The Court rejects the Lanham Act false advertising claims, citing the Ninth Circuit's decision in Prager III. The Court claimed that videos being made unavailable in Restricted Mode is not actionable as commercial advertising and promotion and merely accurate explanations of the applications of defendants' content review and monitoring procedures.[147] The Court ruled that the decisions about Restricted Mode were made to explain a user tool not for promotional purposes of any kind.[148]

The remaining claims that the plaintiffs advance are state law claims, and the Court considers whether as a federal Court, it has jurisdiction to adjudicate over these issues. In making a decision to retain supplemental jurisdiction, the Court noted that it should consider further factors such as "economy, convenience, fairness and

[147] Prager III, 951 F.3d at 1000
[148] Fashion Boutique of Short Hills, Inc. v. Fendi USA, Inc., 314 F.3d 48, 57 (2d Cir. 2002)

comity."[149] In weighing these factors, the Court ruled in favor of dismissal. For example, it claimed that this current case was at a pleading stage with no discovery, so a current dismissal would have enabled the conservation of federal resources. Moreover, dismissal would have promoted comity in allowing California Courts to adjudicate over questions of state law.

Next the Court addressed the plaintiffs' assertion that Section 230 of the CDA is unconstitutional and their subsequent claim for declaratory relief regarding CDA Section 230 immunity. This section of the CDA "immunizes providers of interactive computer services against liability arising from content created by third parties'' in order to "protect websites not merely from ultimate liability, but [also] from having to fight costly and protracted legal battles."[150] Ultimately for the Court to issue declaratory relief in this case, the plaintiffs must show that their first Amendment rights have been violated. However, the plaintiffs have not sufficiently shown such a violation so their declaratory claims fail. Second in this case, the plaintiffs included a claim for declaratory relief in anticipation of the defendants' assertion of Section 230 immunity. However, courts have previously refused to grant declaratory relief to parties that attempt to assert only anticipatory defenses.[151]

The plaintiffs additionally made a broad omnibus claim for declaratory relief, on the grounds that the defendants have violated the U.S. Constitution, the California

[149] Acri v. Varian Assocs., 114 F.3d 999, 1001 (9th Cir. 1997)
[150] Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008)
[151] Veoh Networks, Inc. v. UMG Recordings, Inc., 522 F. Supp. 2d 1265, 1271 (S.D. Cal. 2007)

Constitution, the Unruh Civil Rights, California Business and Professions Code §§ 17200, et seq., the Lanham Act and the various express and implied terms of the parties' contracts. The Court dismissed these claims because the plaintiffs have not demonstrated that there are any federal claims over which this Court has jurisdiction. Moreover, the Court, as a federal entity, declined to exercise additional jurisdiction over the plaintiffs' state law claims.

This case reveals the thinking courts have about the issue of private entities that host some type of speech, using AI-related systems to determine what kinds of speech they can ultimately host on a platform. The jurisprudence in this case suggests that provided that the actor is a private entity, its applications of rules to determine what content it allows and how it labels such content, do not constitute violations of the First Amendment. Moreover, claims that an actor facilitates an important speech hosting function is not sufficient to demonstrate that it should be regarded as a state actor. This decision is significant and meaningful for other social media entities that likewise host content and want to understand how they can employ AI systems to monitor the kind of content they can ultimately host.

4. Conclusion

A growing number of economic actors are deploying Artificial Intelligence (AI) technology in a variety of domains and incorporating it into an ever greater number of decisions and practices. There is a continuous decrease in cost per achieved

computing performance as digital devices are increasingly prevalent in our daily lives and across our economy, which creates an immense amount of data that is produced persistently. Together, these two factors provide fertile ground for the dissemination and uptake of artificial intelligence, with the accumulated impacts on economic activity and society as a whole being difficult to anticipate.

In this paper, we provided insights on the reactions of law enforcement institutions to the increasing deployment of artificial intelligence systems in addition to a collection of the various responses to AI adoption, the guardrails developed to prevent abuse as a part of the overall regulatory efforts to reach the right balance between achieving benefits and minimizing risks associated with this powerful technology. The paper focused on select cases from the period between 2017 and 2022 in order to better capture the current status quo of the rulings. Furthermore, the article briefly discussed emerging regulatory initiatives targeting AI and automated decision-making on both sides of the Atlantic by way of presenting key facts and developments that can inform current and future debates with respect to regulatory frameworks applicable to AI systems.

An overview and analysis of selected cases were presented in this paper: from the EU judiciary and administrative authorities and from US courts on a range of artificial intelligence and automated decision-making subjects including automated web scraping, facial recognition, voice-recognition for detecting emotions, and government use of digital welfare fraud detection systems, algorithms assisting

judicial decisions, computerized rules to process personal injury protection claims, automated recommender systems in social network leading to harmful content, AI's eligibility to obtain patent rights, use of facial recognition technology during exam sessions, use of digital fraud detection systems for insurance sector, and discriminatory social media algorithms. By summarizing and breaking down essential elements of select judicial and administrative case examples from the European Union and the United States where the use of algorithmic systems was brought to court or otherwise ruled on, this article examined the way that regulatory and legal systems are de facto accommodating the ongoing deployment of AI systems.