ONPOINT / A legal update from Dechert's Global Finance, Privacy & Cybersecurity, Litigation, and Financial Services Groups

Artificial Intelligence: Legal and Regulatory Issues for Financial Institutions

Authored by Linda Ann Bartosch, K. Susan Grafton, Paul Kavanagh, Daniel Natoff, Mark D. Perlow, Corey F. Rose, Brenda R. Sharton, Timothy Spangler, Robert J. Rhatigan, Audrey Wagner, Katherine Hurley, Michael McGrail, James Smith, and Lucy Yang

April 2023

Dechert LLP

Artificial Intelligence: Legal and Regulatory Issues for Financial Institutions

April 2023 / Authored by Linda Ann Bartosch, K. Susan Grafton, Paul Kavanagh, Daniel Natoff, Mark D. Perlow, Corey F. Rose, Brenda R. Sharton, Timothy Spangler, Robert J. Rhatigan, Audrey Wagner, Katherine Hurley, Michael McGrail, James Smith, and Lucy Yang

Over the last six months, artificial intelligence (AI) has captured the public imagination in a way it never has before. A new generation of AI-powered language models make use of a deep learning architecture known as a transformer. Through the transformer architecture, AI can generate coherent and contextually relevant text based on input prompts provided by users. Trained on an extensive dataset, such AI predicts the next word in a sequence of text, allowing it to produce human-like written content. Its natural language processing capabilities have allowed it to be applied in various fields, ranging from content generation to translation and summarization.

AI combines computer science and structured data sets to create programs that perform tasks which typically require human intelligence, such as reasoning, learning and decision-making. "Real" AI traditionally refers to AI systems that attempt to demonstrate a broad range of cognitive abilities that may be perceived as being similar to those of a human being. Although large language model (LLM)-based AI software have demonstrated the ability to produce coherent and contextually relevant text based on input prompts, it is crucial to recognize that such AI software are not "real" AI in the traditional sense. Rather, these are powerful tools that excel at predicting statistically the next word in a given sequence.[1] In fact, many LLM-based AI software lack the ability to truly comprehend or reason beyond the patterns they observe in the text, and cannot form independent thoughts, reason through complex problems or make decisions based on abstract concepts.

Regulatory Oversight of AI and AI Software Implementation

As the use of AI by financial market participants increases in popularity, United States (US), European Union (EU), and United Kingdom (UK) regulatory agencies are slowly adapting to changes in market practices stemming from AI developments. Although banks and investment firms using AI may benefit from increased efficiency and reduced transaction time and costs, among other benefits, they must consider potential legal and regulatory risks associated with each new instance of AI use.

The White House Office of Science and Technology Policy released a white paper in October 2022 providing a framework to "guide the responsible use of automated systems."[2] The framework highlights the need for (i) safe and effective systems; (ii) algorithmic discrimination protections; (iii) data privacy; (iv) notice and explanation; and (v) human alternatives, considerations, and fallback for systems that "have the potential to meaningfully impact the…public's rights, opportunities, or access to critical resources or services."[3] Regulatory agencies—such as the

---

1 Scott W. Bauguess, Acting Director and Acting Chief Economist, DERA, SEC, "The Role of Big Data, Machine Learning, and AI in Assessing Risks: a Regulatory Perspective," Champagne Keynote Address (June 21, 2017), https://www.sec.gov/news/speech/bauguess-big-data-ai (noting that latent dirichlet allocation "measures the probability of words within documents and across documents").

2 WHITE HOUSE OFF. OF SCI. AND TECH. POL'Y, BLUEPRINT FOR AN AI BILL OF RIGHTS 4 (2022).

3 *Id.* at 5-8.

Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC)—further emphasize the need to protect investors in financial markets. SEC Chairman Gary Gensler has noted that investment professionals must exercise caution when using an AI platform to ensure that investors' interests take priority.[4] CFTC Commissioner Christy Goldsmith Romero has emphasized the need for financial services firms to implement strategies to ensure that AI is "deployed in a way that aligns with the interests of all stakeholders."[5]

Although specific regulations addressing the use of AI software have not yet been implemented by financial regulators, the use and deployment of AI software is subject to broader legal and ethical considerations. In the US, there are several regulatory frameworks, including industry-specific regulations, that may apply to the use of AI models, depending on the context of their use. Additionally, several other jurisdictions are considering regulations that address algorithmic accountability and transparency.

Banking and Finance

Regulatory requirements arising under the Bank Secrecy Act (BSA), the Dodd-Frank Wall Street Reform and Consumer Protection Act and the Basel III framework mandate strict compliance requirements for banks and financial institutions, including risk management, capital adequacy, and consumer protection.

For example, financial institutions are required to implement an anti-money laundering program that includes a Customer Due Diligence (CDD) program consisting of a Customer Identification Program (CIP) to identify and verify the identity of customers and beneficial owners of legal entity customers when opening accounts, understand the nature and purpose of customer relationships to develop risk profiles and conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[6] In such circumstances, AI software must ensure that it effectively identifies potential risks and red flags, such as suspicious transaction patterns or high-risk customers. Further, financial institutions must maintain systems that monitor suspicious activity that may indicate money laundering, terrorism financing or other illicit activity are occurring.[7] Compliance systems should also contain protocols that identify and report transactions in currency exceeding $10,000 to the Financial Crimes Enforcement Network (FinCEN).[8] Finally, the BSA requires that financial institutions maintain records for a designated period of time.[9] AI software systems and protocols should be regularly monitored to ensure compliance with the BSA and FinCEN regulations.

---

4 Gary Gensler, Chairman, SEC, "Investor Protection in a Digital Age," Remarks Before the 2022 NASAA Spring Meeting & Public Policy Symposium (May 17, 2022), https://www.sec.gov/news/speech/gensler-remarks-nasaa-spring-meeting-051722.

5 Christy Goldsmith Romero, Commissioner, CFTC, Opening Statement of Commissioner Christy Goldsmith Romero at the Technology Advisory Committee on DeFi, Responsible Artificial Intelligence, Cloud Technology & Cyber Resilience (Mar. 22, 2023), https://www.cftc.gov/PressRoom/SpeechesTestimony/romerostatement032223.

6 *See* Information on Complying with the Customer Due Diligence (CDD) Final Rule, FinCEN, https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule (last accessed Mar. 30, 2023); 31 C.F.R. § 1010.210-230 (2021).

7 31 C.F.R. § 1010.320 (2021).

8 31 C.F.R. § 1010.310 (2021).

9 31 C.F.R. § 1010.430 (2021).

Lending

Lenders have been using AI tools for several years to target consumer marketing, identify and protect against fraud, make credit decisions, and service portfolios. The emergence of more sophisticated AI and machine learning programs over the past six months is only accelerating these trends, particularly towards algorithmic underwriting decisions used by lenders to determine which customers to lend to and on what terms. Financial institutions should be mindful of the guidelines and regulations related to fair lending, consumer protection and anti-discrimination when incorporating AI tools into the lending lifecycle.

In May 2022, the Consumer Financial Protection Bureau (CFPB) affirmed that federal anti-discrimination laws, for example, the Equal Credit Opportunity Act (ECOA) (which requires a lender to explain to a customer the reason an application for credit was denied or other adverse action was taken), also apply when those decisions were made by a credit model using complex algorithms, such as those operating within AI tools.[10] The CFPB has also stated that the fact that an algorithm is "too complicated, too opaque in its decision-making, or too new" is not a sufficient reason to justify the failure to comply with the ECOA.[11]

In addition, other lending laws, such as such as the Fair Lending Act and the Fair Credit Reporting Act (FCRA), also require a variety of disclosures to consumers about what data is collected and used by lenders, even if it is used by their AI algorithms rather than by a lender directly, as well as what the effect of that can be.[12] If AI software will be used to collect or analyze consumer data, lenders may need to disclose its use and to have policies that govern its use in place.[13] Lenders are responsible for ensuring any data used by algorithms for credit decisions is accurate and up to date, so if a financial institution is using a third-party dataset for training purposes, it should have policies and procedures in place to ensure it has a reasonable belief that its data is accurate and up to date.[14] Lenders are also required to investigate consumer disputes, which could require investigation of the practices of sourcing and using data.[15]

Other regulators, such as the Department of Justice, CFPB and Office of the Comptroller of the Currency, have announced plans to increase scrutiny of potential disparate impact and digital redlining through proxy information.[16] As more lenders embrace AI software as part of their credit approval process and during other phases of the lending lifecycle, we can expect to see increased attention from the CFPB and other regulators including the Federal Trade

---

10 *CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex* Algorithms, CFPB (May 26, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/.

11 *Id.*

12 12 C.F. R. §§ 1022.72-73 (2023).

13 Andrew Smith, *Using Artificial Intelligence and Algorithms*, FED. TRADE COMM'N (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

14 12 C.F. R. 1022.42 (2023).

15 12 C.F. R. 1022.43 (2023).

16 Press Release, US Dep't of Just., Justice Department Announces New Initiative to Combat Redlining (Oct. 22, 2021) (on file with author).

Commission (FTC), SEC and banking regulators looking to ensure that all consumer protections requirements are being fully complied with.[17]

Investment and Asset Management

The SEC has published interpretive guidance on the use of digital and other computer technologies in providing investment advice ("digital investment advice" or "DIA"). This guidance emphasizes the importance of transparency; fulfilling the duty of care when using these technologies; robust processes, controls and risk management; and compliance policies and procedures. While these statements do not expressly apply to current AI tools that have attracted widespread attention in the last six months, the underlying principles are the clearest guidance financial services firms currently have from the SEC and FINRA on this topic.[18] The Financial Industry Regulatory Authority (FINRA) has published guidance that directly addresses the use of AI. The CFTC, through LabCFTC, monitors AI use to understand its impact on current regulations and derivatives markets.[19] As Chair Gensler noted, "there are tradeoffs that come with new technologies."[20]

SEC/Investment Advisers

In a 2019 interpretive release, the Commission Interpretation Regarding Standard of Conduct for Investment Advisers (*Fiduciary Interpretation)*, the SEC states that investment advisers are subject to federal fiduciary duties that consist of a duty of care and a duty of loyalty, which, taken together, require an adviser to act in the best interest of its client at all times.[21] The SEC's statements and guidance on DIA have largely focused on the duty of care and related controls and compliance procedures. As articulated by the SEC in the *Fiduciary Interpretation*, the fiduciary duty of care includes a duty to provide suitable investment advice to each client. The SEC conceptualizes suitability as a duty to provide individually tailored advice to each client. While the scope of an adviser's suitability responsibilities varies with the size, sophistication and objectives of advisory clients, the SEC expects advisers to implement processes reasonably designed to assure that investment advice is and remains suited to clients' needs.

In addition, the SEC Staff has interpreted an investment adviser's fiduciary duty to mean that, when an investment adviser has committed an error in the investment process that violates its standard of care, the adviser is responsible for resulting losses. While SEC and Staff practice can vary, the SEC and Staff in enforcement actions and examinations often apply a negligence standard to errors made by investment advisers in implementing investment advice, based on their fiduciary duty of care. The SEC has brought a number of enforcement actions alleging that

---

17 *FTC Report Warns About Using Artificial Intelligence to Combat Online Problems*, FED. TRADE COMM'N (June 16, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems; s*ee generally* Betsy Vereckey, *SEC's Gensler on how artificial intelligence is changing finance*, MIT (Oct. 12, 2022), https://mitsloan.mit.edu/ideas-made-to-matter/secs-gary-gensler-how-artificial-intelligence-changing-finance (internal quotations omitted).

18 For an in-depth discussion of SEC guidance regarding robo-advisers, see Mark D. Perlow, Michael L. Sherman, & Ashley N. Rodriguez, *Strategies in Applying Securities Laws to Digital Investment Advice*, 29 INV. LAW. (Sept. 2022).

19 Commodity Futures Trading Commission, *Primer on Artificial Intelligence in Financial Markets*, LABCFTC, https://www.cftc.gov/media/2846/LabCFTC_PrimerArtificialIntelligence102119/download (last accessed Mar. 30, 2023).

20 Vereckey, *supra* note 17.

21 *Commission Interpretation Regarding Standard of Conduct for Investment Advisers*, SEC Interpretive Release, SEC Rel. No. IA-5248 (June 5, 2019), available at https://www.sec.gov/rules/interp/2019/ia-5248.pdf.

errors in coding were negligent because the adviser ignored red flags that the defendant should have seen and responded to.[22]

These issues are presented in a distinct form for the adviser that uses AI tools in formulating investment advice. The differentiating factors derive from what have come to be called the "AI control problem," the "AI explainability problem" and the "AI data/input problem." First, the "AI control problem" is the risk that AI systems will program themselves in ways outside of the control, expectations or objectives of their human creators. Second, the "AI explainability problem" is the related issue that AI systems are complex, black box models, and the mechanism by which they reach a result are often or generally not understandable or explainable to humans. Finally, the "AI data/input problem" derives from the fact that the patterns that machine learning systems recognize are a function of the data that is inputted, and thus a data set that is high quality and free to the extent possible of inappropriate biases is key to an AI system effectively and appropriately achieving its objectives. In response to these three problems, quality controls around AI have tended to focus on the inputs (*i.e.*, data) to models and outputs from models (*i.e.*, decisions). Anomalous outputs (as determined by human monitors) lead to re-examining the inputs and the design parameters for issues and then trying to correct or adjust them.

As AI systems become more prevalent among investment advisers, these three AI problems could generate distinct variations on the fiduciary duty of care issues discussed above. In particular, it could be more difficult for advisers using AI tools to demonstrate to, and win the trust of, regulators and clients that investment-related errors are not negligent because they derived from a reasonable investment process. To the extent that investment decisions are made using AI software rather than by a human portfolio manager, the adviser would not be able to reveal how the model reached its decision in the same way that traditional advisers can make human portfolio managers available to the SEC to explain their reasoning and their sources of information, and they would not be able to point to rule-based algorithms or code intended to fulfill the same functions. In addition, it might not be detectable to the adviser or the SEC Staff if an AI model does not reflect and effect the factors that the adviser considers to be important. The SEC therefore is likely to focus more on an investment adviser's controls around inputs and after-the-fact monitoring and testing procedures, in particular monitoring for red flags, and on the expertise and experience of personnel developing and overseeing AI investment models. This emphasis will put even more stress on these personnel and processes, with the regulatory and governance consequences of data issues and process mistakes being magnified.

The SEC has not yet provided meaningful guidance on these questions. Nonetheless, there is some regulatory guidance (which still is incomplete and high-level) in an International Organization of Securities Commissions (IOSCO) report from September 2021.[23] Translating its recommendations (which are directed to national regulators) to principles and policies for advisers, one can derive a reasonable framework for AI policies and procedures relating to investment advice:

1. Designate senior managers responsible and accountable for the oversight of the development, testing, deployment, monitoring and controls of AI tools.

---

22 *See* Mark D. Perlow, Michael L. Sherman, & Ashley N. Rodriguez, *Strategies in Applying Securities Laws to Digital Investment Advice*, 29 INV. LAW. (Sept. 2022).

23 *See* Final Report FR 06/2021, International Organization of Securities Commissions (IOSCO) (Sept. 2021) (IOSCO AI Report), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf at 17-21.

2. Test and monitor AI techniques to validate their outputs on an initial (*i.e.*, pre-implementation) and regular basis, including how they behave in stressed market conditions and whether they comply with regulatory expectations.

3. Assure that the investment adviser has personnel with sufficient skills, expertise and experience to develop, test, deploy, monitor and implement controls for the AI techniques that the investment adviser uses.

4. Implement appropriate controls to assure that the data that is input into AI systems is of sufficient quality, minimizes inappropriate biases and is sufficiently broad for a well-founded application of AI tools.

5. Monitor and oversee the conduct and performance of third-parties on which the investment adviser relies in using AI software, including data providers.

6. Disclose the investment adviser's reliance on AI techniques and related risks.

FINRA/Broker-Dealers

Current FINRA guidance for broker-dealers may also be relevant to AI software usage. FINRA highlights potential considerations that broker-dealers should consider when reviewing their model risk management programs, such as conducting regular testing and developing performance benchmarks.[24] FINRA guidance also highlights challenges attendant to members' use of AI for risk management programs, including "model explainability, data integrity, and customer privacy."[25] Broker-dealers should also take into account how AI should be accounted for in a broker-dealer's supervisory control systems and ensure that their written supervisory procedures take into account the use of AI technology, and should "update and test related supervisory procedures."[26] FINRA recommends broker-dealers "establish a cross-functional governance structure, conduct extensive testing of applications to identify potential harm to customers through the use of AI, establish fallback plans in case an AI-based application fails, and evaluate and verify personnel registrations as the roles of technology, back-office, trading, and investment management begin to blend. As discussed below, broker-dealers (and other financial services firms) are also subject to data privacy concerns. Broker-dealers are subject to Regulation S-P, which requires that broker-dealers maintain written policies and procedures to protect customers' personally identifiable information.[27] Thus, financial services firms using AI software should establish appropriate oversight and control mechanisms to ensure compliance with applicable securities laws and regulations.

---

24 Artificial Intelligence (AI) in the Securities Industry, FINRA (June 2020) (FINRA AI Guidance), https://www.finra.org/sites/default/files/2020-06/ai-report-061020.pdf.

25 *Artificial Intelligence (AI) in the Securities Industry, Key Challenges and Regulatory Considerations,* https://www.finra.org/rules-guidance/key-topics/fintech/report/artificial-intelligence-in-the-securities-industry/key-challenges

26 *Id.*

27 *FINRA AI Guidance, supra* note 24 at 15.

CFTC

CFTC's Technology Advisory Committee (TAC) held its inaugural meeting on March 22, 2023, which included a panel on "*Responsible Artificial Intelligence*."[28] The panel discussed the white paper, *Blueprint for an AI Bill of Rights*, released by the White House and emphasized the need to understand the implications and considerations surrounding recent emerging technologies. The panel also heard presentations from industry experts on the ethical concerns of AI tools and the cybersecurity considerations that accompany this budding technology. While the CFTC did not introduce specific guidance and regulations at this time, the TAC established a sub-committee on "Emerging Technologies" to further explore the topic, its issues and implications on existing CFTC regulations and policies.

Privacy and Cybersecurity

FTC

The FTC published guidelines on AI usage, which provide insight into the FTC's expectations for organizations using AI tools.[29] Financial institutions using AI software should consider taking the following measures into account:

- **Be truthful about the claims the company can make through its use of AI software**. The FTC's recent guidance from February 2023 emphasizes that companies using AI technology should not overpromise or exaggerate what the algorithm can provide.[30]

- **Be truthful about the data the company uses**. In its guidance, the FTC has consistently stated that companies must be honest about how they acquire the data they use to power their algorithms.

- **Be transparent about how AI software is used and what decisions are made using it**. The FTC has stated that companies will want to be prepared to explain the rationale behind decisions made using AI software, particularly those affecting consumers directly. Entities will want to be transparent in their use of AI software, informing customers when AI-generated content or automated decision-making processes are being used.

- **Take measures to establish oversight protocols for its use of AI software and its resulting outputs.** Financial institutions will want to take measures to follow legal and ethical obligations, such as implementing internal policies and procedures, providing training to employees, and designating personnel to oversee AI software's usage. In addition to adopting and maintaining oversight protocols, financial services firms should hold themselves accountable for AI software generated content, or, as the FTC notes, "be ready for the FTC to do it" for them.

---

28 Commissioner Goldsmith Romero Announces Technology Advisory Committee Meeting Agenda That Includes Cybersecurity, Decentralized Finance, and Artificial Intelligence, COMMODITY FUTURES TRADING COMM'N (Mar. 22, 2023), https://www.cftc.gov/PressRoom/Events/opaeventtac032223.

29 *See* Michael Atleson, Keep your AI claims in check, FED. TRADE COMM'N (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check; Elisa Jillson, Aiming for truth, fairness, and equity in your company's use of AI, FED. TRADE COMM'N (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai; Andrew Smith, Using Artificial Intelligence and Algorithms, FED. TRADE COMM'N (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

30 Atleson, *supra* note 29.

- **Understand what data sets power the AI model to ensure it would not yield unfair or inequitable results to legally protected groups.** Financial services firms should consider monitoring AI software's outputs to ensure that they do not discriminate against protected classes or perpetuate existing biases. As explained in the FTC's 2021 guidance, companies should regularly assess the data used to train AI software and review its outputs for potential bias.[31]

The intersection of privacy, security and consumer protection and evolving technologies continues to be an area of particular interest for the FTC, as evidenced by its recent Advance Notice of Proposed Rulemaking, which explored rulemaking for "automated decision making systems," and through the FTC's launch of the Office of Technology to bolster its subject-matter expertise in this area.[32] As recent FTC enforcement actions show in *U.S. v. Kurbo, Inc. and WW Int'l, Inc.*[33], *In the Matter of Everalbum, Inc*.,[34] and *In the Matter of Cambridge Analytica, LLC,*[35] companies that fail to comply with the FTC's expectations through their creation of algorithms and use of AI could face regulatory penalties and/or be forced to delete algorithms, data, and models.[36]

As discussed above, financial institutions that make credit decisions powered by machine learning algorithms will be subject to the Fair Credit Reporting Act, also enforced by the FTC, and must comply with its requirements.[37]

Applicable US State Law Considerations

The patchwork of US state privacy laws contains various provisions addressing artificial intelligence, with which financial institutions using AI software will need to comply. For example, the California Consumer Privacy Act[38] (as

---

31 Jillson, *supra* note 29.

32 April J. Tabor, Trade Regulation Rule on Commercial Surveillance and Data Security, Fed. Trade Comm'n, 16 CFR Part 464, https://www.ftc.gov/system/files/ftc_gov/pdf/commercial_surveillance_and_data_security_anpr.pdf (last visited Mar. 28, 2023).

33 *U.S v. Kurbo, Inc. and WW Int'l, Inc.*, No. 3:22-cv-00946, Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, ECF No. 15, Fed. Trade Comm'n (March 3, 2022) (requiring the company to delete an algorithm it created for its weight-loss app and pay $1.5 million ($1,500,000) for collecting personal information from children under age 13 in violation the Children's Online Privacy Protection Act), https://www.ftc.gov/system/files/ftc_gov/pdf/wwkurbostipulatedorder.pdf

34 *In the Matter of Everalbum, Inc.*, File No. 192 3172, Fed. Trade Comm'n (May 6, 2021) (requiring the company to delete the algorithms that it created from photographs that users uploaded to tits platform, even after users of the platform turned off its facial recognition feature), https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf.

35 *In the Matter of Cambridge Analytica, LLC*, Final Order, Dkt. No. 9383, Fed. Trade Comm'n, at 4 (Nov. 25, 2019) (ordering the company to "delete or destroy all Covered Information collected from consumers ... and any information or work product, including any algorithms or equations, that originated" from such consumers"), https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_orderpublic.pdf.

36 *In the Matter of Everalbum, Inc.*, File No. 192 3172, Fed. Trade Comm'n (May 6, 2021), https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf; *In the Matter of Cambridge Analytica, LLC*, Final Order, Dkt. No. 9383, Fed. Trade Comm'n (Nov. 25, 2019), https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_orderpublic.pdf.

37 Fed. Trade Comm'n, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/545A-FCRA-08-2022-508.pdf.

38 State of California Department of Justice, *California Consumer Privacy Act* (updated Feb 15, 2023), https://oag.ca.gov/privacy/ccpa.

amended by the California Privacy Rights Act (CPRA)),[39] Virginia Consumer Data Protection Act,[40] Colorado Privacy Act (COPA)[41], and Connecticut Data Privacy Act[42] grant applicable data subjects the right to opt out of automated decision-making. The concept of automated decision making differs slightly in each state's law, but generally includes technology that facilitates decisions made through, or otherwise uses, AI tools. In addition, each of these four states require companies using AI to conduct data privacy impact assessments to the extent a company's processing of personal information presents a "heightened risk of harm to a consumer." These data privacy impact assessments are not intended to be made public; rather they must be made available to each state's applicable regulator upon request. According to COPA's final regulations, companies using AI software must be transparent about how they use such AI and would need to make certain disclosures in their website privacy policies regarding how the company conducts "automated processing." The CPRA's draft regulations contain similar disclosure requirements.[43] The California Privacy Protection Agency (CPPA) is seeking comments for proposed rulemaking on automated decision-making technologies, which will likely impose additional requirements on covered entities. The Utah Consumer Privacy Act[44] does not provide Utah residents with a right to opt out of processing and does not require companies to conduct data privacy impact assessments.

EU/UK Privacy Considerations

The EU and UK General Data Protection Regulation (GDPR) mandate strict requirements for organizations processing personal data in the EU and UK, respectively. Financial institutions that plan to use AI software within

---

39 The California Privacy Rights Act and Enforcement Act of 2020, https://oag.ca.gov/system/files/initiatives/pdfs/19-0017%20%28Consumer%20Privacy%20%29.pdf (last visited Mar. 28, 2023) Cal. Civ. Code. § 1798.185(15) ("potential risks to … the consumers").

40 Virginia Consumer Data Protection Act (Jan 1, 2023) Va. Code § 59.1-580(5) ("heightened risk of harm to consumers"), https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/.

41 The requirements are as follows:

1. What decision(s) is (are) subject to Profiling;
2. The categories of Personal Data that were or will be Processed as part of the Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects;
3. A non-technical, plain language explanation of the logic used in the Profiling process;
4. A non-technical, plain language explanation of how Profiling is used in the decision making process, including the role of human involvement, if any;
5. If the system has been evaluated for accuracy, fairness, or bias, including the impact of the use of Sensitive Data, and the outcome of any such evaluation;
6. The benefits and potential consequences of the decision based on the Profiling; and
7. Information about how a Consumer may exercise the right to opt out of the Processing of Personal Data concerning the Consumer for Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects.

See Phil Weiser, Colorado Attorney General, *Colorado Privacy Act* (2023) Colo. Pub. Act No. 22-15 § 8 ("heightened risk of harm to a Consumer"), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf.

42 William Tong, The Office of the Attorney General, *Connecticut Data Privacy Act* (2022) Conn Sen Colo. Code Regs. § 8.02(A)("heightened risk of harm to a Consumer"), https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF.

43 The CPRA provides that the CPPA must issue regulations addressing "profiling," and indicates that covered entities responding to "access requests" must provide "meaningful information about the logic involved in such decision-making processes …" as well as a "description of the likely outcome of the process with respect to the consumer." Cal. Civ. Code. § 1798.185(16).

44 The Utah Consumer Privacy Act, https://le.utah.gov/~2022/bills/sbillenr/SB0227.pdf (last visited Mar. 28, 2023).

their technologies will want to do so with EU and UK GDPR requirements and fundamental principles in mind—including: (i) establishing a lawful basis for processing personal data when using AI software, which may include obtaining an individual's consent, processing further to an organization's legitimate interests or processing data to comply with legal requirements; (ii) only collecting and processing relevant personal data that is necessary for the intended purpose; (iii) ensuring individuals can exercise their rights under the EU and UK GDPR when their personal data is processed by AI software; and (iv) conducting Data Protection Impact Assessments (DPIAs) if the intended use of AI software is likely to pose a high-risk to the rights and freedoms of individuals. DPIAs help organizations identify, assess, and mitigate risks associated with data processing activities, including those involving AI software, and are a key part of accountability obligations under the EU and UK GDPR.

The EU's proposed Artificial Intelligence Act (AI Act) is intended to act in tandem with the EU GDPR, and aims to regulate AI systems developed, placed and used on European markets or which may affect individuals in the EU.[45] The AI Act will classify AI systems based on their potential risk to cause harm to individuals with three categories (i) unacceptable risk, (ii) high-risk and (iii) low or minimal risk. Where an AI system is classified as being high-risk, it will be subject to additional scrutiny and risk assessments that would likely increase compliance costs for organizations. For example, financial institutions looking to adopt a high-risk AI system may undergo a conformity assessment to verify compliance with the AI Act's requirements before the system is put into service. Further, the AI Act mandates that high-risk AI systems must have human oversight to prevent or minimize risks and effectively monitor AI systems for signs of potential dysfunction. Financial institutions may therefore be required to implement measures to provide that human intervention is available for AI software-generated content or decision-making processes, such as through a "stop" button or similar procedure. In addition, financial services firms must also have adequate quality management systems in place, such as procedures to report any incidents or malfunctions involving AI software to relevant national supervisory authorities.[46] As the AI Act is still in its infancy, we will continue to monitor its developments and potential impact on financial institutions deploying LLM-based AI systems, within their technologies.

Recent UK Developments

In the UK, the government is currently grappling with novel issues presented by AI tools and seeking to find a way to regulate them. This follows its trend of formulating a regulatory framework for other new digital technologies (*e.g.*, see *Dechert OnPoint* on recent proposals for the regulation of cryptoassets in the UK[47]). On March 29, 2023, the UK government published a white paper[48] which sets out its proposals for AI software. The government is seeking to balance public trust in AI tools, while creating a pro-innovation environment for businesses. The overall aim is to

---

45 *See* 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 (Apr. 04, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

46 Karen L. Neuman, Hilary Bonaccorsi, Michael P. Tierney, and Madeleine White, *European Commission's Proposed Regulation on Artificial Intelligence: Requirements for High-Risk AI Systems*, 4 J. OF ROBOTICS, ARTIFICIAL INTELLIGENCE & L. 443-44 (Nov.-Dec. 2021).

47 *Treating Crypto Fairly: The New UK Government Consults on a Comprehensive Regulatory Regime for Crypto* Assets, DECHERT LLP (Feb. 13, 2023) https://www.dechert.com/knowledge/onpoint/2023/2/treating-crypto-fairly--the-new-uk-government-consults-on-a-comp.html.

48 *See* "A pro-innovation approach to AI" (March 29. 2023) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1146542/a_pro-innovation_approach_to_AI_regulation.pdf

ensure that regulation does not hinder the development of AI. However, as explained below, the proposed regulatory regime may prove to be burdensome and unclear for financial institutions, and time will tell how the proposals develop in practice.

The future UK regulatory regime will be based on five pillars:

1. **Safety, security and robustness**: measures may need to be introduced for organizations to ensure that their AI systems are technically secure and function reliably.

2. **Transparency and explainability**: AI systems should be appropriately transparent and explainable, to increase public trust and allow for the regulations to have meaningful effect.

3. **Fairness**: AI systems should not undermine legal rights of individuals/organizations or create unfair market outcomes.

4. **Accountability and governance**: governance measures should be put in place to ensure effective oversight of the supply and use of AI systems, with clear lines of accountability established.

5. **Contestability and redress**: impacted parties should be able to contest an AI outcome that is harmful or creates a material risk of harm.

The UK government does not propose that an AI-specific regulator should be established. Instead, the proposal is to adapt the current UK system to cater for AI systems, by requiring various existing regulators such as the UK Financial Conduct Authority and Information Commissioner's Office to adjust their rules accordingly. Without further details of how this will work in practice, this might appear to be an unwieldy task which gives rise to inconsistencies in approach and financial institutions may be burdened with trying to ensure that they are complying with a variety of AI-related regulations. Perhaps with this in mind, governmental functions will be put in place to coordinate, monitor and adapt the framework. Further, the UK government recognizes the need for AI assurance techniques (*i.e.*, practical tools for financial institutions to aid governance of and compliance with the UK's AI regulatory principles) and the UK is establishing the 'UK AI Standards Hub' to assist businesses in this regard.

Financial institutions will therefore need to be alert to the risks posed by their AI systems and ensure appropriate systems and controls are in place to mitigate any potential harm, including providing appropriate training to their staff. That work should start promptly as UK regulators will soon be increasing their spotlight on issues relating to AI tools.

Cybersecurity Considerations

The proliferation of AI-based technologies generally, and the use of AI software specifically, pose certain unique challenges from a cybersecurity perspective. Financial institutions using AI software need to be aware of, and take measures to protect against, the following risks, among others:

- **Data Breaches**. AI software collects a tremendous amount of data from users and permits companies to put confidential and client information in its systems. As such, companies need to be aware of the heightened potential for data breaches to occur and take measures to prepare for and mitigate such breaches.

- **Data Poisoning**. Individuals could tamper with a financial institution's trained datasets, which could affect the decisions that AI makes, or the responses that AI software gives users, thereby reducing their accuracy. As described above, AI software is based on word association, and does not include an independent fact

checking feature. By incorporating incorrect data into the data used to train AI software, the system could learn incorrect patterns.

- **Compromised Trade Secrets or Confidential Information**. Sensitive company information, including trade secrets and other confidential information (i.e., financial information, intellectual property, etc.) could become ingested into a company's AI model and reproduced upon demand by AI software. This could happen in a number of ways, including through employees feeding this information (either accidently or maliciously) into the model or outside threat actors who penetrate a company's information technology systems intentionally seeking to expose certain company information.

- **Use by Threat Actors to Launch Attacks**. Threat actors can use AI tools to launch attacks, create language for phishing emails that appear convincing and realistic, or to query data bases to generate spam or create sophisticated social engineering attacks. In addition, there are unknown and infinite uses in terms of aiding threat actors in perpetrating brute force and other attacks as the AI gets more sophisticated.

- **Use by Threat Actors to Breach Accounts**. LLM-based AI software can be used to make sophisticated guesses of user passwords or other sensitive information by asking it to query publicly available information or social media data.

Conclusion

Financial institutions that adopt innovative and disruptive technology to improve their products and services offerings in the coming months will need to take appropriate steps to ensure they remain on the right side of lines yet to be drawn by US and international regulators. Recent enforcement actions in the US regarding messaging apps like WhatsApp demonstrate an alternative to how financial institutions adopt and implement new technologies with respect to record-retention and client communication.[49]

Although US and international regulators have not yet proposed or implemented new regulations specifically directed at AI use by financial institutions, it is likely that regulators will take a closer look as AI use continues to increase. AI tools will also continue to play a larger and larger role in the workforces of banks, fund managers, broker-dealers and investment firms. It will be imperative for lawyers advising on key decisions to fully consider the legal and regulatory implications of each new use case.

[49] See Press Release, Sec. and Exch. Comm'n, SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures (Sep. 27, 2022), https://www.sec.gov/news/press-release/2022-174; Press Release, Commodities Future Trading Comm'n, CFTC Orders 11 Financial Institutions to Pay Over $710 Million for Recordkeeping and Supervision Failures for Widespread Use of Unapproved Communication Methods (Sep. 27, 2022), https://www.cftc.gov/PressRoom/PressReleases/8599-22.

This update was authored by:

Linda Ann Bartosch
Partner
Philadelphia
+1 215 994 2132
lindaann.bartosch@dechert.com

K. Susan Grafton
Partner
Washington, D.C., New York
+1 202 261 3399
susan.grafton@dechert.com

Paul Kavanagh
Partner
London
+44 20 7184 7510
paul.kavanagh@dechert.com

Daniel Natoff
Partner
London
+44 20 7184 7676
daniel.natoff@dechert.com

Mark D. Perlow
Partner
San Francisco
+1 415 262 4530
mark.perlow@dechert.com

Corey F. Rose
Partner
Washington, D.C.
+1 202 261 3314
corey.rose@dechert.com

Brenda R. Sharton
Partner
Boston
+1 617 728 7113
brenda.sharton@dechert.com

Timothy Spangler
Partner
Los Angeles | +1 949 442 6044
Silicon Valley | +1 650 813 4803
timothy.spangler@dechert.com

Robert J. Rhatigan
Counsel
Washington, D.C.
+1 202 261 3329
robert.rhatigan@dechert.com

Audrey Wagner
Counsel
Washington, D.C.
+1 202 261 3365
audrey.wagner@dechert.com

Katherine Hurley
Associate
Boston
+1 617 728 7126
katherine.hurley@dechert.com

Michael McGrail
Associate
Boston
+1 617 728 7140
michael.mcgrail@dechert.com

James Smith
Associate
Washington, D.C.
+1 202 261 3362
james.smith@dechert.com

Lucy Yang
Associate
San Francisco
+1 415 262 4520
lucy.yang@dechert.com