What is Fair: Enforcement Trends Concerning the Use of Consumer Data

July 13, 2022

ACC Association of Corporate Counsel

JENNER&BLOCK

CHICAGO | LONDON | LOS ANGELES | NEW YORK | SAN FRANCISCO | WASHINGTON, DC | JENNER.COM

Presenters

Ali M. Arain

Partner
Jenner & Block

Michael W. Ross

Partner
Jenner & Block

Bernadette Walli

Senior Counsel, Regulatory Affairs
Mastercard

This publication is not intended to provide legal advice but to provide information on legal matters and firm news of interest to our clients and colleagues. Readers should seek specific legal advice before taking any action with respect to matters mentioned in this publication. The attorney responsible for this publication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome.

Agenda

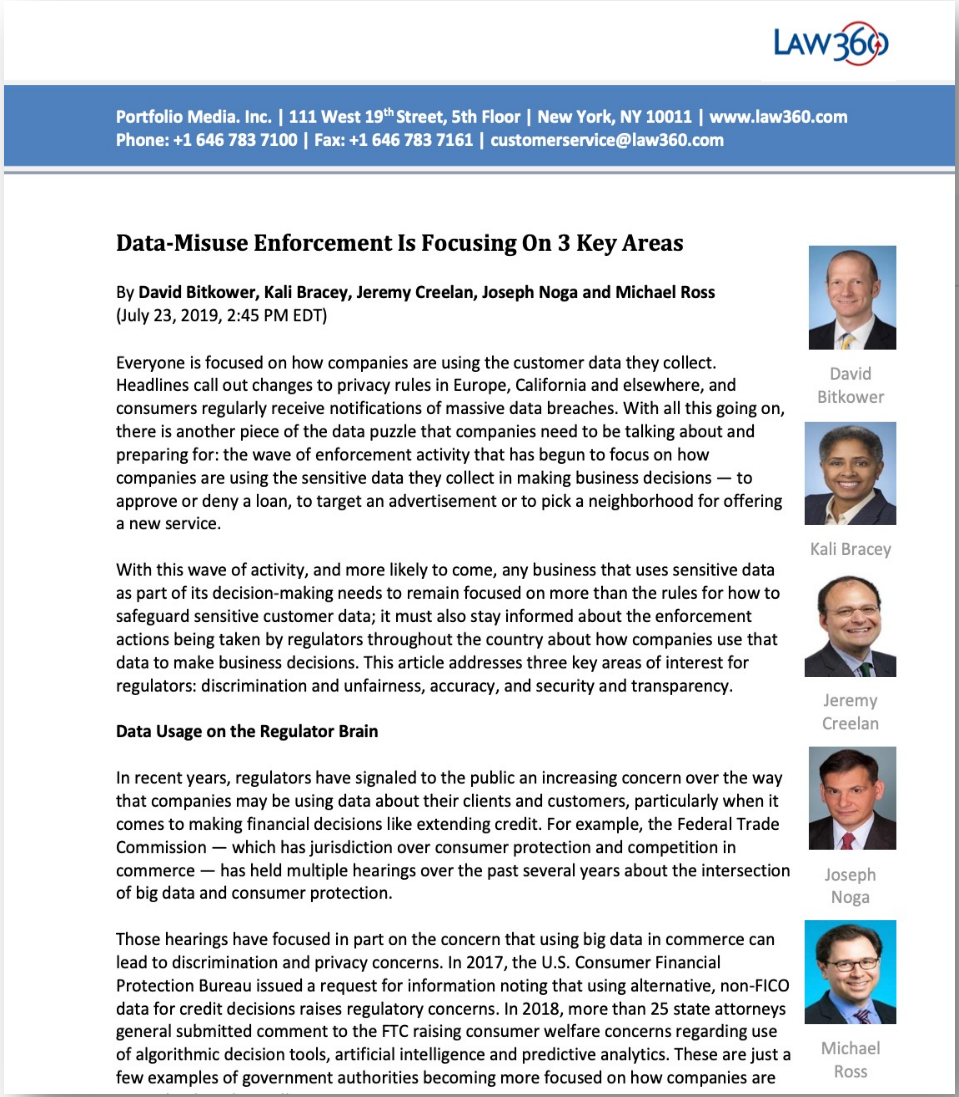
- Overview
- Discrimination and Unfairness
- Security and Transparency
- Accuracy

Overview

Data Use is a Hot Topic for Regulators

- Regulators are no longer *discussing* their growing concern related to the use of data but are taking substantial affirmative actions.
- Federal and state regulators have issued dozens of advisory opinions, RFIs, and new regulations in addition to filing enforcement actions related to big data, algorithmic decision-making, and artificial intelligence (AI).

- Agencies include:
  - Department of Justice (DOJ)
  - Department of Housing and Urban Development (HUD)
  - Federal Trade Commission (FTC)
  - Consumer Financial Protection Bureau (CFPB)
  - Securities and Exchange Commission (SEC)
  - Equal Employment Opportunity Commission (EEOC)
  - Office of the Comptroller of the Currency (OCC)
  - Federal Deposit Insurance Corporation (FDIC)
  - National Credit Union Administration (NCUA)
  - New York State Department of Financial Services



LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Data-Misuse Enforcement Is Focusing On 3 Key Areas

By **David Bitkower, Kali Bracey, Jeremy Creelan, Joseph Noga and Michael Ross**
(July 23, 2019, 2:45 PM EDT)

David Bitkower

Kali Bracey

Jeremy Creelan

Joseph Noga

Michael Ross

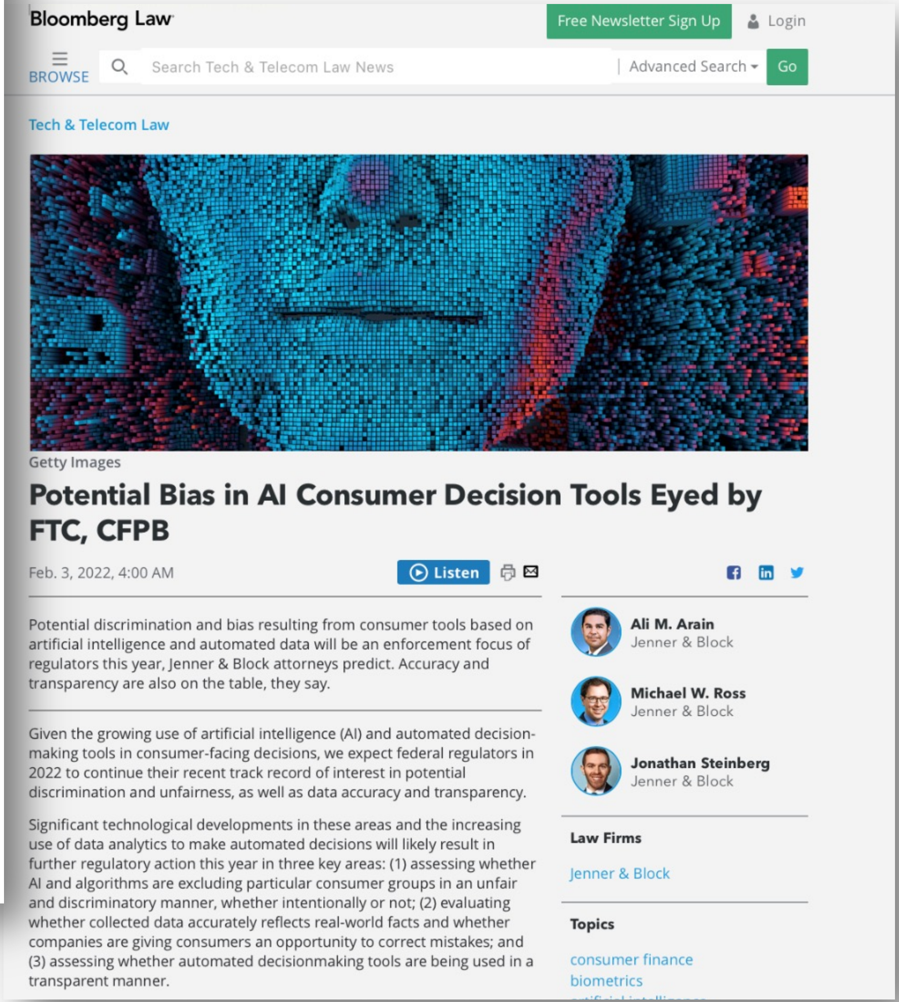
Everyone is focused on how companies are using the customer data they collect. Headlines call out changes to privacy rules in Europe, California and elsewhere, and consumers regularly receive notifications of massive data breaches. With all this going on, there is another piece of the data puzzle that companies need to be talking about and preparing for: the wave of enforcement activity that has begun to focus on how companies are using the sensitive data they collect in making business decisions — to approve or deny a loan, to target an advertisement or to pick a neighborhood for offering a new service.

With this wave of activity, and more likely to come, any business that uses sensitive data as part of its decision-making needs to remain focused on more than the rules for how to safeguard sensitive customer data; it must also stay informed about the enforcement actions being taken by regulators throughout the country about how companies use that data to make business decisions. This article addresses three key areas of interest for regulators: discrimination and unfairness, accuracy, and security and transparency.

Data Usage on the Regulator Brain

In recent years, regulators have signaled to the public an increasing concern over the way that companies may be using data about their clients and customers, particularly when it comes to making financial decisions like extending credit. For example, the Federal Trade Commission — which has jurisdiction over consumer protection and competition in commerce — has held multiple hearings over the past several years about the intersection of big data and consumer protection.

Those hearings have focused in part on the concern that using big data in commerce can lead to discrimination and privacy concerns. In 2017, the U.S. Consumer Financial Protection Bureau issued a request for information noting that using alternative, non-FICO data for credit decisions raises regulatory concerns. In 2018, more than 25 state attorneys general submitted comment to the FTC raising consumer welfare concerns regarding use of algorithmic decision tools, artificial intelligence and predictive analytics. These are just a few examples of government authorities becoming more focused on how companies are



Getty Images

Potential Bias in AI Consumer Decision Tools Eyed by FTC, CFPB

Feb. 3, 2022, 4:00 AM

Ali M. Arain
Jenner & Block

Michael W. Ross
Jenner & Block

Jonathan Steinberg
Jenner & Block

Law Firms

Jenner & Block

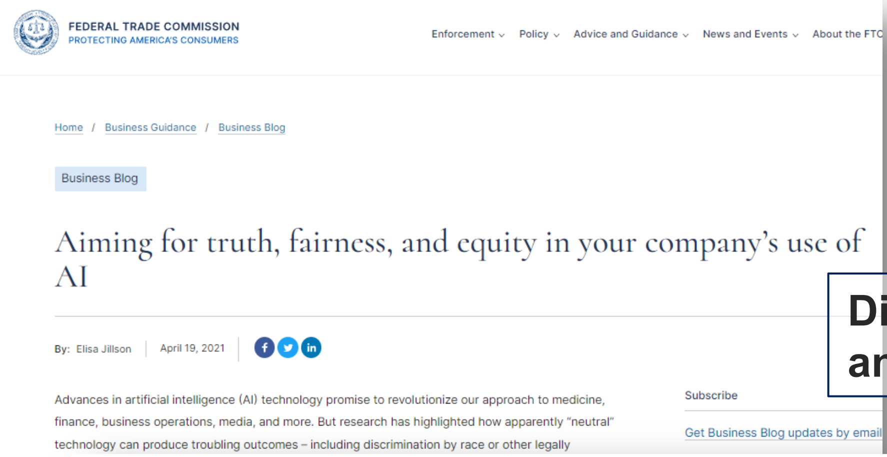
Topics

consumer finance
biometrics

Potential discrimination and bias resulting from consumer tools based on artificial intelligence and automated data will be an enforcement focus of regulators this year, Jenner & Block attorneys predict. Accuracy and transparency are also on the table, they say.

Given the growing use of artificial intelligence (AI) and automated decision-making tools in consumer-facing decisions, we expect federal regulators in 2022 to continue their recent track record of interest in potential discrimination and unfairness, as well as data accuracy and transparency.

Significant technological developments in these areas and the increasing use of data analytics to make automated decisions will likely result in further regulatory action this year in three key areas: (1) assessing whether AI and algorithms are excluding particular consumer groups in an unfair and discriminatory manner, whether intentionally or not; (2) evaluating whether collected data accurately reflects real-world facts and whether companies are giving consumers an opportunity to correct mistakes; and (3) assessing whether automated decisionmaking tools are being used in a transparent manner.



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement ⌄ Policy ⌄ Advice and Guidance ⌄ News and Events ⌄ About the FTC

Home / Business Guidance / Business Blog

Business Blog

Aiming for truth, fairness, and equity in your company's use of AI

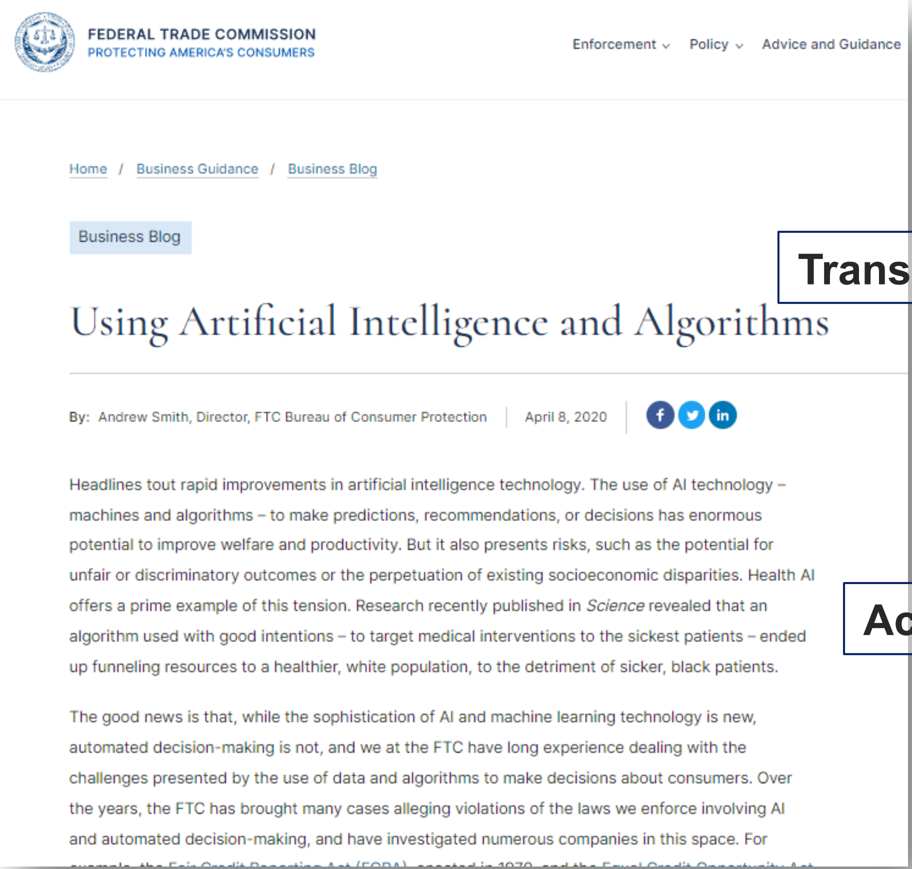
By: Elisa Jillson | April 19, 2021

Advances in artificial intelligence (AI) technology promise to revolutionize our approach to medicine, finance, business operations, media, and more. But research has highlighted how apparently "neutral" technology can produce troubling outcomes – including discrimination by race or other legally pro

viru tha wo Th oth att

Subscribe

Get Business Blog updates by email



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Home / Business Guidance / Business Blog

Business Blog

Using Artificial Intelligence and Algorithms

By: Andrew Smith, Director, FTC Bureau of Consumer Protection | April 8, 2020

Headlines tout rapid improvements in artificial intelligence technology. The use of AI technology – machines and algorithms – to make predictions, recommendations, or decisions has enormous potential to improve welfare and productivity. But it also presents risks, such as the potential for unfair or discriminatory outcomes or the perpetuation of existing socioeconomic disparities. Health AI offers a prime example of this tension. Research recently published in *Science* revealed that an algorithm used with good intentions – to target medical interventions to the sickest patients – ended up funneling resources to a healthier, white population, to the detriment of sicker, black patients.

The good news is that, while the sophistication of AI and machine learning technology is new, automated decision-making is not, and we at the FTC have long experience dealing with the challenges presented by the use of data and algorithms to make decisions about consumers. Over the years, the FTC has brought many cases alleging violations of the laws we enforce involving AI and automated decision-making, and have investigated numerous companies in this space. For example, the Fair Credit Reporting Act (FCRA), enacted in 1970, and the Equal Credit Opportunity Act

Discrimination and Unfairness

- Ensure that your decisions are fair.
- Hold yourself accountable for compliance, ethics, fairness, and nondiscrimination.

Transparency

- Be transparent.
- Explain your decision to the consumer.

Accuracy

- Ensure that your data and models are robust and empirically sound.

What are the Issues?

- Three main areas of regulatory concern

Discrimination and Unfairness

Security and Transparency

Accuracy

Discrimination and Unfairness

Discrimination and Unfairness – Overview

Risks

- Using data analytics to intentionally target or exclude particular consumer groups
- Using data analytics to make decisions that have disparate impact on particular groups
- Example: Zip code as a proxy for race

Laws to Highlight

- Fair Housing Act (FHA)
- Equal Credit Opportunity Act (ECOA)
- Federal Trade Commission Act (FTC Act) and state Unfair or Deceptive Acts or Practices (UDAP) laws
- Consumer Financial Protection Act (UDAAP)

Fair Housing Act (FHA)

- The FHA prohibits discrimination in any aspect of the sale or rental of a dwelling, the acquisition of home financing, and other housing-related activities based on:
  - Race or color
  - Religion
  - National origin
  - Sex
  - Familial status
  - Disability
- The FHA anti-discrimination provisions apply, in the advertising context, both to persons who place real estate-related advertisements and to the publishers, such as online portals, who provide them to potential consumers.

Equal Credit Opportunity Act (ECOA)

- ECOA prohibits discrimination in any aspect of a credit decision based on an applicant’s:
  - Race or color
  - Religion
  - National origin
  - Sex
  - Marital status
  - Age (as long as the applicant has the capacity to contract)
  - Receipt of income derived from any public assistance program
  - Exercise, in good faith, of any right under Consumer Credit Protection Act

- ECOA applies to any decision regarding credit extension, including to small businesses, corporations, partnerships, and trusts.

Unfair or Deceptive Acts or Practices (UDAP)

- FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce” 15 U.S.C. § 45(a).

- Factors relevant to whether practice is “unfair”:
  - If practice “causes or is likely to cause substantial injury to consumers” that is not outweighed by any countervailing benefits to consumers and that consumers themselves could not reasonably have avoided; and
  - “[E]stablished public policies,” although “public policy considerations may not serve as a primary basis for [an unfairness] determination.” Id. § 45(n)

- Combatting Disparate Impact
  - One “established public policy” in statute and case law that FTC may consider in an “unfairness” determination is anti-discrimination (e.g., Civil Rights Act of 1964; ECOA; Fair Housing Act)
  - Less tested application of these laws

- Many state UDAP laws employ the same / similar approach.

Consumer Financial Protection Act (CFPA)

- Consumer Financial Protection Act (CFPA or Dodd-Frank) prohibits any provider of consumer financial products or services from engaging in any unfair, deceptive, or abusive act or practice (UDAAP).

- The standard for unfairness under the Dodd-Frank Act is that an act or practice is unfair when:
  - (1) It causes or is likely to cause substantial injury to consumers;
  - (2) The injury is not reasonably avoidable by consumers; and
  - (3) The injury is not outweighed by countervailing benefits to consumers or to competition.

- Dodd-Frank provides the CFPB with rule-making authority as well as supervisory authority to detect and assess risks to consumers and to markets for consumer financial products and services.

Discrimination and Unfairness – Sources

Category	Source
Lending	• CFPB Advisory Opinion and Consumer Financial Protection Circular on ECOA and Regulation B Coverage (May 2022): Affirms that ECOA protects people from discrimination in all aspects of the credit lifecycle – *i.e.,* not only during the application process, but also *after* borrowers have received credit. The Advisory Opinion underscores that the ECOA requires lenders to provide “adverse action notices” to borrowers explaining why an unfavorable decision was made. Subsequently, the Circular highlighted that the ECOA applies regardless of the technology or data tools used to make the lending decisions. • CFPB Automated Valuation Model (AVM) Rulemaking Proposal (Feb. 2022): The CFPB recently published a 42-page outline of possible rulemaking designed to: (1) ensure a high level of confidence in AVM estimates; (2) protect against the manipulation of data; (3) avoid conflicts of interest; and (4) require random sample testing and reviews. In addition, federal regulators are considering whether to include explicit nondiscrimination quality control requirements as a “fifth factor.” Once adopted, the new rules would apply to banks and mortgage lenders who use AVMs to make underwriting decisions, and mortgage-backed securities issuers. • CFPB Inquiry into “Buy Now, Pay Later” (BNPL) (Dec. 2021): CFPB launched a market monitoring inquiry into BNPL lenders’ data collection practices, behavioral targeting, data monetization, and the corresponding risks the industry poses for US consumers. The Bureau issued orders to obtain information from Affirm, Afterpay, Klarna, PayPal, and Zip. The CFPB highlighted their concern about consumers who accumulate debt from multiple BNPLs as well as the disuniformity of BNPL data furnishing practices to national consumer reporting companies.

Discrimination and Unfairness – Sources

Category	Source
Lending (cont'd)	• Interagency Combatting Redlining Initiative (Oct. 2021): DOJ, CFPB, and the Office of the Comptroller of the Currency announced initiative to combat discriminatory redlining. The agencies announced plans to proactively monitor for redlining practices of depository and non-depository lenders and take action against "modern day" digital and algorithmic redlining that reinforce long existing biases. • KleinBank (May 2018): Settlement resolving Department of Justice (DOJ) allegations of "redlining" – *i.e.*, intentionally avoiding providing lending services to individuals living in predominantly minority neighborhoods. • Bancorp South Bank (July 2016): Settlement resolving DOJ allegations of redlining and pricing discrimination in mortgage lending. • FTC Report (Jan. 2016): Lenders cannot make decisions based on an applicant's zip code if doing so has disparate impact on protected class (*e.g.*, race, national origin). • Franklin Acceptance Corp. (May 1999): Settlement resolving FTC allegations of marital status discrimination, where company excluded/discounted applicant's income from child support payments and failed to aggregate incomes of unmarried co-applicants (but aggregated married applicants).

Discrimination and Unfairness – Sources

Category	Source
Advertising/ Marketing	• DOJ /Meta Settlement on Algorithmic Bias (June 2022): DOJ and Meta settlement resolving allegations of discriminatory algorithmic in advertising by Meta Platforms Inc. The lawsuit alleged that Meta's housing advertisement targeting and delivery system resulted in "disparate treatment and disparate impact discrimination" under the Fair Housing Act (FHA). Under the settlement terms, Meta will stop using certain housing advertising tools and will develop a new system to address racial and other disparities that result from the company's use of personalized algorithms for housing ad delivery. • Facebook (July 2019): NY DFS stated that it would investigate Facebook after reports that Facebook's platform allowed advertisers to discriminate using user's geographic data as a proxy for protected categories. • Facebook (Mar. 2019): HUD alleged that Facebook violated the FHA "by encouraging, enabling, and causing housing discrimination through the company's advertising platform." This enforcement action came just 10 days after Facebook settled five lawsuits related to allegedly discriminatory advertising practices, a reminder that settling lawsuits with private plaintiffs is no guarantee that a federal or state regulator will not bring its own, separate action. • FTC Report (Jan. 2016): The FTC stated that data analytics may reflect that members of a particular group (*e.g.*, unmarried women) are more likely to apply for less attractive credit products; potential liability for advertising only those less attractive products to that group, if it leads to members of the protected group obtaining only those less attractive products.

Discrimination and Unfairness – Sources

Category	Source
Advertising/ Marketing (cont'd)	• Hudson City Savings Bank (Sept. 2015): Consent order resolving DOJ/CFPB allegations that a bank limited marketing of its loan products to neighborhoods with relatively few Black and Hispanic residents, thereby discouraging prospective Black and Hispanic borrowers.
Sale of Data	• FTC Report (Jan. 2016): May be "unfair" for company to provide data to customers that use it for discriminatory purpose. • Sequoia One (Aug. 2015): Settlement resolving FTC claim that data broker sold personal information of financially distressed payday loan applicants to scam operation that debited millions of dollars from their bank accounts and charged their credit cards without consent. • ChoicePoint (Jan. 2006): Settlement resolving FTC claims that data broker sold personal information to identity thieves, despite red flags of potential fraud, and requiring data broker to implement new compliance procedures. ChoicePoint later violated that settlement order.
Other Consumer	• CFPB Adds "Discrimination" to its "Unfair, Deceptive, or Abusive Acts and Practices" ("UDAAP") Examination Guidance (Mar. 2022): The Bureau announced its intent to address discrimination as an "unfair practice" under the Consumer Financial Protection Act (commonly known as Dodd-Frank). Specifically, by indicating that discrimination falls within "unfair practices" in its Exam Manual, the CFPB has authorized its examiners to look "beyond discrimination directly connected to fair lending laws" and ask companies to "review any policies or practices that exclude individuals from products and services, or offer products or services with different terms, in an unfairly discriminatory manner."

Discrimination and Unfairness – Sources

Category	Source
Other Consumer	• EEOC Initiative on Algorithmic Fairness in Hiring and other Employment Decisions (Oct. 2021; May 2022): Launched an effort to assess how AI and other data-driven tools are used in the employment context and whether these uses comply with federal civil rights law. In May, the EEOC issued guidance highlighting how employers may be liable under the Americans with Disabilities Act (ADA) if their data-driven hiring tools "screen out" disabled candidates where a "reasonable accommodation" would be required under the law. • Amazon (Apr. 2016): Failed to offer same-day delivery service to certain majority-minority neighborhoods in New York and other cities; claims of racial discrimination by using geography as proxy for race, although not obvious statutory violation. US Rep. Bobby Rush (D-IL) issued a letter to the FTC, arguing that Amazon's conduct might be "unfair" business practice under the FTC Act and violation of Civil Rights Act of 1964. Amazon voluntarily expanded same-day delivery service to minority neighborhoods before any regulatory action taken.

Discrimination and Unfairness – Sources

Category	Source
Other Key Sources	• FTC Report to Congress on Using AI to Combat Online Harms (June 2022): The report is a response to 2021 legislation that directed the FTC to study how AI may be employed to address online fraud, impersonation scams, fake reviews and accounts, bots, media manipulation, illegal drug sales and other illegal activities, sexual exploitation, hate crimes, online harassment and cyberstalking, and misinformation campaigns. The FTC greatly cautioned Congress in viewing AI as a solution to the spread of harmful content and outlines the limitations of AI tools (e.g., AI tools can be inaccurate, biased, and discriminatory by design). • Termination of Upstart No-Action Letter (June 2022): CFPB issued an order terminating a 2017 no-action letter (NAL) that was put in place to address gaps in the company's AI-based model for making underwriting and pricing decisions. The NAL required Upstart to inform the CFPB of any changes to its AI model. In April 2022, Upstart informed the Bureau it was adding several new variables to its underwriting and pricing model. With the NAL no longer in effect, CFPB is released from the letter's restriction that prevented the Bureau from making supervisory findings or bringing an enforcement action against Upstart under the ECOA, Regulation B, or the Bureau's UDAAP authority for discriminatory conduct.

Discrimination and Unfairness – Sources

Category	Source
Other Key Sources (cont'd)	• FTC Compulsory Process Resolution Regarding Algorithm Bias (Sept. 2021): FTC identified "technology companies and digital platforms," "bias in algorithms and biometrics," and "deceptive and manipulative conduct on the Internet" as among its top enforcement priorities for the coming years and directed staff to use compulsory processes to demand documents and testimony to investigate potential abuses in these areas. • CFPB Report (June 2019): The CFPB noted that "[t]he use of alternative data and modeling techniques may expand access to credit or lower credit cost and, at the same time, present fair lending risks." The agency recommended supervisory reviews of credit-scoring models and stated that an area of enforcement focus was use of models to predict recovery outcomes in collecting credit card and auto loan debts. • The Government Accountability Office (GAO) Report (Dec. 2018): The GAO reported that the CFPB and federal banking regulators are monitoring use of alternative data by collecting information and developing reports, but have not provided specific guidance on using the data. The reliability of alternative data was deemed one of the risks, and the GAO called upon multiple federal agencies to address the appropriate use of this data in underwriting. • Federal Reserve of Philadelphia Report (July 2017): The Federal Reserve of Philadelphia published a report analyzing Lending Club's data, which concluded that the use of alternative data sources, such as payment history, insurance claims and social networks, expanded access to lower-priced credit.

Discrimination and Unfairness – Enforcement

Category	Source
State and Local Actions	• NYC Law on Preventing Bias in Employment Decisions (Nov. 2021): Going into effect in 2023, the law will govern how AI and data tools are used in employment hiring and promotion processes. The legislation requires NYC employers using automated employment decision tools and software to notify candidates of these practices, and to conduct annual bias audits and make audit results publicly available. Violations will result in an initial $500 penalty for each violation, and $500 to $1,500 penalties for each day the violating tool is subsequently used. • Colorado Law to Restrict Insurers' Use of Consumer Data and Algorithms (2021): Colorado enacted a law that directs the state's Commissioner of Insurance to promulgate rules regulating insurer's use of algorithms and predictive models that rely on external consumer data that may result in discrimination based on "race, color, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity, or gender expression." The law noted that external consumer data includes social media habits, educational attainment, location data, purchasing habits in addition to others. • UnitedHealth's Algorithm-based Discrimination (Oct. 2019): New York State Departments of Financial Services and Health jointly sent a letter to UnitedHealth Group after a study found racial biases in the company's data analytics program. Specifically, the study found that an algorithm intended to provide data on which patients would benefit from complex health procedures favored treating white patients over sicker Black patients.

Discrimination and Unfairness – Lessons

- Keep these issues top of mind when giving advice to your clients.
- Ensure proper “tone from the top” (board/senior management).
  - Clear anti-discrimination messaging (*e.g.*, policy statements)
  - Allocation of resources for development and testing
  - Periodic reporting to board/senior management
- Consider self-monitoring regimes for business activities. A program could include:

Monitoring Program
1. Training
2. Process for: (a) review of data inputs; (b) back-end review of whether loans/services disproportionately impact certain groups/communities
3. Proper oversight of and response to validation testing • Compliance officer(s) responsible for ensuring lending and service-offering decisions are fair and non-discriminatory • Process for recording and reviewing results of validation testing • Process for identifying takeaways and implementing changes

Security and Transparency

Security and Transparency – Overview

Risks

- Failing to **reasonably safeguard** sensitive consumer data
- Making **inaccurate or misleading** statements about data protection practices
- Making service-related data-driven decisions without adequately disclosing the data used or reasoning behind a given service-related decision

Laws to Highlight

- FTC Act and State UDAP Laws

Security and Transparency – Overview

- Broad Enforcement
  - The FTC has brought hundreds of enforcement actions related to consumer privacy and data security.
  - State AGs have broad enforcement authority and may partner with FTC.
  - Growing push for state regulators to address privacy, data protection, and cybersecurity.
  - CFPB and FTC use of wide-ranging RFIs to greatly expand agency knowledge of industry data and AI practices.

Security and Transparency

- Potential Theories of Liability
  - Failure to provide meaningful information about the use of automated decisionmaking or profiling.
  - Failure to obtain consent (if required) for automatic data collection, particularly when combining data from multiple sources or from third parties.
  - Use of facial recognition for payment may implicate both biometric and payments legal/regulatory regimes.
  - Insufficient disclosures when collecting new types of sensitive data.

Security and Transparency – Sources

Category	Source
Failure to Secure **Data**	- FTC Signals New Data Breach Disclosure Obligations (May 2022): FTC declares that failures to disclose a data breach may be a violation of Section 5 of the FTC Act. This new disclosure requirement, articulated in a recent blog post, signals the FTC's plans to exercise its enforcement authority to impose additional scrutiny around data breach notification—including the timing and accuracy of the disclosure. - FDIC Computer-Security Incident Notification Rule (April 2022): The FDIC's final rule governing how banks and "bank service providers" respond to computer-security incidents took effect in April 2022. The Rule requires banks to notify government agencies of an incident within 36 hours and for bank service providers to notify at least one designated contact as soon as possible. The Rule applies to "notification incidents"—those incidents that have "materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's: "(1) ability to carry out banking activity affecting a material portion of the customer base, (2) lines of business that would result in a material loss of revenue, and (3) operations whose "failure or discontinuance of which would pose a threat to the financial stability of the United States." The FDIC provided the following examples: "a major computer-system failure; a cyber-related interruption, such as a distributed denial of service or ransomware attack; or another type of significant operational interruption."

Security and Transparency – Sources

Category	Source
Failure to Secure Data (cont'd)	• CafePress (March 2022): FTC reached a $500,000 settlement with CafePress, an e-commerce platform, for failing to inform consumers of multiple data breaches and allegedly attempting to cover them up. The complaint alleges that CafePress was aware of the data security problems prior to a 2019 breach and failed to inform consumers until the breach was widely reported. In addition to paying the settlement amount, the companies that own CafePress must implement new information security programs, replace inadequate authentication measures, and notify consumers whose personal information was compromised and inform them of how they can protect themselves going forward. • Spyfone (Sept. 2021): FTC banned SpyFone from the surveillance business after allegations that it secretly harvested and shared people's private information through a device hack. The company's app sold real-time access to the company's secret surveillance department, allowing stalkers, domestic abusers, hackers, and identity thieves to stealthily track potential targets. The FTC alleged that the company also failed to implement basic security protocols such as encrypting private information, restricting personal information to authorized users, and protecting consumers' passwords. • SkyMed International, Inc. (Feb. 2021): FTC reached a settlement with SkyMed, an emergency travel service provider, over the company's failure to secure a cloud-based database containing 130,000 member records, many of which included sensitive health information. The Commission also alleged that SkyMed deceived consumers by displaying a "HIPAA Compliance" seal on its webpage, which gave the false impression that its policies were compliant with HIPAA requirements.

Security and Transparency – Sources

Category	Source
Failure to Secure Data (cont'd)	• Equifax (July 2019): $575 Million settlement with FTC, CFPB, and States involving the company's failure to secure data, leading to a 2017 breach that compromised the personal information of over 140 million people. The FTC alleged that Equifax failed to take reasonable steps to enforce security when it was first notified of a vulnerability in its system. According to the Commission, the company violated the FTC Act's prohibition against unfair and deceptive practices and the Gramm-Leach-Bliley Act's Safeguards Rule, which requires financial institutions to develop and maintain comprehensive safeguard systems that "protect the security, confidentiality, and integrity of customer information." • Uber (Apr. 2018): $148 million expanded settlement after Uber failed to disclose a second data breach that occurred in 2016 while the company was in the midst of an FTC investigation related to a similar 2014 data breach that resulted in the initial 2017 settlement. The FTC alleged that Uber failed to disclose a breach of its consumer data stored on a third-party cloud provider's servers. Intruders were able to download 25 million names and email addresses, 22 million names and mobile phone numbers, and 600,000 names and driver's license numbers of US Uber drivers and riders.

Security and Transparency – Sources

Category	Source
Failure to Secure Data (cont'd)	• Oracle (2016): The FTC alleged that, despite being aware of major security issues with prior versions of its software, Oracle failed to inform consumers that updating their software may have left these potentially vulnerable versions of the software intact. • *FTC v. Wyndham Worldwide Corporation* (2015): The FTC filed complaint against Wyndham, alleging that it misrepresented its security practices and failed to safeguard consumers' personal information. • Fandango and Credit Karma (2014): Failure to secure mobile applications by overriding or disabling default validation processes to transmit information securely.
Failure to Disclose Collection & Data Misuse	• Twitter (May 2022): The FTC lodged a $150 million penalty against Twitter for violating a 2011 FTC Order addressing the company's failures to protect user privacy and confidentiality, and for deceptively using account security data (users' phone numbers and email addresses) for targeted advertising. The DOJ's complaint alleges that Twitter misled its users by requesting that they disclose their phone numbers and email addresses for security purposes and then shared this data with advertisers to target specific users. • FTC Staff Report on Internet Service Providers (Oct. 2021): Following up on orders sent to six internet service providers (ISPs) that cover 98 percent of the mobile internet market (AT&T, Cellco, Charter, Comcast, T-Mobile, Google Fiber), the report found that many ISPs collect and share data across product lines, combine app and web browsing data for ad targeting, and share real-time location data with third parties. Moreover, many of the ISPs claim that consumers have a choice in how their data is used, but make it exceedingly difficult to exercise that choice, and in some cases, nudge consumers to share more data.

Security and Transparency – Sources

Category	Source
Failure to Disclose Collection & Data Misuse (cont'd)	• OpenX Technologies, Inc. (Dec. 2021): $2 million settlement with the FTC for allegedly collecting personal information from children under 13 without parental consent, a violation of federal children's privacy protection law. The company also allegedly stored geolocation information from users who specifically declined to be tracked. • WW International, Inc. (March 2022): $1.5 million FTC settlement fining WW International (formerly known as Weight Watchers) and its app, Kurbo, a weight loss app for use by children as young as eight, for collecting children's personal data. In addition to paying a penalty, WW was ordered to delete the data and destroy any algorithms derived from the data. • Upromise, Inc. (2012, 2017): Upromise settled with the FTC over claims of failure to disclose the extent of its data collection—including web browsing history, search terms, user names, passwords, payment card numbers, and Social Security numbers—and failure to take reasonable measures to protect consumer data. In 2017, the FTC brought a civil penalty action against Upromise for violating the 2012 order. • InMobi (2016): FTC alleged that mobile advertising company tracked geolocation of hundreds of millions of consumers despite statements in its software claiming that consumers would only be tracked when they opted in.

Security and Transparency – Sources

Category	Source
Third Parties	- Lenovo (2017): Failure to disclose software pre-installed on Lenovo computers, which functioned as "man-in-the-middle" between consumers and all websites, and transmitted data to an advertising company.
Other	- FTC Orders (2019): The FTC announced that they have "improved" their recent data security orders by requiring more specific data security programs, requiring more accountability from third-party assessors, and emphasizing executive accountability.

Security and Transparency – Sources

Category	Source
RFIs	• CFPB RFI related to Tech Payment Systems (Oct. 2021): CFPB sent orders to Amazon, Apple, Facebook, Google, PayPal, and Square requesting information on how the platforms use personal payment data and manage data access. Specifically, the orders related to data harvesting and monetization, access restrictions and user choice, and consumer protections related to fraud and privacy. • CFPB RFI on Financial Institutions' Use of Artificial Intelligence (May 2021): CFPB along with the FDIC, National Credit Union Admin, and the Office of the Comptroller of the Currency announced an RFI seeking information on the use of AI by financial institutions, AI governance within these institutions, risk management and controls, and their challenges related to developing, adopting, and managing data-driven AI tools. • FTC Orders to Social Media and Video Streaming Providers (Dec. 2020): FTC issued orders to nine social media and video streaming companies related to their data use and collection practices as well as their advertising and user engagement practices. The companies include Amazon.com, Inc., ByteDance Ltd., TikTok, Discord Inc., Facebook, Inc., Reddit, Inc., Snap Inc., Twitter, Inc., WhatsApp Inc., and YouTube LLC. The order was issued under Section 6(b) of the FTC Act, which authorizes studies without a law enforcement purposes.

Security and Transparency – Lessons

- Regulators may demand self-monitoring regimes for business activities. Perfection is not possible, but a program could include:

Lessons
Periodic reviews, with the involvement of **all** relevant internal stakeholders, to ensure public-facing statements accurately reflect current practices.
Review data security practices regularly to ensure they are "reasonable".
Review data collection practices, only collect what you need, and safely dispose of the rest.
Conduct due diligence on libraries and other third-party code.
Ensure compliance with specialized data obligations (*e.g.*, health, financial, minors).
Incorporate evolving regulator guidance.
Assess existing consumer-facing communications about use of data and whether additional disclosures are necessary, especially when related to an adverse service.

Accuracy

Accuracy – Overview

Risks

- Maintaining data for use in credit decisions that is **inaccurate or incomplete**
- Failing to give consumers an **opportunity to control their data by correcting errors or gaps in data**

Laws to Highlight

- Fair Credit Reporting Act (FCRA)
- FTC Act and State UDAP laws

Fair Credit Reporting Act (FCRA)

- FCRA governs consumer credit reports, which “bear[] on a consumer’s credit worthiness” and are “used or expected to be used” in establishing consumer’s eligibility for credit or other permissible purposes.
  - Contours of distinction between consumer and business reports

- FCRA applies to:
  - Credit reporting agencies (CRAs) – “Some data brokers that compile non-traditional information . . . may also be considered CRAs subject to the FCRA[.]”
  - Users of consumer reports
  - Furnishers of consumer credit data to CRAs

FCRA (cont'd)

- **CRAs** must:
  - Implement reasonable procedures to ensure maximum possible accuracy
  - Provide consumers with access to their own information and opportunity to correct
  - Provide reports only to entities that will use them for permissible purposes
- **Users** must:
  - Have a permissible purpose to use consumer reports
  - Notify consumers before and when adverse actions are taken on the basis of consumer report information
  - Notify consumers when providing less favorable terms on the basis of consumer report information (Risk-Based Pricing Rule)
- **Furnishers** must:
  - Take steps to provide information that is accurate and complete
  - Investigate consumer disputes about the accuracy of information provided

Accuracy – Public Commentary

Activity
• FTC Blog Post (April 2020): Ensure that your data and models are robust and empirically sound. If you provide data about consumers to others to make decisions about consumer access to credit, employment, insurance, housing, government benefits, check-cashing or similar transactions, you may be a consumer reporting agency that must comply with the FCRA, including ensuring that the data is accurate and up to date • FTC Senate Testimony (July 2018): “As the consumer reporting system evolves and new technologies and business practices emerge, vigorous enforcement of the FCRA continues to be a top priority for the Commission, as well as consumer and business education concerning applicable rights and responsibilities under the statute.” • National Consumer Law Center (NCLC) Report (Mar. 2019): The NCLC warned about errors and inaccuracies in alternative data and the inability to correct them. It noted that many big data brokers could be considered consumer reporting agencies subject to the FCRA, but it is highly unlikely that the companies that provide big data analytics—and the users of that data—are meeting FCRA obligations.

Accuracy – Sources

Category	Source
Background Checks	• CFPB Advisory Opinion on Background Screeners (Nov. 2021): The Bureau affirmed that the practice of matching consumer records, for tenant or employment screenings, solely through the matching of names is illegal under the Fair Credit Reporting Act. The CFPB specifically advised that "matching consumer records solely through the matching of names" is not a "reasonable procedure to assure maximum possible accuracy" under the FCRA. • AppFolio, Inc. (Dec. 2020): $4.25 million settlement with the FTC over allegations that AppFolio, which provides background reports to property management companies, failed to follow reasonable procedures to ensure the accuracy of criminal and eviction records it received from a third-party vendor. In addition to the monetary penalty, the company is prohibited from using records older than seven years.

Accuracy – Sources

Category	Source
Background Checks (cont'd)	• RealPage, Inc. (Oct. 2018): $3 million settlement resolving FTC claim that the company failed to take reasonable steps to ensure the accuracy of tenant screening information provided to its clients. • When a client requested criminal record information on applicants, RealPage conducted a nationwide criminal records search that "(1) used broad search criteria at the outset, (2) then applied only limited filters to the broad results, and (3) did not have policies or procedures to assess the accuracy of the results. In multiple instances, RealPage's practices led to the identification of criminal records that did not belong to the applicant and the inclusion of this inaccurate information in tenant screening reports." • Instant Checkmate, Inc. (Apr. 2014): $525,000 settlement resolving FTC claim that the company, a service that provided background checks for purposes including employment and housing, failed to follow reasonable procedures to assure that its reports were as accurate as possible, among other claims. • InfoTrack Information Services, Inc. (Mar. 2014): $1 million settlement resolving FTC claim that the company, which provided background checks for employers, failed to use reasonable procedures to assure maximum possible accuracy of consumer report information obtained from sex offender registry records.

Accuracy – Sources

Category	Source
Check Screening	• Telecheck Services (Jan. 2014): $3.5 million settlement resolving FTC claims that the company, which provides recommendations to businesses on whether to accept consumers' checks, failed to comply with requirements under the Furnisher Rule about the accuracy of information it provides to CRAs, among other claims. • Certegy Check Services (Aug. 2013): $3.5 million settlement resolving FTC claims that the company, which provides recommendations to businesses on whether to accept consumers' checks, failed to properly investigate accuracy disputes and correct inaccurate information within a reasonable time.
Other	• Dun & Bradstreet (Jan 2022): Settlement with FTC over allegations that D&B, a leading provider of business credit reports, failed to provide businesses with a meaningful way to correct errors in D&B reports. Instead, D&B offered a suite of products they purported would help companies improve their reports. As part of the settlement, D&B must refund certain businesses that purchased the company's products in the belief that using the products would improve their business' credit score and rating.

Accuracy – Sources

Category	Source
Other (cont'd)	- FDA Report on AI use in Medical Device Software (Sept. 2021): The FDA issued an action plan on AI and Machine Learning-Based Software as a Medical Device (SaMD). SaMD is software that relies on AI/ML and is intended to treat, diagnose, cure, mitigate, or prevent disease or other conditions. The report outlines the FDA's plans to step up AI governance in healthcare and how the agency envisions managing premarket submissions and oversight of the industry. - App Annie (Sept. 2021): $10 million settlement between SEC and App Annie and its founder stemming from their alleged failure to adequately disclose how App Annie generated market data on mobile app performance, such as how many times an app is downloaded. Per the SEC, App Annie and its founder sold manipulated data, misrepresented to trading firms how their data was derived, and encouraged firms to make trading decisions based on those numbers. - GAO Report on AI Use by Federal Agencies (June 2021): The GAO developed an accountability framework to identify key practices to help ensure accountability and responsible AI use by federal agencies and related entities. The framework is divided into four principles: data, governance, monitoring, and performance. The report breaks down data into two areas—data used to develop an AI model and data used to operate an AI system. The GAO seeks to ensure that government entities are implementing appropriate AI/ML training and validation and closely examining data streams to identify potential biases, and security and privacy risks.

Accuracy – Lessons

- Consider internal practices to address risk areas, such as:

Lessons
Review processes to ensure opportunities for data subject to confirm and correct data
Periodic data collection and algorithm testing to assess data collection parameters, focusing on whether relevant pieces of data are not being collected and/or analyzed or whether irrelevant data is being collected and/or analyzed
Maintain records of all data validation processes, legitimate interests assessments, or similar evaluations
Properly dispose of data as it becomes less useful
Ensure that inaccurate, incomplete, or unverifiable information is removed or corrected within required period (usually 30 days) of a dispute

Thank you!

Ali M. Arain

Partner
Jenner & Block
212 407-1721
aarain@jenner.com

Michael W. Ross

Partner
Jenner & Block
212 891-1669
mross@jenner.com

Bernadette Walli

Senior Counsel, Regulatory Affairs
Mastercard
914 267-7795
bernadette.walli@mastercard.com

© 2022 Jenner & Block LLP. Attorney Advertising. Jenner & Block is an Illinois Limited Liability Partnership including professional corporations. This publication is not intended to provide legal advice but to provide information on legal matters and firm news of interest to our clients and colleagues. Readers should seek specific legal advice before taking any action with respect to matters mentioned in this publication. The attorney responsible for this publication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome.