

GIBSON DUNN

# FTC PRIVACY UPDATE

Privacy + Security Academy  
November 4, 2022

# PANELISTS



**DANIELLE ESTRADA**

ATTORNEY ADVISOR TO  
COMMISSIONER ALVARO  
BEDOYA



**JANICE KOPEC**

ATTORNEY ADVISOR TO  
COMMISSIONER REBECCA  
SLAUGHTER



**ROBIN SPECTOR**

ATTORNEY ADVISOR TO  
COMMISSIONER CHRISTINE  
WILSON



**SVETLANA GANS**

GIBSON, DUNN & CRUTCHER  
LLP

# ADVANCED NOTICE OF PROPOSED RULEMAKING ON COMMERCIAL SURVEILLANCE & DATA SECURITY

**Federal Register / Vol. 87, No. 161 / Monday, August 22, 2022 / Proposed Rules** **51273**

072-36262A, dated September 14, 2021, specifies to submit certain information to the manufacturer, this AD does not include that requirement.

**(f) Other FAA AD Provisions**  
The following provisions also apply to this AD:

(1) *Alternative Methods of Compliance (AMOCs):* The Manager, Large Aircraft Section, International Validation Branch, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or responsible Flight Standards Office, as appropriate. If sending information directly to the Large Aircraft Section, International Validation Branch, send it to the attention of the person identified in paragraph (j)(2) of this AD. Information may be emailed to: 9-AVS-ARB-730-AMOC@faa.gov. Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the responsible Flight Standards Office.

(2) *Contracting the Manufacturer:* For any requirement in this AD to obtain instructions from a manufacturer, the instructions must be accomplished using a method approved by the Manager, Large Aircraft Section, International Validation Branch, FAA; or the United Kingdom Civil Aviation Authority (U.K. CAA); or BAE Systems (Operations) Limited; a U.K. CAA Design Organization Approval (DOA). If approved by the DOA, the approval must include the DOA-authorized signature.

**(g) Related Information**

(1) Refer to Mandatory Continuing Airworthiness Information (MCAI) U.K. CAA AD G-2022-0002, dated February 11, 2022, for related information. This MCAI may be found in the AD docket at <https://www.regulations.gov> by searching for and locating Docket No. FAA-2022-1053.

(2) For more information about this AD, contact Todd Thompson, Aerospace Engineer, Large Aircraft Section, FAA, International Validation Branch, 2200 South 216th St., Des Moines, WA 98198; telephone 206-231-3228; email [todd.thompson@faa.gov](mailto:todd.thompson@faa.gov).

(3) For service information identified in this AD, contact BAE Systems (Operations) Limited, Customer Information Department, Prestwick International Airport, Ayrshire, KA9 2RW, Scotland, United Kingdom; telephone +44 1292 675207; fax +44 1292 675794; email [RApublications@baesystems.com](mailto:RApublications@baesystems.com); internet [https://www.baesystems.com/Businesses/Regional\\_Aircraft/index.htm](https://www.baesystems.com/Businesses/Regional_Aircraft/index.htm). You may view this service information at the FAA, Airworthiness Products Section, Operational Safety Branch, 2200 South 216th St., Des Moines, WA. For information on the availability of this material at the FAA, call 206-231-3195.

Issued on August 10, 2022.  
**Gastano A. Sciortino,**  
Deputy Director for Strategic Initiatives,  
Compliance & Airworthiness Division,  
Aircraft Certification Service.  
[FR Doc. 2022-17965 Filed 8-19-22; 8:45 am]

**BILLING CODE 4910-13-P**

**FEDERAL TRADE COMMISSION**  
**16 CFR Chapter I**  
**Trade Regulation Rule on Commercial Surveillance and Data Security**  
**AGENCY:** Federal Trade Commission.  
**ACTION:** Advance notice of proposed rulemaking; request for public comment; public forum.

**SUMMARY:** The Federal Trade Commission ("FTC") is publishing this advance notice of proposed rulemaking ("ANPR") to request public comment on the prevalence of commercial surveillance and data security practices that harm consumers. Specifically, the Commission invites comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.

**Comments due date:** Comments must be received on or before October 21, 2022.

**Meeting date:** The Public Forum will be held virtually on Thursday, September 8, 2022, from 2 p.m. until 7:30 p.m. Members of the public are invited to attend at the website <https://www.ftc.gov/news-events/events/2022/09/commercial-surveillance-data-security-anpr-public-forum>.

**ADDRESSES:** Interested parties may file a comment online or on paper by following the instructions in the Comment Submissions part of the SUPPLEMENTARY INFORMATION section below. Write "Commercial Surveillance ANPR, R111004" on your comment, and file your comment online at <https://www.regulations.gov>. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex B), Washington, DC 20580.

**FOR FURTHER INFORMATION CONTACT:** James Tilling, 202-326-3497; Peter Magee, 202-326-3538; Olivier Sylvain,

**FEDERAL TRADE COMMISSION**  
**16 CFR Chapter I**  
**Trade Regulation Rule on Commercial Surveillance and Data Security**  
**AGENCY:** Federal Trade Commission.  
**ACTION:** Advance notice of proposed rulemaking; request for public comment; public forum.

**SUMMARY:** The Federal Trade Commission ("FTC") is publishing this advance notice of proposed rulemaking ("ANPR") to request public comment on the prevalence of commercial surveillance and data security practices that harm consumers. Specifically, the Commission invites comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.

- **Purpose** – Seeks public comment on the harms stemming from commercial surveillance and whether new rules are needed to protect people’s privacy and information
- **Contents** – Consists of 95 questions which consider:
  - Harm to consumers (including children)
  - Balance of costs and benefits
  - How the Commission should regulate prevalent and harmful surveillance practices
- **Comment Deadline** – November 21

# ADVANCED NOTICE OF PROPOSED RULEMAKING ON COMMERCIAL SURVEILLANCE & DATA SECURITY (CONT'D)

- **Commissioner Statements**

- Commissioner Bedoya – Stated ANPR should focus on the needs of people most at risk of being left behind by new technology in the modern economy. Sought comment on emerging discrimination issues; the mental health of kids and teens; protecting non-English speaking communities; and unfair or deceptive practices related to biometrics. Supports the ADPPA and will not vote for a Rule that interferes with it.
- Commissioner Slaughter – Stated that unfettered commercial data collection, retention, use, and sharing has contributed to data abuses such as surreptitious biometric or location tracking, unaccountable and discriminatory algorithmic decision-making, and lax data security practices. Sought comment on minimization and purpose and use specifications, impact of data harms on civil rights and harms related to kids and teens.
- Commissioner Wilson – Dissented and expressed concern that the ANPR might derail the American Data Privacy and Protection Act. She further noted that the changes to the Section 18 Rules of Practice could impact public input and that the proposal was overbroad in some areas.



- Held on Sept. 8 to gather public feedback on the proposed rulemaking
- Commissioner Statements regarding the ANPRM:
  - Chair Khan noted the rulemaking seeks to determine whether unfair or deceptive trade practices are prevalent, requiring more than case-by-case adjudication
  - Commissioner Slaughter noted the FTC has a duty to act until Congress passes federal privacy legislation
  - Commissioner Bedoya emphasized the need to hear how the public has been personally impacted by commercial surveillance and poor data security practices
- The FTC also convened panels of industry experts and consumer advocates who held a variety of viewpoints, including:
  - Future rulemaking should be calibrated to the different levels of risk presented by particular types of data collection and uses
  - Children over 13 who have aged out of COPPA should be protected
  - FTC should consider algorithmic discrimination and dark patterns
  - Implementation of a Global Privacy Control would allow consumers to opt out of multiple websites at once

# PRIVACYCON 2022



- Convenes researchers, academics, industry representatives, consumer advocates, and government regulators, to discuss the latest research and trends related to consumer privacy and data security

- Discussion and research:
  - Commercial surveillance
  - Children's privacy
  - Devices that listen to users
  - Interfaces and dark patterns

# PRIVACY-RELATED CONSENT DECREES

- Chair Lina Khan has told the Senate Judiciary Committee that the FTC is examining ways to prevent companies from “treating FTC orders as suggestions”
- FTC has strengthened recent consent decrees using the following measures:
  - Requiring Everalbum to delete any models or algorithms developed with users’ photos or videos over its use of facial recognition technology
  - Requiring upgraded multifactor authentication methods, encrypted SSNs, and a reduction in data collection in its recent settlement order with CafePress
  - Naming individual executives, as in its recent settlement with Drizly and its CEO for failing to upgrade security measures after a 2018 breach, leading to a second breach.
  - Requiring Chegg to bolster its data security, limit the data the company can collect and retain, offer users multifactor authentication to secure their accounts, and allow users to access and delete their data.
  - Enhancing assessments of a company’s security practices

# CHILDREN'S PRIVACY – COPPA RULE REVISION

## PART 312 - CHILDREN'S ONLINE PRIVACY PROTECTION RULE

**Authority:** 15 U.S.C. 6501-6508.

**Source:** 78 FR 4008, Jan. 17, 2013, unless otherwise noted.

### § 312.1 Scope of regulations in this part.

This part implements the Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501, *et seq.*) which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.



Congress of the United States  
Washington, DC 20515

September 29, 2022

“The FTC must also utilize its authority to update its COPPA regulations. Under this legislation, in response to technological and societal development, the Commission can regularly promulgate rules to protect children’s privacy. In 2012, for example, the FTC approved revisions to the COPPA regulations, broadening the definition of protected information to include photos, videos, geolocation information, and online cookies. Now, we encourage the FTC to use its regulatory authority to institute additional protections that address pressing threats online, a process the Commission has already begun. For example, the Commission should consider:

- Rule last amended in 2013
- Congress has requested further amendment to address new and more prevalent online threats to children

- expanding the definition of “personal information” covered under COPPA;
- implementing rules to effectuate COPPA’s prohibition on conditioning a child’s participation in an online activity on the child sharing more data than is reasonably necessary;
- implementing rules to effectuate COPPA’s requirement that platforms protect the confidentiality, security, and integrity of children’s data;
- ensuring that COPPA’s requirements protect children on the platforms they actually use by updating COPPA’s regulations defining platforms that are directed to children and updating regulations defining platforms that have actual knowledge they are collecting data from children;
- implementing regulatory protections that reflect the increased use of online platforms for educational purposes; and
- implementing regulatory protections that reflect changes in online advertising practices.”

# CHILDREN'S PRIVACY (CONT'D)



- October 19, 2022 event convened researchers, child development and legal experts, consumer advocates, and industry professionals to discuss:
  - Children's capacity at different ages and developmental stages to recognize and understand advertising content and distinguish it from other content
  - The harms to children resulting from the inability of children to recognize advertising
  - What measures should be taken to protect children from blurred content in digital marketing, and
  - The need for and efficacy of disclosures as a solution for children of different ages, including the format, timing, placement, wording, and frequency of disclosures

# CHILDREN'S PRIVACY (CONT'D)

- The FTC has recently finalized several consent decrees to further protect children's privacy
  - Settlement orders with Recolor and Kurbo, Inc. (Subsidiary of Weight Watchers International) for allegedly not asking parental consent before collecting sensitive data
  - 2021 settlement order with OpenX Technologies for allegedly collecting sensitive data including geolocation information, even if customers opted out



# CHILDREN'S PRIVACY (CONT'D)

The FTC has also reaffirmed its commitment to COPPA for EdTech platforms in a recent Policy Statement

**Policy Statement of the Federal Trade Commission on Education Technology  
and the Children's Online Privacy Protection Act**

The Federal Trade Commission ("Commission") is committed to ensuring that education technology ("ed tech") tools and their attendant benefits do not become an excuse to ignore critical privacy protections for children. When Congress enacted the Children's Online Privacy Protection Act<sup>1</sup> ("COPPA"), it empowered the Commission with tools beyond administering compliance with notice and consent regimes. The Commission's COPPA authority demands enforcement of meaningful substantive limitations on operators' ability to collect, use, and retain children's data, and requirements to keep that data secure. The Commission intends to fully enforce these requirements—including in school and learning settings where parents may feel they lack alternatives.

# ALGORITHMIC BIAS

- Last year, Commissioner Slaughter published an article discussing algorithmic bias, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*
  - Notes algorithms have the potential to “amplify injustice while simultaneously making injustice less detectable”
  - Calls for the FTC to “deploy Section 5 of the FTC Act, FCRA, ECOA, COPPA, and Section 6(b) studies creatively to mitigate algorithmic harms”

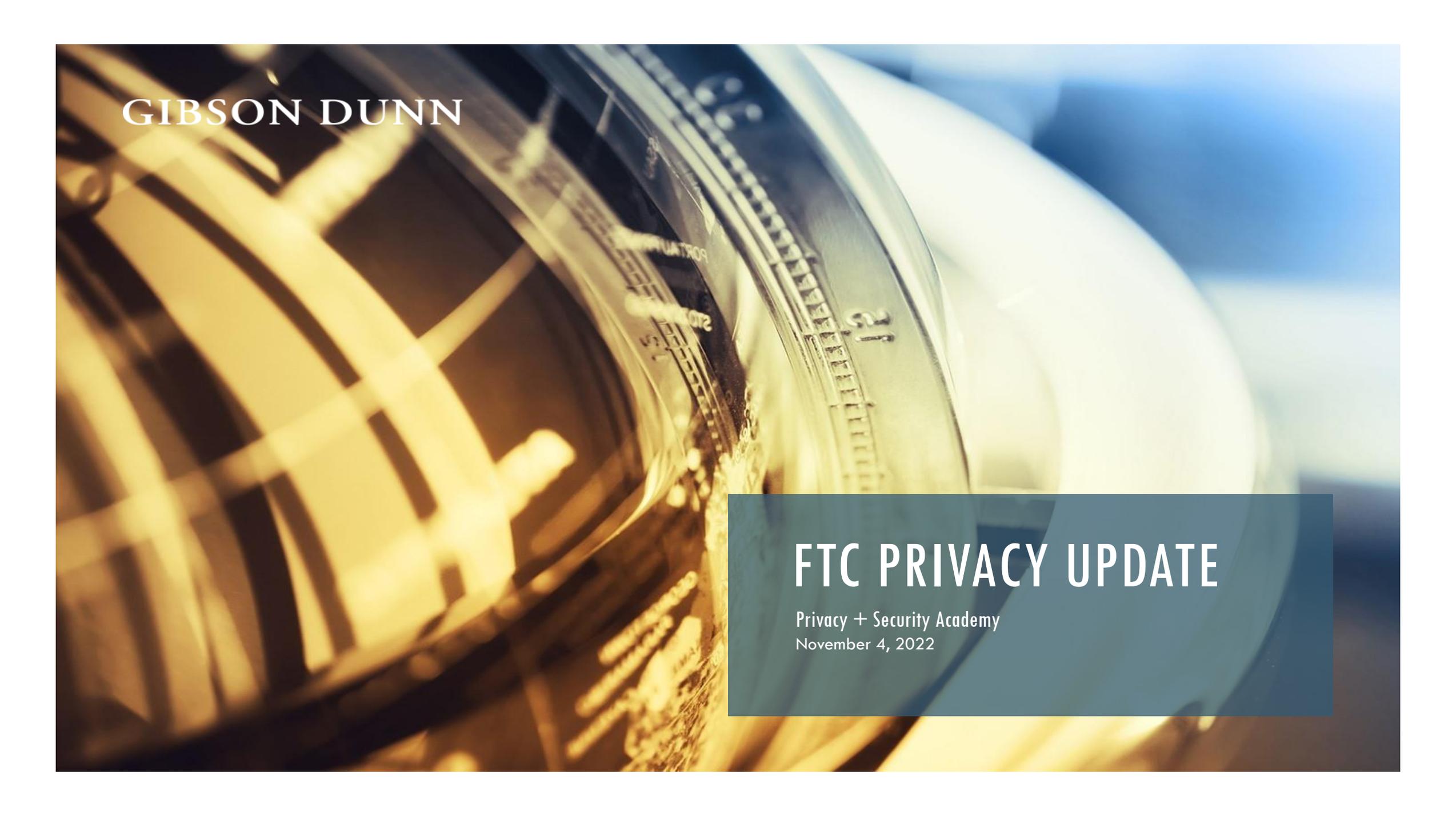
## Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission

Rebecca Kelly Slaughter

Janice Kopec & Mohamad Batal

23 Yale J.L. & Tech. Special Issue 1

As an FTC Commissioner, I aim to promote economic and social justice through consumer protection and competition law and policy. In recent years, algorithmic decision-making has produced biased, discriminatory, and otherwise problematic outcomes in some of the most important areas of the American economy. This article describes harms caused by algorithmic decision-making in the high-stakes spheres of employment, credit, health care, and housing, which profoundly shape the lives of individuals. These harms are often felt most acutely by historically disadvantaged populations, especially Black Americans and other communities of color. And while many of the harms I describe are not entirely novel, AI and algorithms are especially dangerous because they can simultaneously obscure problems and amplify them—all while giving the false impression that these problems do not or could not possibly exist.



GIBSON DUNN

# FTC PRIVACY UPDATE

Privacy + Security Academy  
November 4, 2022