Danielle Estrada

Attorney Advisor to Commissioner Alvaro Bedoya
Federal Trade Commission

Kevin Moriarty

Attorney Advisor to Chair Lina Khan
Federal Trade Commission

Svetlana Gans
Partner, Gibson, Dunn & Crutcher
Moderator

Gaurav Laroia

Attorney Advisor to Commissioner Rebecca Slaughter
Federal Trade Commission

Elisa Jillson

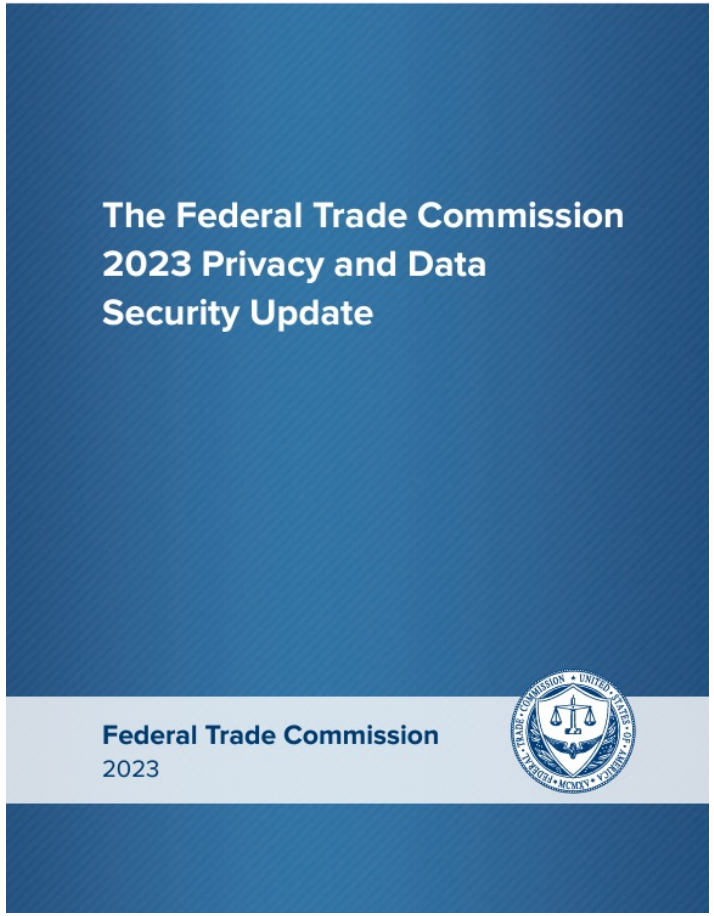
Attorney Advisor to Commissioner Melissa Holyoak
Federal Trade Commission

Report Released Announcing 2023 Highlights

Privacy+ Security Forum

FTC Issues Privacy and Data Security Update in March, 2024

- "The FTC is taking bold actions to challenge the indiscriminate collection and monetization of consumers' data. We are securing meaningful remedies to protect consumers' information, rather than placing the burden on consumers to protect themselves." – Samuel Levine, Director of the FTC's Bureau of Consumer Protection
- To date, the FTC has brought:
  - 97 Privacy cases
  - 89 Data Security cases
  - 169 Telemarketing Sales Rule/CAN-SPAM cases
- Recent Key Areas of Focus:
  - Artificial Intelligence
  - Health Privacy
  - Children's Privacy
  - Geolocation Data



Artificial Intelligence

Privacy+ Security Forum

Policy: Biometric Info and Section 5

FTC Issued Policy Statement in May 2023

- Numerous practices relating to use and processing of biometric information may violate Section 5 of the FTC Act:
  - False claims relating to the accuracy or fairness of technology
  - Deceptive statements about collection and use of biometric information
  - Failing to assess forseeable harms from data breaches
  - Failing to provide appropriate training for employees or contractors
- Local laws restricting the use of certain technologies in certain locations also apply

Commissioners Deliver Remarks Supporting the FTC's Biometric Information Policy Statement

- Chair Khan and Commissioners Slaughter and Bedoya each delivered remarks at the Commission's May 18 Open Commission Meeting
  - Chair Khan discussed why consumer "consent" may represents a fiction
  - Commissioner Slaughter called for specific enforcement of the Health Breach Notification Rule
  - Commissioner Bedoya expressed particular concern about the discriminatory effects caused by improper use of biometric information.

Rite Aid Banned from Using Facial Recognition

- FTC announced settlement with Rite Aid in December 2023
- The Order prohibits Rite Aid's use of AI Facial Recognition for 5 years
- FTC alleged that Rite Aid's facial recognition falsely flagged customers as potential shoplifters, prompting contractors to search, follow, and remove innocent customers
  - The embarrassment of falsely being identified as a shoplifter allegedly disproportionately impacted people of color
- Rite Aid allegedly used low quality images and an incomplete data set to train its AI powered system, leading to thousands of false-positive matches that its contractor incorrectly acted upon.

Chair Khan's Remarks Re: Artificial Intelligence

Privacy+ Security Forum

FTC Chair Lina Khan Gives Remarks at the FTC Tech Summit on Jan. 25, 2024

- FTC focused on four key principles with respect to AI legislation and enforcement:
  - Scrutinizing existing and emerging **bottlenecks and monopolies**
  - **Consumer protection** surrounding the improper use of data – "our remedies will [require] that firms delete models trained on unlawfully acquired data."
  - **Aligning liability with capability** and control
  - **Effective remedies** that establish bright-line rules

Commissioner Levine on the Digital Economy

Privacy+ Security Forum

BCP Director Samuel Levine Remarks at Fordham Law School on Apr. 17, 2024

- Notice and Choice is not a permanent regime. "Notice and choice is a fantasy world, divorced from the reality of how people live or how firms operate."
- Three goals for a better digital economy:
  - Establishing a zone of privacy on the internet
  - Making the internet less like a casino
  - Ensuring AI works for us, not the other way around

Health Privacy

Privacy+ Security Forum

Monument Banned from Disclosing Health Data for Advertising

- FTC reached settlement with Monument following FTC allegations that Monument shared consumer health data with third-party advertising platforms without consent
- DOJ complaint alleged that Monument shared sensitive information about patients seeking help for alcohol addiction with advertisers despite promises not to share such information.
- Settlement would impose a $2.5 Million Penalty

Proposed Order will Prohibit Cerebral from Using Sensitive Data for Advertising

- Complaint alleges that Cerebral and its former CEO deceived users about its data sharing and security practices, and misled consumers about its cancellation policies
- Telehealth firm Cerebral will be required to pay $7 Million in civil fines.
- Cerebral allegedly:
  - Engaged in careless marketing
  - Allowed former employees to access user data
  - Used insecure access methods.

FTC Changes to Health Breach Notification Rule

Privacy+ Security Forum

FTC Finalized Rule in Apr. 2024 Underscoring its Application to Health Apps and Similar Technologies Not Covered by HIPAA

- The HBNR requires vendors of personal health records (PHR) and related entities that are not covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data. It also requires third party service providers to vendors of PHRs and PHR related entities to notify such vendors and PHR related entities following the discovery of a breach.
- According to the Majority statement, "codifying how HBNR applies to online platforms and applications, today's Final Rule provides market participants with more clarity about what entities are covered—thereby providing greater certainty and notice."
- Commissioners Holyoak and Ferguson dissented: "The Commission takes liberties . . . to adopt a new, capacious definition of "covered health care provider" and a new, similarly capacious definition of "health care services and supplies," whose joint effect is to sweep a large swath of apps and app developers under the purview of the Final Rule."

Children's Online Privacy Protection Act (COPPA)

Privacy+ Security Forum

Amendments to COPPA

2034 Federal Register / Vol. 89, No. 8 / Thursday, January 11, 2024 / Proposed Rules

FEDERAL TRADE COMMISSION

16 CFR Part 312

RIN 3084–AB20

Children's Online Privacy Protection Rule

AGENCY: Federal Trade Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Commission proposes to amend the Children's Online Privacy Protection Rule, consistent with the requirements of the Children's Online Privacy Protection Act. The proposed modifications are intended to respond to changes in technology and online practices, and where appropriate, to clarify and streamline the Rule. The proposed modifications, which are based on the FTC's review of public comments and its enforcement experience, are intended to clarify the scope of the Rule and/or strengthen its protection of personal information collected from children.

DATES: Comments must be received by March 11, 2024.

ADDRESSES: Interested parties may file a comment online or on paper by following the instructions in the Request for Comment part of the SUPPLEMENTARY INFORMATION section below. Write "COPPA Rule Review, Project No. P195404" on your comment and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. 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 E), Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Manmeet Dhindsa (202–326–2877) or James Trilling (202–326–3497), Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission.

SUPPLEMENTARY INFORMATION:

I. Background

Congress enacted the Children's Online Privacy Protection Act ("COPPA" or "COPPA statute"), 15 U.S.C. 6501 *et seq.*, in 1998. The COPPA statute directed the Federal Trade Commission ("Commission" or "FTC") to promulgate regulations implementing COPPA's requirements. On November 3, 1999, the Commission issued its Children's Online Privacy Protection Rule, 16 CFR part 312 ("COPPA Rule" or "Rule"), which became effective on April 21, 2000.[1] Section 6506 of the COPPA statute and § 312.11 of the initial Rule required that the Commission initiate a review no later than five years after the initial Rule's effective date to evaluate the Rule's implementation. The Commission commenced this mandatory review on April 21, 2005.[2] After receiving and considering extensive public comment, the Commission determined in March 2006 to retain the COPPA Rule without change.[3] In 2010, the Commission once again undertook a review of the COPPA Rule to determine whether the Rule was keeping pace with changing technology. After notice and comment, the Commission issued final amendments to the Rule, which became effective on July 1, 2013 ("2013 Amendments").[4]

The COPPA Rule imposes certain requirements on operators of websites [5] or online services directed to children under 13 years of age, and on operators of websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age (collectively, "operators"). The Rule requires that operators provide notice to parents and obtain verifiable parental consent before collecting, using, or disclosing personal information from children under 13 years of age.[6] Additionally, the Rule requires that operators must provide parents the opportunity to review the types or categories of personal information collected from their child, the opportunity to delete the collected information, and the opportunity to prevent further use or future collection of personal information from their child.[7] The Rule also requires operators to keep personal information they collect from children secure, including by imposing retention and deletion requirements, and prohibits them from conditioning children's participation in activities on the collection of more personal information than is reasonably necessary to participate in such activities.[8] The Rule contains a "safe harbor" provision enabling industry groups or others to submit to the Commission for approval self-regulatory guidelines that would implement the Rule's protections.[9]

The 2013 Amendments [10] revised the COPPA Rule to address changes in the way children use and access the internet, including through the increased use of mobile devices and social networking. In particular, the 2013 Amendments:

- Modified the definition of "operator" to make clear that the Rule covers an operator of a child-directed website or online service that integrates outside services—such as plug-ins or advertising networks—that collect personal information from the website's or online service's visitors, and expanded the definition of "website or online service directed to children" to clarify that those outside services are subject to the Rule where they have actual knowledge that they are collecting personal information directly from users of a child-directed website or online service;
- Permitted a subset of child-directed websites or online services that do not target children as their primary audience to differentiate among users, requiring them to comply with the Rule's obligations only as to users who identify as under the age of 13;
- Expanded the definition of "personal information" to include geolocation information; photos, videos and audio files containing a child's image or voice; and persistent identifiers that can be used to recognize a user over time and across different websites or online services;
- Streamlined the direct notice requirements to ensure that key information is presented to parents in a succinct "just-in-time" notice;
- Expanded the non-exhaustive list of acceptable methods for obtaining prior verifiable parental consent;
- Created three new exceptions to the Rule's notice and consent requirements, including for the use of persistent identifiers for the support for the internal operations of a website or online service;

[1] Children's Online Privacy Protection Rule, Statement of Basis and Purpose, 64 FR 59888 (Nov. 3, 1999), available at *https://www.federalregister.gov/documents/1999/11/03/99-27740/childrens-online-privacy-protection-rule.*

[2] Children's Online Privacy Protection Rule, Request for Public Comment, 70 FR 21107 (Apr. 22, 2005), available at *https://www.federalregister.gov/documents/2005/04/22/05-8160/childrens-online-privacy-protection-rule-request-for-comments.*

[3] Children's Online Privacy Protection Rule, Retention of Rule Without Modification, 71 FR 13247 (Mar. 15, 2006), available at *https://www.federalregister.gov/documents/2006/03/15/06-2356/childrens-online-privacy-protection-rule.*

[4] *See* Children's Online Privacy Protection Rule, Statement of Basis and Purpose, 78 FR 3972 (Jan. 17, 2013), available at *https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule.*

[5] *See* Part IV for further discussion of the Commission's proposal to change the term "Web site" to "Web site" throughout the Rule. This Notice of Proposed Rulemaking incorporates this proposed change in all instances in which the term "Web site" is used.

[6] 16 CFR 312.3, 312.4, and 312.5.

[7] 16 CFR 312.3 and 312.6.

[8] 16 CFR 312.3, 312.7, 312.8, and 312.10.

[9] 16 CFR 312.11.

[10] 78 FR 3972.

FTC Proposed Amendments to COPPA in Dec. 2023

- First amendment to COPPA in a decade
- Changes include:
  - Requiring separate opt-in for targeted advertising;
  - Prohibiting conditioning a child's participation on collection of personal information;
  - Imposing restrictions on educational technology companies, including prohibiting these companies' use of students' data for commercial purposes;
  - Increasing accountability for Safe Harbor programs, including by requiring each program to publicly disclose its membership list and report additional information to the Commission;
  - Strengthening data security requirements; and
  - Limiting data retention.

Increased Enforcement to Protect Kids

Privacy+ Security Forum

FTC Will Require Microsoft to Pay $20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent

Proposed order will require Microsoft to bolster protections for children; makes clear that avatars and biometric and health data are protected under COPPA

FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts

Under proposed order, Edmodo will be prohibited from conditioning participation in an educational activity on providing unnecessary data

FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data

FTC says that the company violated 2020 privacy order; proposes new protections for children and teens

Open Questions Surrounding Children's Privacy

Privacy+ Security Forum

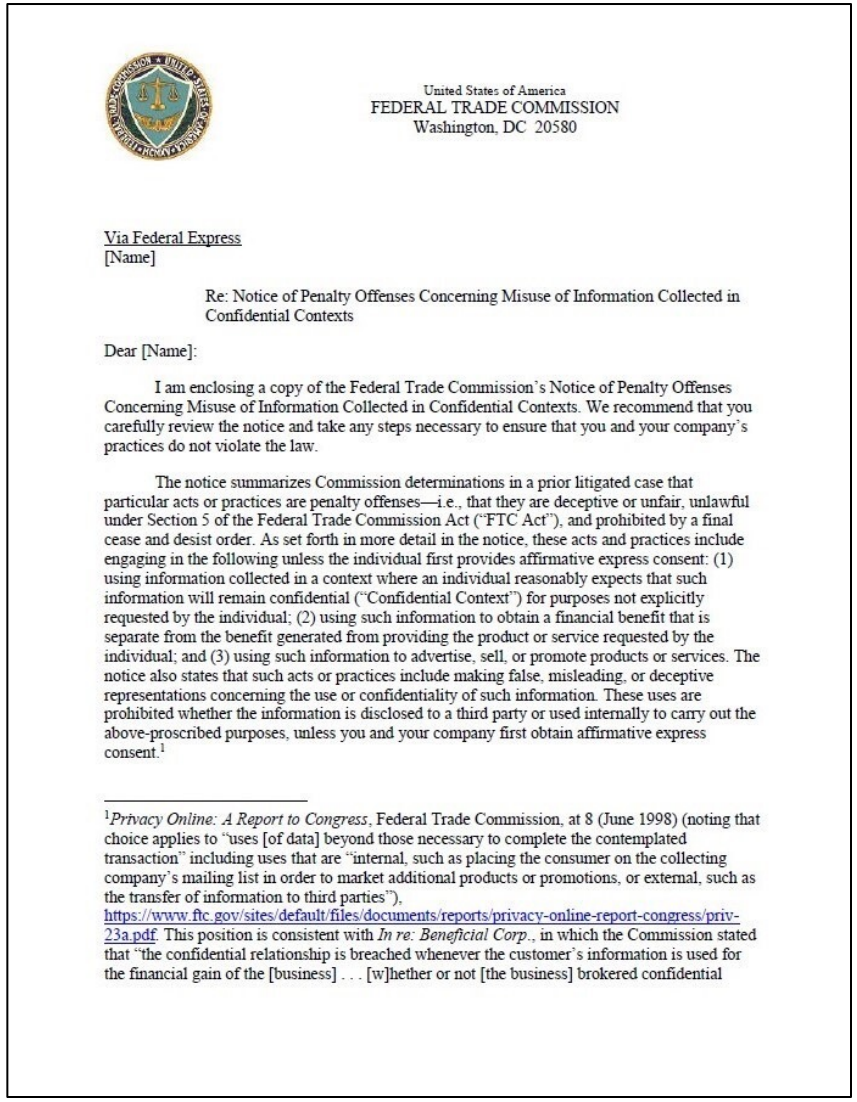
FTC Denied Application for Facial Age Verification

- Entertainment Software Rating Board (ESRB) and others applied to use a new technology to obtain parental consent under COPPA
- The FTC denied the application without prejudice on March 29, 2024
- The Commission unanimously elected to deny the application until it has more information about the technology at issue including the technology's risks and potential benefits.

Data Collection and Data Minimization

Privacy+ Security Forum

Notice of Penalty Offenses (NPO)



United States of America
FEDERAL TRADE COMMISSION
Washington, DC 20580

Via Federal Express
[Name]

Re: Notice of Penalty Offenses Concerning Misuse of Information Collected in Confidential Contexts

Dear [Name]:

I am enclosing a copy of the Federal Trade Commission's Notice of Penalty Offenses Concerning Misuse of Information Collected in Confidential Contexts. We recommend that you carefully review the notice and take any steps necessary to ensure that you and your company's practices do not violate the law.

The notice summarizes Commission determinations in a prior litigated case that particular acts or practices are penalty offenses—i.e., that they are deceptive or unfair, unlawful under Section 5 of the Federal Trade Commission Act ("FTC Act"), and prohibited by a final cease and desist order. As set forth in more detail in the notice, these acts and practices include engaging in the following unless the individual first provides affirmative express consent: (1) using information collected in a context where an individual reasonably expects that such information will remain confidential ("Confidential Context") for purposes not explicitly requested by the individual; (2) using such information to obtain a financial benefit that is separate from the benefit generated from providing the product or service requested by the individual; and (3) using such information to advertise, sell, or promote products or services. The notice also states that such acts or practices include making false, misleading, or deceptive representations concerning the use or confidentiality of such information. These uses are prohibited whether the information is disclosed to a third party or used internally to carry out the above-proscribed purposes, unless you and your company first obtain affirmative express consent.[1]

[1] *Privacy Online: A Report to Congress*, Federal Trade Commission, at 8 (June 1998) (noting that choice applies to "uses [of data] beyond those necessary to complete the contemplated transaction" including uses that are "internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties"), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf. This position is consistent with *In re: Beneficial Corp.*, in which the Commission stated that "the confidential relationship is breached whenever the customer's information is used for the financial gain of the [business] . . . [w]hether or not [the business] brokered confidential

NPO Summarizes Acts Previously Found to Violate Law

An NPO serves as a warning that certain activity may leave a company vulnerable to enforcement action.

NPO Sent to 5 Tax Prep Companies

Warns that using data for any purpose other than that for which it was collected violates the law. Such uses include:

- Using data for advertising
- Obtaining an alternative financial benefit
- Violating an expectation of confidentiality for any purpose

FTC Banned BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information

- FTC issued a Proposed Order against BetterHelp in March, 2023
- The Proposed Order requires BetterHelp to pay $7.8 million to consumers to settle charges that it revealed consumers' sensitive data to third parties including Facebook and Snapchat for advertising after promising to keep such data private.

"When a person struggling with mental health issues reaches out for help, they do so in a moment of vulnerability and with an expectation that professional counseling services will protect their privacy[.]Instead, BetterHelp betrayed consumers' most personal health information for profit. Let this proposed order be a stout reminder that the FTC will prioritize defending Americans' sensitive data from illegal exploitation."

Samuel Levine, Director of the FTC's Bureau of Consumer Protection

Chegg Inc.

Privacy+ Security Forum

FTC Finalized Order in Jan. 2023 with Ed Tech Provider Chegg for Lax Security that Allegedly Exposed Student Data

- Chegg allegedly experienced four data breaches that exposed the personal information of about 40 million users and employees.
- FTC alleged that Chegg stored users' personal data on its cloud storage databases in plain text and employed outdated and weak encryption to protect user passwords.
- Among other remedies, the FTC's Order limits the data Chegg is permitted to collect or retain.

Other Enforcement Actions

Privacy+ Security Forum

FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations

Agency Alleges that Kochava's Geolocation Data from Hundreds of Millions of Mobile Devices Can Be Used to Identify People and Trace Their Movements

FTC Order Will Ban Avast from Selling Browsing Data for Advertising Purposes, Require It to Pay $16.5 Million Over Charges the Firm Sold Browsing Data After Claiming Its Products Would Block Online Tracking

FTC says despite its promises to protect consumers from online tracking, Avast sold consumers' browsing data to third parties

FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data

FTC charges X-Mode and Outlogic with selling raw location data, failing to obtain informed consumer consent

Addressing Vulnerabilities Systematically

FTC Issues Guidance from the Cybersecurity and Infrastructure Security Agency (CISA)

- “The best way to address the risk of security vulnerabilities in products is systematically, not in ad-hoc or one-off ways.”
- FTC has been bringing enforcement actions based on poos cybersecurity practices for more than two decades.
- Current best practices include preemptively protecting against the following vulnerabilities:
  - Cross Site Scripting
  - SQL Injection
  - Buffer Overflows and Use-After-Free Vulnerabilities

Sensitive Information and Dark Patterns

Privacy+ Security Forum

Dark Patterns Generally

Privacy+ Security Forum

- Coined in 2010 by user design specialist Harry Brignull, the term “dark patterns” has been used to describe design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm.
- Common Dark Patterns include:
  - Design Elements that Induce False Beliefs
  - Design Elements that Hide or Delay Disclosure of Material Information
  - Design Elements that Lead to Unauthorized Charges
  - Design Elements that Obscure or Subvert Privacy Choices
- The FTC has used its enforcement authority to prevent dark patterns across a range of industries and varied deceptive practices.

Recent Enforcement

Privacy+ Security Forum

FTC Takes Action Against Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel

Complaint outlines details of company's knowing failure to address non-consensual subscriptions and cancellation trickery

FTC, California Obtain Order Against DNA Testing Firm over Charges it Made a Myriad of Misrepresentations to Consumers to Entice Them to Buy Ancestry Reports

CRI Genetics will halt deceptive conduct, pay civil penalty, and give consumers a right to delete biometric information to settle the agencies' charges

FTC Takes Action to Stop Credit Karma From Tricking Consumers With Allegedly False "Pre-Approved" Credit Offers

Nearly One Third of Some "Pre-Approved" Offers Resulted in Denials; Company to Pay $3 Million and Halt Deceptive Claims

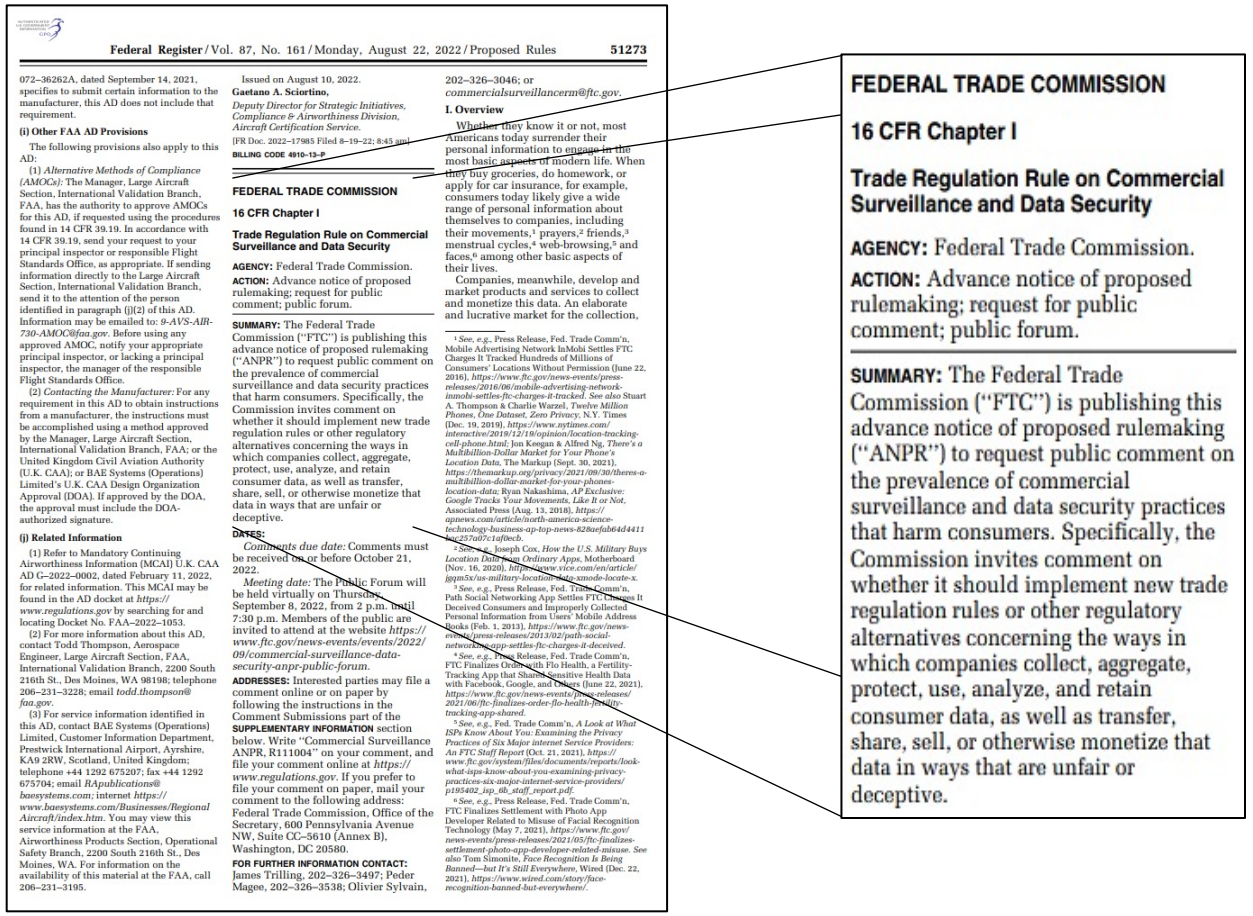
Advanced Notice of Proposed Rulemaking (ANPR)

Surveillance and Lax Data Security

Privacy+ Security Forum

Consumer Data Privacy

Privacy+ Security Forum



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.

(i) 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-AIR-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) *Contacting 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's U.K. CAA Design Organization Approval (DOA). If approved by the DOA, the approval must include the DOA-authorized signature.

(j) 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.*

(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 675704; email *RApublications@baesystems.com*; internet *https://www.baesystems.com/Businesses/RegionalAircraft/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.

Gaetano A. Sciortino,

Deputy Director for Strategic Initiatives, Compliance & Airworthiness Division, Aircraft Certification Service.

[FR Doc. 2022–17985 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.

DATES:

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 Trilling, 202–326–3497; Peder Magee, 202–326–3538; Olivier Sylvain, 202–326–3046; or *commercialsurveillancerm@ftc.gov.*

I. Overview

Whether they know it or not, most Americans today surrender their personal information to engage in the most basic aspects of modern life. When they buy groceries, do homework, or apply for car insurance, for example, consumers today likely give a wide range of personal information about themselves to companies, including their movements,[1] prayers,[2] friends,[3] menstrual cycles,[4] web-browsing,[5] and faces,[6] among other basic aspects of their lives.

Companies, meanwhile, develop and market products and services to collect and monetize this data. An elaborate and lucrative market for the collection,

[1] *See, e.g.,* Press Release, Fed. Trade Comm'n, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission (June 22, 2016), *https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked. See also* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy,* N.Y. Times (Dec. 19, 2019), *https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html;* Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data,* The Markup (Sept. 30, 2021), *https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data;* Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not,* Associated Press (Aug. 13, 2018), *https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb.*

[2] *See, e.g.,* Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps,* Motherboard (Nov. 16, 2020), *https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.*

[3] *See, e.g.,* Press Release, Fed. Trade Comm'n, Path Social Networking App Settles FTC Charges It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), *https://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived.*

[4] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (June 22, 2021), *https://www.ftc.gov/news-events/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared.*

[5] *See, e.g.,* Fed. Trade Comm'n, *A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers: An FTC Staff Report* (Oct. 21, 2021), *https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.*

[6] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology (May 7, 2021), *https://www.ftc.gov/news-events/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse. See also* Tom Simonite, *Face Recognition Is Being Banned—but It's Still Everywhere,* Wired (Dec. 22, 2021), *https://www.wired.com/story/face-recognition-banned-but-everywhere/.*

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.

FTC exploring new rule on consumer data

- FTC issued ANPR on commercial collection and use of consumer data in August 2022
- Goal of ANPR is to determine the need for a data privacy rule and its potential impact
- Priorities are youth mental health, data security, bias and discrimination, consumer choice, and deceptive collection practices
- Public comment period closed November 2022
- FTC still reviewing more than 10,000 comments

Audience Questions