JUDICIAL COUNCIL OF CALIFORNIA

520 Capitol Mall, Suite 600 • Sacramento, California 95814-4717
Telephone 916-323-3121 • Fax 916-323-4347 • TDD 415-865-4272

MEMORANDUM

Date
August 30, 2022

To
Members of the Legislation Committee

From
Li Gotch, Analyst

Subject
Request for authorization to submit comments on behalf of the Court Security Advisory Committee and the Judicial Council of California to the Federal Trade Commission on proposed rulemaking pursuant to Federal Register Commercial Surveillance ANPR, R111004

Action Requested
Approve request to submit comments

Deadline
October 21, 2022

Contact
Li Gotch, 415-865-4365
lisa.gotch@jud.ca.gov

Sponsor

Federal Trade Commission

Description of Proposal

Commercial Surveillance ANPR, R111004 requests 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 (1) collect, aggregate, protect, use, analyze, and retain consumer data, as well as (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive."[1]

[1] See www.ftc.gov/system/files/ftc_gov/pdf/commercial_surveillance_and_data_security_anpr.pdf.

Recommendation

The Court Security Advisory Committee (CSAC) recommends that the Legislation Committee of the Judicial Council submit comments to the Federal Trade Commission in response to the request for comment. Specifically, the CSAC recommends the following comments be submitted:

1. When discussing consumer harm, the FTC should take judicial officers into particular consideration.

A small portion of the potential consumer damages associated with deficient data security or commercial surveillance methods have been mentioned in this ANPR; however, one physical security risk should be specifically stated and considered as it poses an increasing danger to a critical part of our nation's infrastructure, the judicial branch. Commercial surveillance practices that include the display and transfer of home addresses, phones, and email put all judicial officers and their families at risk. Whether by public record, data broker, data aggregator, map, or real estate websites … the display and transfer of that information increases potential harm to commissioners, referees, judges, and justices nationwide. Judicial officers' home addresses, phones, and emails should be included in any potential trade regulation rule to more adequately address physical security risks such as intrusion, vandalism, and violence.

2. FTC should consider judicial officers in discussions about collection, use, retention, and transfer of consumer data.

FTC should strive to implement limitations that would remove all judicial officer home addresses, phones, and email from source data prior to collection, or that would require the automatic redaction of the information immediately afterwards.

3. FTC should include protective measures for judicial officers in regulation, regardless of their consumer consent.

FTC should strive to restrict collection, display, and transfer of all judicial officers' home addresses, phones, and email without requiring special consent, or requiring them to research and follow multiple sets of opt in and opt out instructions.

Relevant Previous Council Action

None.

Analysis/Rationale

The opportunity to comment on proposed rulemaking that has the potential to address ongoing risks caused by data broker display and transfer of judicial officers' home street addresses, phones, and email is rare. Even a brief comment, in these circumstances, could help influence discussions and decisions that could lead to improved personal security.

Policy implications
The submission of comments on the Federal Register adds the Judicial Council's voice to the national dialog about consumer surveillance practices—the business of collecting, analyzing, and profiting from information about people—which affect the safety of all judicial officers.

Comments
Staff concurs with the recommendation of the CSAC.

Alternatives considered
The CSAC did not consider alternatives.

Fiscal and Operational Impacts
The CSAC's comments would not result in any known cost or implementational issues.

Attachments and Links
1. Attachment A: Proposed comments for Federal Register Commercial Surveillance ANPR, R111004
2. Attachment B: *Federal Register, Vol. 87, No. 161, Monday, August 22, 2022, p. 51273–51299*

CO/LG
cc: Judicial Council Trial Court Presiding Judges Advisory Committee
Judicial Council Court Executives Advisory Committee
Appellate Court Security Committee

Attachment A: Comments for Federal Register Commercial Surveillance ANPR, R111004 (to be filed at *www.regulations.gov* or mailed to Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue, NW, Suite CC-5610 (Annex B), Washington, DC 20580)

Commercial Surveillance ANPR, R111004

1. When discussing consumer harm, the FTC should take judicial officers into particular consideration.

A small portion of the potential consumer damages associated with deficient data security or commercial surveillance methods have been mentioned in this ANPR; however, one physical security risk should be specifically stated and considered as it poses an increasing danger to a critical part of our nation's infrastructure, the judicial branch. Commercial surveillance practices that include the display and transfer of home addresses, phones, and email put all judicial officers and their families at risk. Whether by public record, data broker, data aggregator, map, or real estate websites … the display and transfer of that information increases potential harm to commissioners, referees, judges, and justices nationwide. Judicial officers' home addresses, phones, and emails should be included in any potential trade regulation rule to more adequately address physical security risks such as intrusion, vandalism, and violence.

2. FTC should consider judicial officers in discussions about collection, use, retention, and transfer of consumer data.

FTC should strive to implement limitations that would remove all judicial officer home addresses, phones, and email from source data prior to collection, or that would require the automatic redaction of the information immediately afterwards.

3. FTC should include protective measures for judicial officers in regulation, regardless of their consumer consent.

FTC should strive to restrict collection, display, and transfer of all judicial officers' home addresses, phones, and email without requiring special consent, or requiring them to research and follow multiple sets of opt in and opt out instructions.