MUSLIM ADVOCATES

Submitted electronically via Regulations.gov

November 21, 2022

Re: Commercial Surveillance ANPR, R111004, Trade Regulation Rule on Commercial Surveillance and Data Security, request for public comment

I. Introduction and Request for Regulations to Protect Privacy

Muslim Advocates respectfully submits the following comment in response to the Federal Trade Commission's Advance Notice of Potential Rulemaking on Commercial Surveillance and Data Security, 87 FR 51273 (Aug. 21, 2022). We thank you for inquiring into the need for this rulemaking.

Muslim Advocates is a national legal advocacy and educational organization that works toward justice for Americans of all faiths. Muslim Advocates regularly receives complaints of surveillance and bigotry experienced by Muslims in the United States. Many of those complainants report fear of being surveilled and a helplessness to avoid surveillance as a Muslim in America. We hear reports of people facing the impossible choice between practicing a faith that sustains them and removing indicia of faith to avoid scrutiny and harm.

The surveillance that permeates all aspects of life in America flows in large part from commercial entities that collect and share consumers' private data. We request the Federal Trade Commission ("FTC") issue regulations that do at least the following:

- Require robust transparency, so consumers know what commercial actors are doing with consumers' data.
- Require commercial actors to return control over data to consumers – including control over what is collected, what is deleted, and what is traded – and to protect what data consumers allow companies to hold.
- Particularly protect people who are of minority status, such as Muslims, or who hold multiple intersectional minority statuses, such as Black Muslims.

T: 202 897 2622
F: 202 508 1007
info@muslimadvocates.org
www.muslimadvocates.org
P.O. Box 34440
Washington, DC 20043

II. Commercial Surveillance and Weak Data Security Harm Muslims and All Consumers

We are concerned with the increasing necessity of giving up privacy over personal data in exchange for participating in public life. As consumers, we are not told what data companies are collecting, nor the uses to which they put the data. Nor can we meaningfully direct companies to delete our data, to stop sharing or selling our data, or to maintain effective security over data they store. In short, our data is treated as belonging to the entities that scrape, store, surveil, and sell it, rather than as belonging to us. We call on the Federal Trade Commission to enact meaningful regulations to prevent commercial surveillance and to require secure data practices.

A. We need transparency to navigate unfair and deceptive data practices – including with regard to protected groups

Current surveillance and data practices unfairly burden consumers with choosing between services without knowing companies' data practices to understand the uses to which our personal information is being put. We can assume, however, that the data industry did not create $240 billion in value last year,[1] but rather harvested something valuable in the data they were collecting about consumers without our consent.

Recent investigations of government actors that buy commercially collected personal data and whistleblower reports from within companies indicate pervasive data sales and anti-Muslim practices. For example, Congressional questioning revealed that the Department of Homeland Security, the Federal Bureau of Investigation, the Internal Revenue Service, the Drug Enforcement Agency, and the Defense Department have spent millions of taxpayer dollars to buy Americans' cell phone location information collected by phone companies, sold to data brokers, and resold to federal agencies.[2] Public records litigation against the Los Angeles Police Department shed light on how a social media monitoring firm, Voyager Labs, marketed its alleged ability to predict

[1] FORTUNE BUSINESS INSIGHTS, MARKET RESEARCH REPORT: BIG DATA ANALYTICS MARKET SIZE, SHARE & COVID-19 IMPACT ANALYSIS…, July 2022. While the resulting loss of privacy may be incremental to each individual, it accretes to impose a significant harm across society. Indeed, nearly every teen and adult in the United States loses privacy over their actions and data due to the country's permissive data surveillance regime.

[2] *See, e.g.*, Sara Morrison, *A surprising number of government agencies buy cellphone location data. Lawmakers want to know why*, VOX, Dec. 2, 2020; Elizabeth Goiten, *The government can't seize your digital data. Except by buying it*; WASH. POST, Apr. 26, 2021; *see also* production responsive to ACLU FOIA demand.

criminality by searching for evidence of Muslim and Arab identity.[3] Whistleblowers have revealed how social media algorithms allow anti-Muslim bias, xenophobia, and white nationalism to flourish without triggering meaningful industry change.[4]

We urge the FTC to require transparency from commercial actors about their data practices and algorithms so that consumers can meaningfully understand what data are collected, how data are stored, shared, spliced, and sold, as well as how algorithms direct information and access.

B. We need privacy protections for outgroups, including Muslims

Within the highly surveilled American society, Muslims are among the groups singled out for particular scrutiny. Many Muslims were disquieted by discoveries that apps aimed at Muslims - mostly Qibla[5] compasses and prayer time alerts used to orient the faithful to Mecca at prayer time - collected, stored, and sold their geolocation data to brokers who sold the information to those who would pay, including to law enforcement agencies and the U.S. military.[6] Companies like Voyager Labs that are willing to exploit bigoted presumptions – including the use of Muslim identity as a proxy for criminality – to track the data of members of minority communities, and

[3] Rachel Lebinson-Waldman and Mary Pat Dwyer, *LAPD Documents Show What One Social Media Surveillance Firm Promises Police* ("Brennan Report"), BRENNAN CENTER, Nov. 17, 2021.
[4] *See, e.g.*, MEGAN SQUIRE, NETWORK ANALYSIS OF ANTI-MUSLIM GROUPS ON FACEBOOK, 10th Internat'l Conf. on Soc. Informatics (2018); Ishmael Daro, *Here's How Anti-Muslim Groups on Facebook Overlap With a Range of Far-Right Extremism,* BUZZFEED NEWS (Aug. 4, 2018); Melissa Nan Burke, *Tlaib not cowed by 'hateful' threats, behavior*, THE DETROIT NEWS (Jan. 28, 2019); Will Carless and Michael Corey, *American cops have openly engaged in Islamophobia on Facebook, with no penalties*, REVEAL NEWS, June 27, 2019; TECH TRANSPARENCY PROJECT, WHITE SUPREMACIST GROUPS ARE THRIVING ON FACEBOOK, May 21, 2020; Olivia Solon, *Facebook ignored racial bias research, employees say*, NBC NEWS, July 23, 2020; TECH TRANSPARENCY PROJECT, FACEBOOK'S BOOGALOO PROBLEM: A RECORD OF FAILURE, Aug. 12, 2020; GLOBAL PROJECT AGAINST HATE AND EXTREMISM & MUSLIM ADVOCATES, COMPLICIT: THE HUMAN COST OF FACEBOOK'S DISREGARD FOR MUSLIM LIFE, Oct. 21, 2020.
[5] Qibla is the direction of the sacred shrine of the Kaaba in Mecca toward which Muslims face to perform prayers. A Qibla compass directs which way to face to perform prayers.
[6] *See, e.g.*, Counsel on American-Islamic Relations, *In the Matter of Request for Investigation of Alleged Violations of Section 5 of the FTC Act by Multiple Actors in the Location Data Industry*, Apr. 12, 2022; Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE MOTHERBOARD, Nov. 16, 2020; Sofia Turki, *Google Bans Dozens of 'Spy Apps with Ties to U.S. Government,' Muslims Targeted*, AL-ESTIKLAL NEWSPAPER, Apr. 22, 2022.

then sell the data to law enforcement and other actors that share anti-Muslim bias,[7] indicate the need for particular protections for outgroups.

The well-documented harmful effects of surveillance on members of Muslim communities include anxiety, depression, self-censorship, and avoidant behaviors.[8] As noted in a response to news about Muslim Pro's data breaches: "Surveilled communities know that surveillance does not keep anyone safe, but only breeds countless forms of community harm. We begin to question everything when we are surveilled, from our own reality and the safety of our friends and family, to our own humanity."[9] While in part behavioral and emotional, these harms have real impacts on people's finances and social well-being, as well as to psyches, community cohesion, and society. Yet due to the ubiquity and opacity of surveillance and data practices, consumers cannot reasonably avoid these surveillance and data sharing harms except by disconnecting from services – including internet-connected products, online communities, and credit cards - that are increasingly essential to modern life.

Surveillance and data sharing based on Muslim religiosity – such as that done by Muslim Pro, the New York Police Department, and social media surveillers – is particularly problematic because it targets Muslims not only on account of their religion, but also on account of their level of practice. Thus, Muslims who track prayer times are doubly surveilled and those who do not, are not. Such surveillance of Muslims in the very practice of religion pressures them to choose between reclusing themselves from society or foregoing their religious practices.

[7] *See, e.g.*, Brennan Report *infra* note 3; citations related to Muslim Pro *supra* note 6.
[8] *See, e.g.*, Farhana Jahan, *Under Surveillance and Overwrought: American Muslims' Emotional and Behavioral Responses to Government Surveillance*, J. MUSLIM MENTAL HEALTH, Vol. 8, Issue 1, 2014 (increased anxiety and avoidant behaviors associated with surveillance); Karen Turner, *Mass surveillance silences minority opinions, according to study*, WASH. POST, Mar. 28, 2016 (knowledge of surveillance leads to non-participation and self-censorship for non-dominant opinion holders). *Cf.* CLEAR, MACLC, and AALDEF, MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS (finding surveillance suppressed religiosity, stifled speech, limited association, sowed suspicion, and severed community connections). Surveillance in the digital world greatly expands these harms because technology is pervasive and does not sleep.
[9] Vanessa Taylor and Sumaiya Zama, *Praying Away Surveillance: A Reflection on Muslim Pro*, SUBSTACK, Nov. 18, 2020.

When your community is presumed guilty and your religious practice is itself criminalized[10] mere surveillance is a threat to safety. We urge the FTC to protect Muslims, and other minority groups, from surveillance based on faith, religiosity, or other community-specific characteristic.

Finally, we call on the FTC to issue regulations that use disparate impact metrics to determine companies' compliance. History tells us that marginalized groups are harmed at disproportionate rates unless enforcement systems specifically identify and redress harms they experience. In other words, data analysis of a company's *practices* and *impacts on protected groups* must be the measure of compliance or violation, rather than the words of a policy document that may be entirely ignored or unevenly applied.

Thank you for your attention.

Respectfully submitted,

Naomi Tsu

Naomi Tsu
Interim Legal Director
Muslim Advocates

[10] *See, e.g.*, Joseph Gerteis *et al.*, *Racial, Religious, and Civic Dimensions of Anti-Muslim Sentiment in America*, 67(4) SOCIAL PROBLEMS 719, Nov. 2020 (finding that nearly half of Americans hold anti-Muslim views).