August 21, 2020

Chairman Jerrold Nadler
2138 Rayburn House Office Building
Washington, D.C. 20515

Chairman David Cicilline
2233 Rayburn House Office Building
Washington, DC 20515

Re: The Anticompetitive Risk Of Consolidated Biometric Training Data

Dear Chairman Cicilline, Ranking Member Sensenbrenner, and Members of the Subcommittee:

My name is Albert Fox Cahn, and I serve as the Executive Director of the Surveillance Technology Oversight Project ("S.T.O.P."), a New York-based privacy and civil rights group. I write in response to recent hearing on Online Platforms and Market Power hearing by the House Judiciary Committee’s Subcommittee on Antitrust, Commercial, and Administrative Law.

Big tech systematically erodes users’ privacy, harvesting ever-growing amounts of our data. Firms monetize our most intimate moments, manipulate our psychological state, and enable abuses ranging from political disinformation to police targeting. Increasing market power leads to a vicious cycle wherein increased user reliance enables the development of ever more invasive forms of artificial intelligence, further cementing incumbent firms’ anticompetitive advantage.

I. AI Training Data Is Market Power

As the Subcommittee considers Big Tech’s anticompetitive conduct, we urge you to examine the monopolistic impact of consumer surveillance products. 1 Amazon Web Services (AWS) provides cloud services for all 17 United States intelligence agencies, including the FBI and DEA, 2 and reporting revealed the FBI was piloting Amazon’s facial recognition tool. 3

Surveillance partnerships between thousands of police departments and Amazon’s internet-connected doorbell company Ring give law enforcement agents unprecedented access to surveillance


data. Amazon is then able to work in tandem with their law enforcement customers to stoke false and racially discriminatory hysteria over “rising crime,” helping Amazon sell more products and feeding police more and more data on our movements and daily life.\(^5\)

Ring is potentially consolidating biometric data on every person who happens to walk within range of one of their doorbells, and Amazon has expressed their intention to use their growing database of faces to develop artificial intelligence (AI)-powered products.\(^6\) Google Nest, a competitor of Ring, has also been using machine learning to build complex AI-powered systems.\(^7\)

Biometric AI, such as facial recognition, requires vast training sets, coded databases of photos, movies, and audio recordings that enable AI systems to better identify human beings by their biological characteristics. Training data is the lifeblood of artificial intelligence, with access to greater data translating into more powerful AI. A company’s likelihood of success in the AI space is directly tied to their access to massive amounts of detailed data to train new systems.\(^8\) Tech giants possess orders of magnitude more data than any of their competitors, giving them a huge advantage when it comes to developing effective AI.\(^9\) In this way, the expansion of Big Tech’s consumer surveillance products risks the creation of an insurmountable barrier to entry for rival firms who will never have enough training data to compete.

Tech giants have been locked in a race to rapidly consolidate their market share in the AI space more broadly, acquiring competitors as well as their data to scale their own AI initiatives. AI acquisitions saw a more than sixfold increase between 2013 and 2018, with Amazon, Google, Apple, Facebook, and Microsoft leading the race.\(^10\)

---


This winner-take-all pattern operates in a cycle: more data means more effective machine learning, which enables tech giants to introduce better functioning products to the market faster, amassing more users and thus more data. Absent taking action to interrupt that cycle, we are on track towards a world in which social, political, and economic power is disturbingly centralized.

II. Structural Separation Is the Only Effective Remedy

The forgoing concerns require lawmakers and enforcement agencies to pursue structural separation of America’s largest tech firms. While there is generally a poor track record of enforcement agencies using behavioral regulation to remedy anticompetitive conduct, the track record for tech giants is particularly poor.

All too often, tech giants are so profitable that even record-level fines are nothing more than the cost of doing business. Facebook alone has paid a $5 billion fine for violating consumers’ privacy and a $122 million fine to Europeans regulators for improperly sharing WhatsApp.

Google has paid a $170 million fine for tracking the viewing histories of children on YouTube and was subject to investigation by the FTC for anticompetitive practices from 2011 to 2013, though commissioners voted unanimously to end the investigation two years later without Google making any real changes to their policies.

Even if the fines and penalties threatened as part of behavioral regulation were sufficient to deter misconduct, any regulations or consent decrees would quickly fall out of date. Given the pace with which these industries shift, safeguards that are meaningful today could easily be circumvented tomorrow. The products and services change, only the monopoly power remains.

III. Conclusion

Left unchecked, tech giants’ monopolistic power will only grow in the coming years. As artificial intelligence, and particularly biometric analytics, become more central to more parts of the American economy, the danger of unchecked training data aggregation will grow. Incumbent


monopolists must not be permitted to use their control over biometric data collection to establish
the same type of dominance over artificial intelligence that they’ve held for the past decade over
Internet-based commerce and communications. If they do, it will not only mean a generational
setback for open competition, but it will undermine the very fabric of our democracy.

Sincerely,

________________
Albert Fox Cahn, Esq.
Executive Director