



July 23, 2020

Congressman David Cicilline
Chair, Subcommittee on Antitrust, Commercial, and Administrative Law

Congressman F. James Sensenbrenner
Ranking Member, Subcommittee on Antitrust, Commercial, and Administrative Law
House Judiciary Committee

RE: Amnesty International Statement for the Record for July 27 Hearing on “Online Platforms and Market Power, Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google”

On behalf of Amnesty International USA and our members and supporters in the United States, we hereby submit this statement for the record to address how the dominant power of Big Tech represents a systemic threat to human rights.

Competition and antitrust remain key tools for challenging the power of Big Tech. However, at this unprecedented juncture, Amnesty urges you to consider taking this opportunity to question the surveillance-based business model itself.

In Amnesty’s November 2019 report *Surveillance Giants: How The Business Model Of Google And Facebook Threatens Human Rights*,¹ we drew attention to Google and Facebook as pioneers of a business model that is predicated on harvesting, analyzing, and profiting from people’s data. This surveillance-based business model fundamentally undermines the right to privacy and threatens other human rights, including the rights to freedom of expression and opinion, freedom of thought, and the right to equality and non-discrimination.

One of our key concerns is how Google’s and Facebook’s business models have enabled them to establish near-total dominance over the primary channels through which people connect and engage with the online world and access and share information online, making them gatekeepers to the “public square” for much of humanity. The dominance of Google and Facebook over core platforms of the internet poses unique risks for human rights.

Google and Facebook have unparalleled power over people’s lives online through having established control over the primary channels that most of the world relies on to engage with the internet. Outside of China, the dominance of Google and Facebook is starkly evident in each of the following areas: Social media, messaging, search, video, web browsing, mobile platforms and digital advertising. These platforms mediate the ways people seek and share information, engage in debate, and participate in society. These products have become fundamental to the modern world and how people interact with each other.

¹ Amnesty International, “Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights,” Nov. 2019, <https://www.amnesty.org/en/documents/pol30/1404/2019/en/>.

Access to the internet has long been recognised as a critical enabler of human rights in the digital age.² The role of Google and Facebook as “gatekeepers” to the digital world means that they have significant influence over people’s enjoyment of human rights online; indeed, most internet users are reliant on the services the companies provide. As such, the platforms have become fundamental to how people are able to exercise their human rights online and are used every day in ways that facilitate freedom of expression, the rights of peaceful assembly and association, and other rights.

The dominance of the companies’ platforms means it is now effectively impossible to engage with the internet without “consenting” to their surveillance-based business model. This has created a paradoxical situation in which, in order to access the internet and enjoy their human rights online, people are forced to submit to a system predicated on interference with the right to privacy on an unprecedented scale, with corresponding impacts on a range of other human rights. This false choice was recently recognised by Germany’s highest court in a ruling on Facebook and antitrust.³

The increasing power of Google and Facebook as gatekeepers to the ways people engage with the digital world has been a key driver of the erosion of privacy online. Various analyses charting the rise to dominance of Google and Facebook show that the companies were able to incrementally increase the breadth and depth of their surveillance in parallel with their control over the primary channels of the internet and the decline in any meaningful alternatives.⁴ Last year, the UK House of Lords found that “Providers of these services currently have little incentive to address concerns about data misuse or online harms, including harms to society.”⁵

Google and Facebook’s business model has in-built tendencies to exponentially increase the platforms’ dominance and scale, and as such, the abuse of privacy and other rights has also helped concentrate power. The business model’s extraction and analysis of data results in specific data-driven network effects. The accumulation of greater amounts of data enables a company to be better able to train the machine-learning models and algorithms which produce behavioural predictions. In turn, these predictive functions are deployed to keep people on the platform, generating further data and maintaining control over data flows. Better predictive functions also lead to greater advertising revenue, enhancing the value of the platform and the company’s power in the market. This system of feedback loops, combined with traditional network effects, has been instrumental in rapidly expanding the scale and impact of the platforms, and thereby concentrating the power of Google and Facebook over the digital world.

Google and Facebook have also been able to use their data-driven advantages to actively prevent the development of alternative services. They do this in several ways: by “tying” one service to

² Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report to the Human Rights Council, 16 May 2011, UN Doc A/HRC/17/27,

³ New York Times, *Facebook Loses Antitrust Decision in Germany Over Data Collection*, 23 June 2020 <https://www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html>.

⁴ See for example Zuboff, 2018; Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist’s Journey Towards Pervasive Surveillance in Spite of Consumers’ Preference for Privacy*, 16 Berkeley Bus. L.J. 39, 2019,

⁵ UK House of Lords Select Committee on Communications, *Regulating in a Digital World*, March 2019, para 45,

another, leveraging dominance in one area to try to increase dominance in another; by downranking the services offered by would-be competitors on their own platforms (in, e.g., search results); and by stifling companies offering similar or potentially competing services by either copying them or purchasing the company outright.

Power obstructs corporate accountability

The speed at which Google and Facebook's platforms have grown to such a vast scale, operating across borders, has meant that state-based regulation has struggled to keep pace with the companies' impacts on people's rights.

The scale and complexity of the human rights harms linked to the surveillance-based business will require a smart mix of structural solutions to address the systemic nature of the threat. Those solutions must include measures that disrupt the market and its incentives for corporate surveillance-based business models. Lawmakers and regulators must limit the depth and scale of data harvesting, prevent major gatekeeper platforms from combining data across services, and ensure that key components of the data infrastructure are not concentrated into the hands of a few companies. Measures that "break up" the platforms, while potentially important, will fail to address systemic human rights abuses unless they holistically tackle the underlying surveillance-based business model itself.

Only a combination of enforcement actions and new legislation and regulatory frameworks will meaningfully address an underlying business model that threatens the rights to privacy and freedom of expression and generate greater government oversight of technology companies such as Facebook and Google. These efforts also have the potential to ensure such companies meet their responsibility to respect human rights.

Congress must enact statutory frameworks to ensure people are able to practically exercise their right to choose privacy-respecting alternatives to surveillance-based business models. For example, rather than merely focusing on data access, lawmakers should adopt measures to ensure interoperability between platforms so so companies are consistent in how they store, process, and transfer data so that people can easily move between services without social detriment and to lessen network effects. This is a key proposal under discussion for Europe's current digital reforms.⁶

For too long Big Tech has been held unaccountable. Amnesty thanks the House Subcommittee on Antitrust, Commercial, and Administrative Law for holding this landmark hearing bringing together the CEOs of four of the world's most powerful tech companies to investigate their dominance of the online economy. Legislators cannot allow Big Tech to continue to abuse its colossal power over our everyday lives. Congress must ensure that public digital space is reclaimed from a powerful and unaccountable few and demand that it is accessible to all, with respect for human rights at its core.

These companies testifying before the Subcommittee have a responsibility to respect our human rights, including the right to privacy, wherever and however they operate. To make sure they fulfil

⁶ Joint letter to European Commission's Executive Vice-President Vestager, *Call to include interoperability provisions as part of the Digital Services Act*, 6 July 2020 <https://www.eff.org/document/letter-vestager-interoperability>

that responsibility, we need effective government regulation to set stricter limits on the kind of data these firms collect, what inferences can be drawn from that data and how that data is used to target and influence us by third parties, including advertisers. Governments are required under international human rights law to protect our rights against abuse by companies. Crucially, that also means challenging the dominance of the platforms through regulatory tools including, but not limited to, antitrust measures.

Recommendations

In this light, Amnesty International calls on the Subcommittee to support the enactment of legislation to:

- Ensure that access to and use of essential digital services and infrastructure – including those provided by Google and Facebook – are not made conditional on interference with the right to privacy. This means guaranteeing people a right not to be tracked by advertisers and other third parties;
- Prevent companies from making access to their services conditional on individuals “consenting” to the collection, processing or sharing of their personal data for marketing or advertising;
- Enact measures that will enable consumers to choose privacy-respecting alternatives to surveillance-based business models.

For further information, please contact Michael Kleinman, Director of Amnesty International’s Silicon Valley Initiative, at mkleinman@aiusa.org, and Charanya Krishnaswami, Amnesty’s Americas Advocacy Director, at ckrishna@aiusa.org.

Sincerely,



Michael Kleinman
Director, Silicon Valley Initiative



Charanya Krishnaswami
Americas Advocacy Director