

Microsoft's Response to Access Now's October 3, 2019 Letter

Thank you for your October 3, 2019 letter on Microsoft's scoring in the Ranking Digital Rights [Corporate Accountability Index](#).

We have a responsibility and commitment to operate our business in a way that respects universal rights such as privacy, freedom of expression and the right to access information. At Microsoft, respecting human rights is a critical component of our mission to empower every person and every organization on the planet to achieve more. A focus on human rights helps our employees to make good decisions and ethical choices, and builds trust with our customers and partners. As articulated in Microsoft's [Global Human Rights Statement](#) we work to ensure that our business activities respect and promote human rights to ensure that technology plays a positive role across the globe.

Our approach is aligned with the UN Guiding Principles on Business and Human Rights (UNGPs) as the authoritative global standard for business and human rights. Additionally, we are a founding member and serve on the board of the Global Network Initiative (GNI), a multi-stakeholder collaboration between information and communications technology (ICT) companies, civil society organizations, socially responsible investors, and academic institutions to protect and advance freedom of expression and privacy in the ICT sector.

Regarding Access Now's "one timely, and achievable, objective based on [Access Now's] insights into the most acute issues facing at-risk users" recommendation that "Microsoft should be more transparent about restrictions on freedom of expression by clarifying its policies for notifying users when it restricts access to content or accounts, either due to government requests or as a result of enforcing its own rules", we would like to provide the information below.

For Microsoft's hosted consumer services evaluated by RDR, our practice is to notify users of the removal of specific content or suspension / termination of their accounts within the applicable service itself. However, there are situations where user notice would be inappropriate or counterproductive – for example if the user content or user activity involves unlawful activity or harm to others.

We would also like to highlight other recent examples of our efforts regarding the privacy rights of our users:

- Before the introduction of the GDPR we announced that we would [extend the rights at the heart of GDPR to all of our consumer customers worldwide](#). "Known as Data Subject Rights, they include the right to know what data we collect about you, to correct that data, to delete it and even to take it somewhere else. Our privacy dashboard gives users the tools they need to take control of their data." On the first anniversary since the GDPR went into effect we

announced that [more than 18 million people from around the world have used our tool to manage their personal information](#). The highest level of engagement, both on a per capita basis and in absolute numbers, came from the United States where around 6.7 million people have used the dashboard. In that same announcement we also expressed our support for the California Consumer Privacy Act (CCPA) which goes into effect on January 1, 2020, and called for the US Congress to take inspiration from the rest of the world and enact federal legislation that extends the privacy protections in GDPR to citizens in the United States.

- In September 2019 we reaffirmed that except in extraordinary circumstances [government agents should seek data directly from our enterprise customers, and if they seek our customers' data from us they should allow us to tell our customers when demands are made](#).

While we agree that secrecy orders that prevent us from notifying our customers may be appropriate in limited circumstances, we also believe there are times when those orders go too far. In those cases, we will litigate to protect our customers' rights. We filed a lawsuit in late 2018 to protect these rights, which was recently unsealed by a U.S. District Court. In September 2018, Microsoft challenged a secrecy order issued by a federal magistrate judge in Brooklyn, New York in connection with a federal national security investigation. The secrecy order prevents Microsoft from notifying our enterprise customer that we received a warrant seeking its data. Based on the limited information available to us in this case, we feel the secrecy order was too broadly drawn and is inconsistent with the U.S. government's policy that secrecy orders be narrowly tailored. We argued to the court that there must be an executive or representative of the company (our customer) – which has thousands of employees – who can be notified of the warrant's existence, without jeopardizing the federal law enforcement investigation. The lower court denied our effort to modify the secrecy order to permit that notification. We have challenged that order in the lower court, and we will pursue an appeal in the appellate court if necessary, and continue to stand up for the principle that our customers are entitled to know when the government obtains their data.

Further information about our policies and practices to respect customers' privacy and freedom of expression is available in our [Reports Hub](#), [Privacy Statement](#), and [Corporate Social Responsibility Report](#).

We value ongoing opportunities to learn from all stakeholders as we continue to implement our human rights policies and practices.