Microsoft

Our commitment to privacy

Principles and practices concerning government access to enterprise customer data

Microsoft

Microsoft's principles and practices for responding to government data requests

Business customers and partners around the world have raised serious questions and concerns as a result of recent disclosures about government surveillance. We share many of these concerns.

Microsoft's longstanding commitment to protecting customers' privacy and security has guided our actions over the years. Those commitments extend to how we respond to lawful government demands for customer information from every government, whether those requests are for the purposes of criminal law enforcement or national security.

- Microsoft is sometimes obligated to comply with legal orders from governments around the world. These demands might relate to criminal law enforcement or to national security but Microsoft's principles in responding to any legal orders we may receive are the same.
- Microsoft provides enterprise customer data only when required by a valid legal order that is targeted at specific accounts. Even then, we always attempt to redirect such requests to the customer and notify the customer promptly, unless legally prohibited from doing so.

There has been confusion as people try to understand the many sensational press reports, some of which have significantly exaggerated the amount of data Microsoft provides to the U.S. government. To address this, we fought for and won the right to publish more detailed data, which shows that all government demands – from law enforcement and national security authorities –impact only a tiny fraction of Microsoft's customers.

To be clear, here's what we don't do:

- We don't provide any government with direct or unfettered access to your data.
- We don't assist any government's efforts to break our encryption or provide any government with encryption keys used to protect data in transit, or stored on our servers.
- We don't engineer back doors into our products and we take steps to ensure governments can independently verify this.
- If, as press reports suggest, governments are engaging in broader surveillance of communications, it is being done without the knowledge or involvement of Microsoft, and we are taking steps to enhance the security our customers' data while it is in transit and at rest.

What our customers and partners should know:

- As of the date of this document, Microsoft has not been compelled to provide any enterprise customer data pursuant to a national security law. In this document, "enterprise customer" means customers with more than 50 licensed users or seats.
- As of the date of this document, Microsoft has not been compelled to provide customer data for an enterprise customer based outside the U.S. for any reason.
- For the last six months of 2013, we received only three legal orders for data associated with use of our commercial services by our enterprise customers, concerning 15 accounts. All these orders arose out of criminal law enforcement actions.

For current information, please visit the following:

- *Providing additional transparency on U.S. government requests for customer data*: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/02/03/providing-additional-transparency-on-us-government-requests-for-customer-data.aspx
- *Microsoft's Law Enforcement Requests Report*: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/pppfaqs/