

Wickr Transparency Report

By Jennifer DeTrani, Wickr General Counsel
August 4, 2013

Our Philosophy:

Wickr received its first government request to hand over data in February of this year, however, because Wickr requires all data requests to go through the U.S. judicial system no information regarding the requested user account was disclosed.

We believe in maintaining a level of transparency with respect to government and court ordered requests and that your data belongs to you. Furthermore, because of the manner in which messages on Wickr are encrypted, even with a properly issued subpoena, Wickr can never provide the content of the messages. Content is protected in transit and at rest and is only readable by you and your intended recipient. We can only provide a snapshot of the account at a given moment and such details as the date of creation of an account, the type of device on which the account is used, and the date of last use of the account. For more information on what type of information we collect related to your account, please read our privacy policy at <https://www.mywickr.com/en/privacypolicy.php>.

Wickr is committed to sharing the number of requests for user information that we receive from law enforcement and how we handle them.

Government Requests:

Country	Reporting Period	Gov't Requests	Accounts Associated	Response Rate
United States	January 2013 to August 1, 2013	0	0	0
Non-United States	January 2013 to August 1, 2013	<10	<10	0

Action to Date:

As of the date of this report, Wickr has not been required by a FISA request to keep any secrets that are not in this transparency report as part of a national security order.

Our Promise:

As the electronic landscape continues to expand and change with regard to user's privacy rights, we remain committed to remaining transparent with our users and various government entities. That having been said, there are no back doors. What you see is what you get.

Prediction of the Future:

In light of recent events involving data-collection practices within the U.S., it is apparent that certain government organizations are eager to gain access to user information for various reasons pursuant to the PRISM Program. We at Wickr are cognizant of such practices but maintain that due to the specific architecture employed by Wickr there are no back-doors to our system. Therefore, should such lawful government requests arise, we will wholly comply, however, such compliance will be limited to metadata based on the specifics of the proprietary encryption process. In other words, while user data requests may certainly increase in the future, our goal is to address them honestly and openly with the understanding that such data requests will reveal only account information, never content, given the nature of our unique technology.