Wickr Transparency Report

By Jennifer DeTrani, Wickr General Counsel
May 9, 2014

Our Philosophy:

By giving back Power to the People, Wickr is working on developing the most secure communications system in the world which protects the interests of our users while adhering to the letter of the law.

Wickr requires a warrant supported by probable cause prior to handing over the content of user communications. Therefore, while we receive *informal* requests or inquiries from law enforcement around the world, we have yet to receive a single formal law enforcement/government request for information regarding our users or their accounts.

Our zero-knowledge system was designed without a central point of failure or control. We do not have a master key nor do we possess your personal information. We designed it this way to protect our friends and families.

If and when lawful government requests arise, we maintain that we will wholly comply. However, such compliance will be limited to metadata based on the specifics of our proprietary encryption process. In other words, we remain committed to resolving lawful user data requests with honesty and openness with the security of knowing that such data requests will reveal only account information, never content, given the nature of our unique technology.

This month in Washington, we received informal confirmation that there is no legal authority which requires a change to our software to create keys to our information that do not otherwise exist.

This means that even with a properly issued warrant, 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.*

More information regarding our law enforcement guidelines can be also be found on our website.

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 (informal and formal):

Country	Reporting Period	Gov't Requests	Accounts Associated	Response Rate
United States	December 31, 2013 to April 1, 2014	<10	<10	0
Non-United States	December 31, 2013 to April 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 ability to make such a statement is proof positive that Wickr is a safe mode of communication. Should this language disappear, that will no longer be the case.

Our Continued Promise:
We believe we were the first company to deploy the 'warrant canary' contained in the statement above. Our canary was placed in the transparency statement last year after much deliberation based on the unwavering belief that our users deserve to know that their communications remain secure. We will continue to use the warrant canary to preserve our users' rights.

Therefore, our continued promise to you is to provide you with the tools to protect your privacy rights and to disclose to you any and all government requests we receive for your information through user notification and the warrant canary.

Prediction of the Future:
While companies have been demanding the ability to disclose governmental requests, the government, in turn, is demanding more from certain companies who have misled their users by marketing privacy and security and then failing to follow-through with their promises.

Privacy and security are no joking matters.

'Do what you say' and 'Say what you do' are the edicts that we believe in at Wickr.

Our Bug Bounty is our way of putting our money where our mouth is. If there are vulnerabilities in our system, we want to be the first to know about them so we can address them head-on.

We maintain that a company that holds its users' communications in trust should operate with the highest level of integrity. We intend to set the gold standard for that and hope that our competitors will follow suite.

Part of that integrity comes from having a clearly written privacy policy and terms of use that spell out for users what they are agreeing to when they sign on for service.

Many companies actually turn these terms into 'Ownership Policies' and take the position that your data belongs to them by virtue of use of their product. What most consumers fail to realize is that hidden within these companies' terms is a FREE, WORLDWIDE, TRANSFERABLE LICENSE to use their data as they see fit.

We at Wickr, knowing that very few consumers take the time to review these policies and terms, believe that they are unconscionable and we hope to see consumers stepping up to protect their own rights and saying 'no' to these terms. We can envision the FTC weighing in here as well – and forcing companies to rectify these one-sided agreements.

Wickr on.