Transparency Report
By Jennifer DeTrani, General Counsel
August 1, 2016

Wickr is committed to meeting and exceeding industry standards for transparency reporting. In this report you will discover the details of the past seven months of our receipt and responses to user information requests or legal processes from January 1, 2016 until July 31, 2016. Additional information can be found in our Legal Process Guidelines.

Our Philosophy & Impact

At Wickr, we hold a long-standing belief that transparency is a prerequisite to earning our users' trust and growing our platform. And while the messages we secure will *never* be outwardly visible, our practices, policies and philosophies – especially as they relate to how our privacy practices - should be front and center.

In line with this belief, we will be expanding our reporting practices by shifting to a semi-annual transparency reporting practice in lieu of quarterly reporting. This will allow for a more detailed historical account of all requests we receive over a more extended time period. Similarly, the form that our transparency reporting takes may change over time as we determine the best way to inform our users about requests for their information.

Changes to Reporting Practices

In line with recommendations set forth in the Transparency Reporting Toolkit – a project by New America's Open Technology Institute and Harvard University's Berkman Center for Internet & Society – our transparency reporting is shifting to exemplify recommended 'best practices'. One of the challenges identified in the Toolkit is to move transparency reporting to a more standardized format which will allow consumers to more readily understand what the reporting actually means. We encourage users to review this document, as we did, to learn more about how user data is processed and produced by companies across the Internet and telecommunications industries, as well as the best practices at play in these spaces. We all have a lot to learn from each other.

FAQs

When Does Wickr Provide Law Enforcement with Details on its Subscriber Accounts?
Wickr cooperates with law enforcement by providing information related to its users' accounts only when properly served with legal process or in life-or-death situations.

What Kinds of Information Does Wickr Turn Over on Those Accounts?
Wickr can provide non-content information describing an account such as: date of its creation, the date of last use, the total number of messages sent and/or received, the type of device on which the account was created. See our Legal Process Guidelines for the full list.

When Does Wickr Provide Law Enforcement with Subscriber Content?
Never! Our system is designed to protect our users' privacy such that we never have access to our users' decrypted message content so can't pass it on to anyone else.

wickr

August 1, 2016 Reporting Statistics[1]

Reporting Period	Types of Requests Received	Numbers of Requests Received	Accounts Associated with Requests Received	Accounts Receiving Notice of Request[2]
January 1, 2016-July 31, 2016	**United States**			
	Search Warrants[3]	1	2	0
	Court Orders[4]	18	48	0
	Law Enforcement Subpoenas	18	33	2
	National Security Requests[5]	0	0	N/A
	Other Requests[6]	8	11	0
	Non-United States			
	Non-U.S. Requests[7]	1	3	0

[1] Wickr is committed to sharing information about the requests it receives for its users' account information. Above is a table detailing requests received for our users' information from January 1-July 31, 2016. Our next report will present data from August 1, 2016 through December 31, 2016.

[2] Wickr notifies users of requests for their information including providing a copy of the legal process, unless required by a non-disclosure order not to do so or when disclosure is not practicable or would not be fruitful such as when a user does not exist, a request is withdrawn, or in an emergency situation such as a missing person investigation.

[3] "Warrants" are used to obtain information which may be similar to information available to a requestor through a subpoena or court order except that requestors often seek the ***content*** of the communications through the use of a warrant. Therefore, in order to get a warrant, law enforcement must demonstrate 'probable cause' to a court that the requested information evidences a crime.

[4] "Orders" are signed by a judge and may include the following: Non-Disclosure Orders requiring us to keep private a request for users' account information, 2703(d) Orders under the Electronic Communications Privacy Act (the federal law that regulates law enforcements' access to customer data and content) in both civil and criminal cases, as well as Pen Register Orders which provide for real-time disclosure of non-content data.

[5] "National Security Orders" includes orders authorized and issued under the Foreign Intelligence Surveillance Act (FISA) and National Security Letters authorized by the Stored Communications Act (SCA).

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

[6] "Other Requests" may include Preservation Requests, Emergency Disclosure Requests, and Civil Requests including Subpoenas. Preservation Requests are requests by law enforcement for preservation of a users' non-content account information for up to 90 days until such time that it serves the proper legal process to receive such information. Emergency Disclosure Requests are requests from a government agency in exigent circumstances involving life or death. We review and process emergency requests upon a showing that the information provided will help save lives.

[7] "Non-U.S. Requests" include formal legal processes deriving from foreign governments. We require that any such requests conform to the Mutual Legal Assistance Treaty (M.L.A.T.) or letters rogatory process.