Wickr Transparency Report

By Jennifer DeTrani, General Counsel
September 29, 2015

Our Philosophy & Impact

The number of mobile devices has skyrocketed in the past 5 years. Almost 1.3 billion people are now part of a mobile global workforce, constantly communicating and regularly transferring sensitive business and personal data. With that growing connectivity comes a threat landscape that is rapidly expanding, with new critical vulnerabilities in major technologies revealed almost daily. Government information systems and critical corporate networks have experienced large-scale breaches exposing high-value data and communications further reinforcing the need to secure vulnerabilities as a matter of national security and corporate best practices.

An understanding of these emerging trends compelled our team to build a platform and a company which can withstand security threats while providing real-time private communications to our users around the world. Wickr's communications platform enables encryption between devices in such a way that unencrypted user data never touches our servers. Further, from a compliance standpoint, our encryption technology meets and exceeds data protection requirements for financial, healthcare, education, and national security purposes.

In recognition of Wickr's vision and unwavering commitment to building a private communications platform which advances the security of individuals and businesses worldwide, the World Economic Forum has named our company a 2015 Technology Pioneer. Wickr is proud to join an outstanding community of innovators and thought leaders including Mozilla, Wikimedia Foundation, Ushahidi, Twitter, Palantir Technologies, CloudFlare, and GitHub, to name just a few of the companies who were recognized for being motivated 'more by a sense of mission than a desire for profit.'

We believe in robust and widespread cross-industry encryption and urge the U.S. government to adopt strong encryption standards to ensure the integrity of information of individuals, businesses and government agencies across the world. With record numbers of information breaches occurring daily, higher security standards are in order. The recent court decision in Wyndham Hotels v. Federal Trade Commission (FTC) extending the FTC's authority to data security further validates the need for urgent implementation of sufficient baseline protections for companies who are entrusted with consumers' personal data. With increased FTC regulatory oversight, maintaining transparent and accurate data protection policies is now equally important to companies seeking to establish trust with their users and compliance with national regulations.

Wickr is passionately committed to providing clear and full information to our users about our technology and policies regarding user privacy and data retention. In addition, each quarter we share the number and types of requests for user information we receive from the government and how we handle them. Below you can find more detailed information about the government requests Wickr received and processed between July 1 and September 29, 2015.

Government Requests

Reporting Period	Country	Government Requests	Accounts Associated
For the Quarter Ending September 29, 2015	**United States**		
	Search Warrant[1]	0	0
	Court Orders[2]	0	0
	Subpoenas[3]	2	3
	National Security Requests[4]	0	0
	Non-United States[5]		
	Non-U.S. Requests	0	0

Action to Date

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

---

[1] **Search Warrant:** Search warrants require judicial review, a showing of probable cause, and must meet specificity requirements regarding the place to be searched and the items to be seized. Search warrants may be issued by local, state or federal governments, and may only be used in criminal cases.

[2] **Court orders:** Court orders are issued by judges and may take a variety of forms, such as a 2703(d) order under the Electronic Communications Privacy Act, in both civil and criminal cases. Court orders may include gag orders requiring us to keep private a request for users' account information.

[3] **Subpoenas:** Subpoenas include any legal process from law enforcement where there is no legal requirement that a judge or magistrate review the legal process. Local, state and federal government authorities may use subpoenas in both criminal and civil cases. Subpoenas are typically issued by government attorneys or grand juries. As set forth in our law enforcement guidelines, we will respond to validly-issued subpoenas but will notify our users of the request(s) for information regarding their accounts unless bound by a court order not to do so.

[4] **National Security Requests:** National Security requests include National Security Letters and orders issued under the Foreign Intelligence Surveillance Act.

[5] **Non-US requests:** We require non-US governments to follow the Mutual Legal Assistance Treaty process or letters rogatory process so that a US court will issue the required US legal process.