Wickr Transparency Report

By Jennifer DeTrani, General Counsel
January 4, 2016

Our Philosophy & Impact

At a time of heightened concerns over data security critical to the operation of the global financial system, energy and government sectors, it is critical for businesses and organizations to retain control over high-value digital assets. The trend of empowering users – whether businesses, organizations or individuals – to take control over the security of their data has been further advanced by the European Union's Data Protection Reform set, likely to be passed in 2016, which strengthens the privacy of EU citizens. Although such new standards may represent an extensive set of new responsibilities and potential repercussions across industries, they also offer an opportunity for technology companies to innovate ways to minimize and streamline data accumulation in order to ensure the security of global information systems and citizens.

We at Wickr believe that it is the responsibility of technology leaders to offer the utmost transparency about the safeguards and policies put in place to handle and defend user data. In our commitment to this promise, Wickr's security team has released its first technical paper detailing the technology protocol at the foundation of our products, designed to ensure the integrity of user information. With a privacy-by-design approach at its core, Wickr is built to provide our partners with robust security while retaining minimal information to reduce the risks of exposing data. Our users always maintain ownership over their information, whether at rest or in transit.

As a security company, we know that robust, uncompromised encryption is paramount to defending the critical infrastructure and high-value data transmitted through corporate and government networks. The ongoing judicial process in which a New York federal judge called on Apple to submit its views on the burden associated with unlocking an iPhone per law enforcement request, further stresses the urgency for balance between law enforcement's need for effective investigative tools and the dire state of individual and national cyber security that will be compromised without proper technological, legal and policy safeguards.

At a time of emerging terrorist threats, we strongly support law enforcement's mission to stop extremists through all means available within the bounds of the law. The Wickr team has developed comprehensive Law Enforcement Guidelines to assist federal and local agencies in understanding how our platform works and what information can potentially be provided in the course of a lawful investigation.

Our technology is architected to protect the security of high-value data and communications of anyone, including law enforcement agencies working tirelessly to protect the public. That is why it is our mission at Wickr to continuously perfect our technology and passionately advocate for improving our collective security and encryption standards.

Government Requests

Wickr is committed to sharing 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 how many government requests Wickr received and processed in the last quarter of 2015.

Reporting Period	Country	Government Requests	Accounts Associated
The 4th Quarter Of 2015	**United States**		
	Search Warrant[1]	0	0
	Court Orders[2]	1	1
	Subpoenas[3]	1	1
	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.