Wickr Transparency Report

By Jennifer DeTrani, Wickr General Counsel
June 30, 2015

Our Philosophy & Impact

For the past 3 years, millions of users in more than 190 countries around the world have trusted Wickr to secure their private communications. We take this responsibility seriously. Our unique technology employs perfect forward secrecy as part of our patented end-to-end encryption platform.

We believe privacy and security are critical components of a global solution in a world where new and increasingly intrusive, large-scale sophisticated cyber attacks occur daily. With technology becoming largely ubiquitous and the ways in which we rely on digital infrastructure continuing to expand, Wickr stands firmly for strong encryption standards that anyone – whether an enterprise partner or a consumer – can employ to protect digital assets, intellectual property and communications. In fact, Wickr's communications platform is compliant-by-design with major regulations governing financial, healthcare, education, and national security standards.

As validation for our mission and technology, we are proud to announce that Wickr was awarded stars in every applicable category in the Electronic Frontier Foundation (EFF)'s annual report Who Has Your Back. Wickr is among nine major tech companies that received a perfect score for our privacy practices, earning the EFF's highest recognition: "We commend Wickr for its strong stance regarding user rights, transparency, and privacy."

Further validation came this quarter in the form of the Report of the United Nation's Office of the High Commissioner, which recognized the value of encryption and the necessity for the states, businesses and civil society to bring encryption by design and default to users around the world after a call for submission of papers from entities, organizations and governments. Our submission, on which we partnered with the Human Rights Foundation, can be found here.

In collaboration with the Wickr Foundation, we actively support education initiatives that promote digital security awareness and encryption among groups such as human rights activists, journalists, policy-makers and youth. For two years in a row, Wickr has been an official app for the Oslo Freedom Forum, the so-called "Davos for Dissidents". This year, we helped teach activists working under oppressive regimes valuable skills to help them protect their communications. At Stanford University, the Foundation recently held a crypto workshop for local high school girls striving to become the next generation of security professionals and business leaders. Wickr will continue to advocate for strong privacy and security protections, as these values are central to our mission and to our business principles.

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.

Reporting Period	Country	Government Requests	Accounts Associated
For the Quarter Ending June 30, 2015[1]	Non-United States[2]	0	0
	United States Request Type:	0	0
	Search Warrant[3]	0	0
	Court Orders[4]	2	11
	Subpoenas[5]	3	10
	National Security Requests[6]	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] This report covers the time period between March 26 and June 30, 2015. Hereafter, transparency reports will be published on a quarterly basis.

[2] **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.

[3] **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.

[4] **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.

[5] **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.

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

Wickr Forecast:

Over the next few years, billions of new devices will be connected to the Internet, significantly increasing the amount of personal data transferred through global networks. Securing these emerging applications and the Internet of Things will inevitably become a top concern for consumers as well as a competitive advantage for businesses worldwide. It is our strong view that encryption is a key defense against cyber attacks. Wickr, with its private-by-design communications platform, is ideally positioned to power growth and tech innovation at a global scale while providing safeguards for sensitive information for consumers and enterprises alike.