

BitTorrent unveils NSA-proof online calling and messaging software

August 1 2014, by Jon Healey, Los Angeles Times



BitTorrent Inc., the San Francisco company behind the most popular technology for sharing files online, is branching out into a new arena: snoop-proof calling and texting.

The company announced the availability Wednesday of a preliminary, test version of BitTorrent Bleep software, which will enable people to make calls (voice only) and send messages over the Internet without using a central server to direct traffic. Instead, users will find one another through groups of other users, with no records of the calls or texts stored anywhere along the way.

Once a connection is made for a call or text, the communication travels directly between the two computers involved. That peer-to-peer

approach also defies mass surveillance. Granted, it doesn't pay to underestimate the National Security Agency's ability to monitor even well-hidden communications. But Bleep certainly makes the job harder than the most popular online calling and messaging apps do.

Bleep will be available by invitation only for now, the company said, because it still has plenty of rough edges. It's also limited to computers running Windows 7 or 8, although support for more platforms is coming.

The product reflects BitTorrent's effort to find more applications for the distributed-computing technology that underlies its file-sharing software. It launched BitTorrent Sync last year to provide an alternative to cloud-based programs that synchronize files across multiple devices. Shortly before that it unveiled BitTorrent Bundles, a publishing platform for digital content. The company has been working on Bleep at least since September, when it announced its plan to develop a secure online chat service.

Online calling and messaging services typically seek to preserve privacy by scrambling the communications between the sender and the recipient. The problem is that they rely on central servers to handle the electronic signals that establish the connection. The metadata that passes through those servers can be monitored or intercepted, potentially exposing the calls and texts themselves to surveillance, as leaked NSA data has revealed about Skype and other Voice over Internet Protocol services.

Bleep encrypts its traffic too, as well as enabling users to keep their identities secret even from those with whom they're communicating. But the main reason it's more secure, the company says, is because it has no central servers. "We are not even storing data temporarily on servers and then deleting it," Farid Fadaie, head of the Bleep project, wrote in a blog post Wednesday. "We never have the metadata in the first place."

Nor does anyone else. Unlike BitTorrent's file-sharing technology, there are no central, surveillance-susceptible indices helping to connect one user to another. Instead, when User X tries to start a call or send a text to User Y, X's Bleep software asks other BitTorrent users if they know Y's IP address. Their query eventually reaches a computer that Y's Bleep software has made contact with, revealing Y's address. The information is sent back to X, enabling X and Y to connect directly.

"Consider Bleep your personal redaction pen controlled by you and only you," Jaehee Lee, senior product manager at BitTorrent, wrote in a blog post Wednesday. "Anything you say is Bleep-ed out to us and everyone else for that matter."

This seems technologically nifty, but who would go to the trouble of running Bleep when millions of people around the world can easily be reached through Skype, WhatsApp or any number of other VOIP and chat apps? Lee offered four possible use cases: diplomats sharing sensitive dispatches, businesses safeguarding communications from industrial espionage, reporters protecting sources, or friends keeping their conversations private.

I could suggest any number of less noble uses for the software too. But as with the BitTorrent protocol itself, Bleep shouldn't be judged by the things people do with it. Instead, it should be judged by its ability to deliver on its promise of security.

The [technology](#) isn't interoperable with other chat or VOIP clients, at least not at this point, so its utility will be limited unless and until it gains a critical mass of users. The tremendous popularity of the BitTorrent protocol gives Bleep a strong global foundation, but not much else. That could change, though, if Bleep were built into updated versions of the apps people use to share torrent files.

One other potential factor is whether Congress changes the 1994 Communications Assistance for Law Enforcement Act to require data communications services to support wiretaps, as the Justice Department and federal security agencies have sought. Today, the wiretap requirement applies only to phone networks (including mobile ones) and online services that are effective substitutes for them (such as Vonage). If CALEA were extended to all online voice and messaging services, BitTorrent might be faced with the choice of withdrawing Bleep somehow from the United States or re-engineering it to remove its distinguishing feature.

©2014 Los Angeles Times

Distributed by MCT Information Services

Citation: BitTorrent unveils NSA-proof online calling and messaging software (2014, August 1) retrieved 25 April 2024 from

<https://phys.org/news/2014-08-bittorrent-unveils-nsa-proof-online-messaging.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.