National Security

Neustar, Telcordia battle over FCC contract to play traffic cop for phone calls, texts

By Ellen Nakashima
August 9, 2014

Influential lawmakers are urging the Federal Communications Commission not to ignore national security as it prepares to choose a company to play the critical role of traffic cop for virtually every phone call and text message in North America.

At issue is the security of the most significant cog in the telecommunications network that most Americans have never heard of.

The Number Portability Administration Center, or NPAC, handles the routing of all calls and texts for more than 650 million U.S. and Canadian phone numbers for more than 2,000 carriers. If numbers are scrambled or erased, havoc could ensue. The FBI and other law enforcement agencies query the database every day, or 4 million times a year, in the course of criminal and intelligence investigations to determine which phone company provides the service for a particular number.

A major concern, national security experts say, is that a foreign government intent on learning which of its agents the United States has under surveillance might hack into the database to see what numbers the FBI or another security agency has wiretaps on.

Since 1997, a Sterling, Va., firm, Neustar, has held the exclusive contract to run that system, which was established to let customers change their carrier but keep their number.

Now, however, a rival firm owned by Sweden-based Ericsson AB is poised to win the lucrative contract — which last year brought in $437 million, or nearly half of Neustar's 2013 revenue of $902 million. The firm, Telcordia Technologies, put in a bid substantially lower than Neustar's, and an FCC advisory panel has recommended that the commission pick Telcordia.

In a letter sent Thursday to the FCC chairman, Rep. Mike Rogers (R-Mich.) and Rep. C.A. Dutch Ruppersberger (D-Md.), the chairman and ranking Democrat of the House Intelligence Committee, urged the commission to consult the FBI and other security agencies before picking a firm.

The lawmakers say they are concerned that the selection process "will not adequately address the inherent national security issues involved in this database." Rogers and Ruppersberger, who said they are neutral on which company should win, urged the FCC to include security requirements in the award process.

Rep. Peter T. King (R-NY) sent a similar letter to commission Chairman Tom Wheeler on July 30, raising concerns about "any security vulnerabilities associated with a non-US vendor."

The FCC declined to comment.

Neustar officials noted that Telcordia runs number portability systems in more than 15 countries, including India, Pakistan and Saudi Arabia. They expressed concern that Telcordia will be using computer code from its overseas systems to run the U.S. database. Neustar senior technologist Rodney Joffe said that is a security risk if a hacker from a foreign country detects a flaw in one of the foreign systems that it can exploit to penetrate the U.S. database.

But officials at Telcordia, which grew out of Bell Labs, the research division of American Telephone & Telegraph, said the software code used for the system will be entirely domestic. "We are not using any of the code used and deployed in foreign installations at all, zero," said Chris Drake, chief technology officer at iconectiv, the Telcordia unit that handles number portability systems.

He said the firm began several years ago to work on the project in anticipation of winning the contract. He said it includes "state-of-the-art" cybersecurity protections, which he declined to elaborate on because of what he said were national security concerns.

He said Telcordia is willing to meet any requirements imposed by the FCC or law enforcement agencies.

Wiretap-related data will be held in "a separate infrastructure — a shadow database — that's even more tightly controlled than the NPAC itself," Drake said. He said wiretap data are encrypted and that no records will be kept of the numbers queried by law enforcement. "That's really the most important point: Law enforcement components are dealt with in a special way," he said.

Neustar said a major issue is that the bid specifications, written by an industry consortium, are deficient. They lack general security and national security requirements that Neustar has built into its system over the years based on working with law enforcement and with officials handling national emergencies, such as Hurricane Katrina , Joffe said.

They do not specify, for instance, that sensitive code be written only by U.S. citizens, which is a common requirement for federal contracts that affect national security.

Steven M. Bellovin, a Columbia University computer scientist who used to work at Bell Labs, said Neustar's concerns are valid but there are measures that can be taken to alleviate them. He pointed, as an example, to

the takeover of Sprint Nextel by Japan's SoftBank Corp. The two firms agreed to appoint a new Sprint board member, to be approved by the federal government, to oversee national security compliance.

"The real issue is access to the network," he said. "If they're doing it right, that shouldn't be an issue."

Lisa Hook, Neustar president and chief executive, noted that Neustar, a Lockheed Martin spin-off, has run the system for 17 years without incident. "Even if the FCC is going to award the contract to someone else, it really needs to step back and get a security plan in place," she said. "Understand the supply chain. Make sure all the infrastructure and code is maintained in the United States. All we're saying is, 'There are real national security issues here.' "

The FCC on Friday extended the public comment period on the Telcordia recommendation to Aug. 22.

Ellen Nakashima

Ellen Nakashima is a national security reporter with The Washington Post. She was a member of two Pulitzer Prize-winning teams, in 2018 for coverage of Russia's interference in the 2016 election, and in 2014 and for reporting on the hidden scope of government surveillance. Follow