as would be expected were the cause an orbiting exoplanet. "You can come up with [natural] explanations, but they seem contrived," says Siemion.

One intriguing possibility, much discussed in the media last fall, is that this star is surrounded by artifacts of an alien civilization, perhaps something akin to a "Dyson sphere," the hypothetical construction an advanced civilization might erect in space to harvest light from its parent star (named after the originator of the concept, physicist Freeman Dyson). Initial efforts by researchers at the SETI Institute using the Allen Telescope Array have, however, failed to turn up any evidence of intelligent life around this star.

Hoping to explore that wild idea, Siemion and his colleagues in early 2015 had submitted various proposals for observation time on the Green Bank telescope. Breakthrough Listen will make further radio observations of this star possible even without any other funding. "One way or another," says Siemion, "come March, we'll be observing this star."

—DAVID SCHNEIDER

THE FINAL FRONTIER: As part of the Breakthrough Listen initiative, astronomers will search for optical signals using a 2.4-meter telescope at the Lick Observatory [top], thanks to funding from Russian billionaire Yuri Milner [bottom].

Don't Expect Encrypted E-mail in 2016

Despite big promises, Yahoo and Google probably won't champion end-to-end encryption

LAST MARCH ALEX STAMOS, then Yahoo's head of information security, showed off prototype software for encrypting sensitive e-mail messages. The new tool, which Stamos said could be ready for deployment by the start of 2016, featured "end-to-end" encryption, meaning that even Yahoo itself wouldn't be able to decrypt messages stored on its servers.

Yahoo promised to make such encryption easy to use, building on open-source software for end-to-end e-mail encryption that Google has been developing. (Google's software implements a standard called OpenPGP, based on an encryption system that Phil Zimmerman created in 1991: Pretty Good Privacy, or PGP.)

If Yahoo and Google were to throw their market weight—not to mention their substantial developer resources—behind end-to-end e-mail encryption this year, it would no doubt displease the many government authorities who claim this technology is rendering them unable to eavesdrop on bad guys' electronic communications—or "going dark" as they call it.

James Comey, director of the Federal Bureau of Investigation, summarized those sentiments in July when he told the Senate Judiciary Committee that "we have on a new scale seen mainstream products and services designed in a way that gives users sole control over access to their data." He pointed to the central role of tech companies, saying, "We would like to emphasize that the Going Dark problem is, at base, one of technological choices and capability."

The implication of Comey's statement was clear: If companies were forbidden by law from offering such privacy protections, the products and services Comey alluded to would have to be shut down—at least in the United States. But it's unlikely that the U.S. government will do that anytime soon. Indeed, the Obama administration signaled in October that it would not ask tech companies to build back doors into their encryption products, given the strong possibility that weakening security in this way would enable criminal hackers and malicious foreign agents to compromise even more systems than they are already doing.

Such concerns aren't so strong on the other side of the Atlantic, though. In particular, U.K. prime minister David Cameron indicated

TOP: LAURIE HATCH; BOTTOM: NIKLAS HALLEN/AFP/GETTY IMAGES

MATTER OF FACT

The name for the now 25-year-old encryption system Pretty Good Privacy (PGP) was inspired by Ralph's Pretty Good Grocery of Garrison Keillor's fictional Lake Wobegon.

last July that he wants to outlaw encrypted messaging systems that don't offer government authorities the means to decrypt content. And in November, U.K. home secretary Theresa May introduced a surveillance bill that would, among other things, outlaw end-to-end encryption. The debate is bound to boil over in the next few months as U.K. lawmakers work to replace the country's Data Retention and Investigatory Powers Act 2014, which is set to expire at the end of 2016.

So are Google and Yahoo headed on a collision course with the U.K. government over their end-to-end e-mail encryption? Probably not, according to Matthew Green, a cryptography expert at Johns Hopkins University, in Baltimore. "I don't think they are putting the resources behind it that it needs," says Green. He estimates that Google has one or two developers working on end-to-end e-mail encryption, too few to meet the challenge of creating a system that's truly versatile. Yahoo, too, hasn't dedicated adequate resources to the project to make their efforts successful, argues Green. "I think eventually they'll have egg on their face."

Christopher Soghoian, principal technologist of the American Civil Liberties Union, is similarly skeptical, characterizing these projects at Google and Yahoo as post-Snowden "feel-good" exercises. Soghoian notes that strong e-mail encryption goes against these companies' self-interest: "Google wants to be your brain," doing things like adding flight times to your calendar when you receive an e-mail confirmation after buying a plane ticket. "That kind of personal digital assistant is possible only if they see everything you're doing."

While he, too, recognizes the PR value Google and Yahoo gain from these projects, Joseph Bonneau, a technology fellow at the Electronic Frontier Foundation, in San Francisco, thinks that these tech giants' interest in developing end-to-end e-mail encryption is more genuine. "It's definitely a problem that Google and Yahoo would like to solve," he says. It's just that the challenges that come along with encrypting e-mail are enormous. They include figuring out how to manage people's cryptographic keys in a way that is secure and yet doesn't make users prone to losing access to their e-mail archives, how to filter spam when only the end user can read the messages, and how to enable users to search through their past messages. "The experience of Gmail would be a lot different if you couldn't search," notes Bonneau.

Both Google and Yahoo declined interview requests, so it's hard to gauge whether these companies really are determined to provide their users with encrypted e-mail this year. Even if they end up putting serious muscle behind the effort, it might still stall. It's a better bet that the main battlefield in this year's cryptowars won't be e-mail so much as instant messaging services like iMessage and WhatsApp, where users have fewer expectations for spam filtering and searching. What makes end-to-end encryption in these messaging services so attractive and popular, Bonneau says, is, ironically, that "nobody knows it's there."

—DAVID SCHNEIDER

TRUTH TO POWER: Alex Stamos, then Yahoo's information-security chief, testified before the U.S. Senate's Homeland Security Committee in 2014. Stamos has since left Yahoo for Facebook, where he is the chief security officer.

WIN MCNAMEE/GETTY IMAGES