Justice Department looks to sharpen computer crime law (Update)

September 9 2015, byEric Tucker

Int his June 17. 2009, file photo, former Hollywood private eye Anthony Pellicano is shown in court in Los Angeles. It's clearly illegal to hack into someone else's computer network and steal information from it. But what about a police officer who uses his own department's computer database to look up women from his past? Or employees who use their log-in credentials to download confidential information from their employer? The issue surfaced in

August 2105 when the California-based 9th U.S. Circuit Court of Appeals threw out computer access charges against Anthony Pellicano, a Hollywood private eye who wiretapped phones for celebrity clients to dig up dirt on rivals, and several of his alleged conspirators. The court upheld most of the convictions in the case but found that the jury had been given improper instructions on the law. (AP Photo/Nick Ut, File)

Stung by recent court decisions that have gone against them, Justice Department lawyers are making a fresh push to clarify a computer trespass law that critics malign as overly broad.

The 1986 law, known as the Computer Fraud and Abuse Act, was intended to punish hackers who breach someone else's computer network and steal information from it.

But federal prosecutors have struggled at times in applying it to people who have permission to access a computer—a police department database, for instance, or a corporate network—but abuse that right by using for purposes that have not been authorized.

The concerns attracted attention this year after President Barack Obama suggested changes to the Computer Fraud and Abuse Act as part of a broader proposal. The Justice Department has appealed to Congress, which is expected to take up other cybersecurity measures in coming weeks.

"These are really hard issues of what should the law cover and what should it not cover," said George Washington University law professor Orin Kerr. "It's totally understandable that we're having this discussion and not sure what the answer should be, because this is a new kind of technological problem."

Critics, including judges, have long expressed concern that people could be prosecuted under the anti-fraud law for computer use that while technically unauthorized is nonetheless benign. An appeals court raised the prospect that checking sports scores at work could theoretically lead to prosecution, though the Justice Department says it's never had any interest in going after that kind of behavior.

Justice Department lawyers have sought to allay those fears by proposing to narrow the circumstances for prosecution, such as in instances when someone knowingly exceeds authorized access or when the computer access targets a government database or was part of another felony like blackmailing a colleague.

In this July 1, 2014, file photo, with his mother Elizabeth Valle by his side, GIlberto Valle, left, makes a short statement to the assembled media as he leaves Manhattan federal court in New York. It's clearly illegal to hack into someone else's computer network and steal information from it. But what about a police officer who uses his own department's computer database to look up women

from his past? A federal appeals court in New York is weighing the issue in the case of Gilberto Valle, a former New York City police detective dubbed the "cannibal cop" for his online exchanges about kidnapping and eating women. Though a judge dismissed most of the case, Valle is appealing his conviction for using an NYPD database to look up women he targeted. His supporters say that action could not have been a crime because, as an officer, he was entitled to access the database. (AP Photo/Seth Weng)

"What we need is a law that makes clear that if you exceed authorized access for nefarious purposes ... that that's a violation of the law," said Assistant Attorney General Leslie Caldwell.

Sens. Lindsey Graham, R-S.C., and Sheldon Whitehouse, D-R.I., have drafted legislation similar to the Justice Department proposal that could be introduced soon. Meanwhile, Whitehouse has attached an amendment that would punish by up to 20 years damage to a "critical infrastructure computer" to broader cyber legislation expected to be considered soon by the Senate.

Yet even some critics of the existing law say they believe the government already has enough tools to punish computer crime, without making the proposed changes. "All of this is a solution in search of a problem," said Hanni Fakhoury, a staff attorney at the Electronic Frontier Foundation, a privacy group.

Though the Justice Department has successfully used the existing statute many times, its proposal comes amid recent decisions in appeals courts—including in a lawsuit involving trade secrets—that have interpreted the law in ways prosecutors didn't like.

The issue surfaced last month when the California-based 9th U.S. Circuit Court of Appeals threw out computer access charges in the case

of Anthony Pellicano, a Hollywood private eye who wiretapped phones for celebrity clients to dig up dirt on rivals. The court upheld most of the convictions but said the jury was given improper instructions on the law.

The same court in 2012 rejected computer access charges against a former employee of an executive search firm who had been accused of encouraging some of his ex-colleagues to help him start a competing business by using their log-in credentials to download information from a confidential database on the company's computer.

Basing criminal liability on a computer's computer-use policies can make innocuous acts criminal, wrote Judge Alex Kozinski.

"Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of The New York Times to read at work, but they'd better not visit ESPN.com," he wrote.

A federal appeals court in New York is weighing the issue in the case of Gilberto Valle, a former New York City police detective dubbed the "cannibal cop" for his online exchanges about kidnapping and eating women. Though a judge dismissed most of the case, Valle is appealing his conviction for using an NYPD database to get information on a woman he'd known since high school.

His supporters say that action could not have been a crime because, as an officer, he had legitimate access to the database.

It's not clear what action Congress will take, but it's also not clear that it needs to do anything, said Kerr, the law professor.

"It's a hard set of problems for Congress to try to figure out, because you have courts disagreeing on what the rules should be," Kerr said. "And

one option is to just wait for the Supreme Court to say what the rules actually are."