

IRS facial scanning plan raises privacy fears



By Hiawatha Bray, Globe Staff

Millions of us unlock our smartphones by letting them scan our faces. Soon we'll have to do the same to review our tax records online.

Starting this summer, the Internal Revenue Service will require taxpayers to provide images of their faces to access their data on the agency's website. It's a major advance in government use of biometric security systems, which unlock data based on a person's physical features, like facial appearance or fingerprints. Biometric systems are designed to be more secure than traditional passwords, which are often easy to crack.

But privacy advocates worry that the new IRS system will normalize the use of biometric systems, compelling citizens to provide this sensitive data to a vast array of government agencies and businesses.

India McKinney, director of federal affairs for the Electronic Frontier Foundation, a digital civil liberties group, noted that taxpayers will have no choice about using the system, because the IRS hasn't offered a non-biometric way to log in.

"You cannot opt out of paying taxes," McKinney said. "This is kind of a big deal, and it's bad."

The IRS said that contrary to some earlier press reports, taxpayers will not have to use the system to file their returns. "The IRS emphasizes taxpayers can pay or file their taxes *without* submitting a selfie or other information to a third-party identity verification company," the agency said in an e-mailed statement.

But people will need the new system for other activities, like filing for the federal child tax credit, reviewing tax records from previous years, or setting up payment plans.

The agency will rely on technology from ID.me, a Virginia company that's already used by a number of state unemployment insurance agencies to combat benefit fraud. Using the system requires a smartphone or a computer with a webcam. Users must take a picture of a photo ID, such as a driver's license or passport. Users then take photos of themselves. The ID.me system compares the live image with the photo ID, confirming that it's the same person.

Data security blogger Brian Krebs, who first reported on the new policy last week, said the IRS and other government agencies are desperate to find better ways to secure their systems. He cited the state of California, where criminals using fake IDs have stolen at least \$20 billion in unemployment benefits linked to the COVID pandemic.

Standard security systems try to confirm a person's identity through phone numbers, street addresses, or Social Security numbers. But data thieves have stolen so much of this information from corporate and government databases that it's easy for criminals to come up with the correct answers. "There are a thousand ways to find out," said Krebs.

Last year, for example, security researchers found an automated bot on the messaging service Telegram that could be used by anybody to look up millions of personal phone numbers that had been stolen from Facebook by hackers.

Biometric data is much harder to fake than a phone number. But McKinney said there's no guarantee that facial databases won't eventually be stolen just like other identifiers. She said this would create a far greater danger, because while somebody can get a new phone number or Social Security number, nobody can get a new face.

ID.me said it stores all data in encrypted form inside highly secure data centers. The company also said that it will delete personal data on request, does not sell the data to other companies, and will only share it with the government when required by law or by court order.

*Hiawatha Bray can be reached at [hiawatha.bray@globe.com](mailto:hiawatha.bray@globe.com). Follow him on Twitter @GlobeTechLab.*