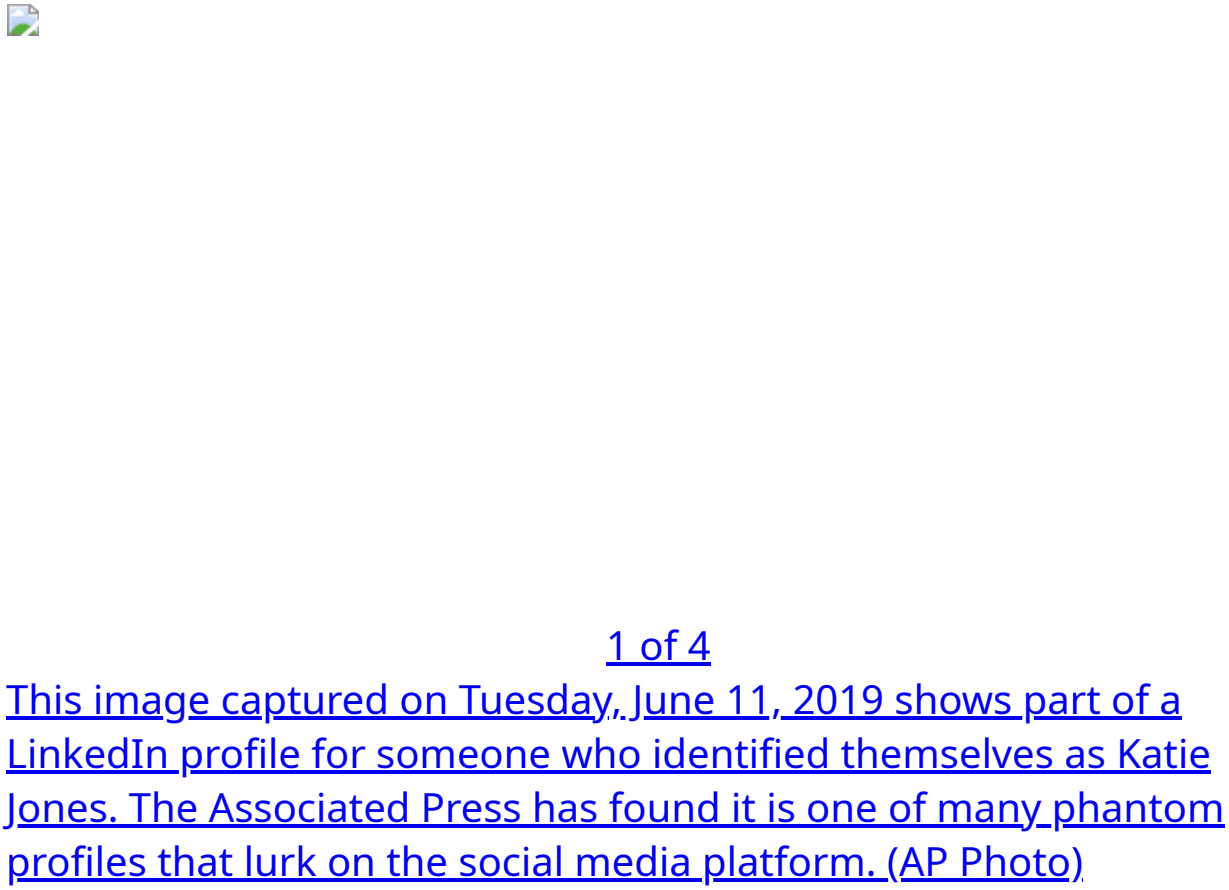
Experts: Spy guys use AI-generated faces to connect with targets on Linkedin, OKCupid, Match.com, Twitter

By RAPHAEL SATTERtoday

1 of 4



This image captured on Tuesday, June 11, 2019 shows part of a LinkedIn profile for someone who identified themselves as Katie Jones. The Associated Press has found it is one of many phantom profiles that lurk on the social media platform. (AP Photo)

LONDON (AP) — Katie Jones sure seemed plugged into Washington's political scene. The 30-something redhead boasted a job at a top think tank and a who's-who network of pundits and experts, from the centrist Brookings Institution to the right-wing

Heritage Foundation. She was connected to a deputy assistant secretary of state, a senior aide to a senator and the economist Paul Winfree, who is being considered for a seat on the Federal Reserve.

But Katie Jones doesn't exist, The Associated Press has determined. Instead, the persona was part of a vast army of phantom profiles lurking on the professional networking site LinkedIn.

Experts who reviewed the Jones profile's LinkedIn activity say it's typical of espionage efforts on the professional networking site, whose role as a global Rolodex has made it a powerful magnet for spies.

"It smells a lot like some sort of state-run operation," said Jonas Parello-Plesner, who serves as program director at the Denmark-based think tank Alliance of Democracies Foundation and was the target several years ago of an espionage operation that began over LinkedIn .

William Evanina, director of the U.S. National Counterintelligence and Security Center, said foreign spies routinely use fake social media profiles to home in on American targets — and accused China in particular of waging "mass scale" spying on LinkedIn.

"Instead of dispatching spies to some parking garage in the U.S to recruit a target, it's more efficient to sit behind a computer in Shanghai and send out friend requests to 30,000 targets," he said in a written statement.

Last month, retired CIA officer Kevin Mallory was sentenced to 20 years in prison for passing details of top secret operations to

Beijing, a relationship that began when a Chinese agent posing as a recruiter contacted him on LinkedIn.

Unlike Facebook's friends-and-family focus, LinkedIn is oriented toward job seekers and headhunters, people who routinely fire out resumes, build vast webs of contacts and pitch projects to strangers. That connect-them-all approach helps fill the millions of job openings advertised on the site, but it also provides a rich hunting ground for spies. And that has Western intelligence agencies worried.

British , French and German officials have all issued warnings over the past few years detailing how thousands of people had been contacted by foreign spies over LinkedIn.

In a statement, LinkedIn said it routinely took action against fake accounts, yanking thousands of them in the first three months of 2019. It also said "we recommend you connect with people you know and trust, not just anyone."

The Katie Jones profile was modest in scale, with 52 connections. But those connections had enough influence that they imbued the profile with credibility to some who accepted Jones' invites. The AP spoke to about 40 other people who connected with Jones between early March and early April of this year, many of whom said they routinely accept invitations from people they don't recognize.

"I'm probably the worst LinkedIn user in the history of LinkedIn," said Winfree, the former deputy director of President Donald Trump's domestic policy council, who confirmed connection with Jones on March 28.

Winfree, whose name came up last month in relation to one of the vacancies on the Federal Reserve Board of Governors, said he rarely logs on to LinkedIn and tends to just approve all the piled-up invites when he does.

“I literally accept every friend request that I get,” he said.

Lionel Fatton, who teaches East Asian affairs at Webster University in Geneva, said the fact that he didn’t know Jones did prompt a brief pause when he connected with her back in March.

“I remember hesitating,” he said. “And then I thought, ‘What’s the harm?’”

Parello-Plesner noted that the potential harm can be subtle: Connecting to a profile like Jones’ invites whoever is behind it to strike up a one-on-one conversation, and other users on the site can view the connection as a kind of endorsement.

“You lower your guard and you get others to lower their guard,” he said.

The Jones profile was first flagged by Keir Giles, a Russia specialist with London’s Chatham House think tank. Giles was recently caught up in an entirely separate espionage operation targeting critics of the Russian antivirus firm Kaspersky Lab. So when he received an invitation from Katie Jones on LinkedIn he was suspicious.

She claimed to have been working for years as a “Russia and Eurasia fellow” at the Center for Strategic and International

Studies in Washington, but Giles said that, if that were true, “I ought to have heard of her.”

CSIS spokesman Andrew Schwartz told the AP that “no one named Katie Jones works for us.”

Jones also claimed to have earned degrees in Russian studies from the University of Michigan, but the school said it was “unable to find anyone by this name earning these degrees from the university.”

The Jones account vanished from LinkedIn shortly after the AP contacted the network seeking comment. Messages sent to Jones herself, via LinkedIn and an associated AOL email account, went unreturned.

Several experts contacted by the AP said Jones’ profile picture appeared to have been created by a computer program.

“I’m convinced that it’s a fake face,” said Mario Klingemann, a German artist who has been experimenting for years with artificially generated portraits and says he has reviewed tens of thousands of such images. “It has all the hallmarks.”

Klingemann and other experts said the photo — a closely cropped portrait of a woman with blue-green eyes, copper-colored hair and an enigmatic smile — appeared to have been created using a family of dueling computer programs called generative adversarial networks, or GANs, that can create realistic-looking faces of entirely imaginary people. GANs, sometimes described as a form of artificial intelligence, have been the cause of increasing concern for policymakers already struggling to get a handle on digital disinformation. On

Thursday, U.S. lawmakers are due to hold their first hearing devoted primarily to the threat of artificially generated imagery .

Hao Li, who directs the Vision of Graphics Lab at the University of Southern California's Institute for Creative Technologies, reeled off a list of digital tells that he believes show the Jones photo was created by a computer program, including inconsistencies around Jones' eyes, the ethereal glow around her hair and smudge marks on her left cheek.

"This is a typical GAN," he said. "I'll bet money on it."

—

Online:

Test your ability to tell a real face from a fake one at: http://www.whichfaceisreal.com/

Generate your own deepfake faces at: https://thispersondoesnotexist.com

——

Raphael Satter can be reached at: https://raphaelsatter.com