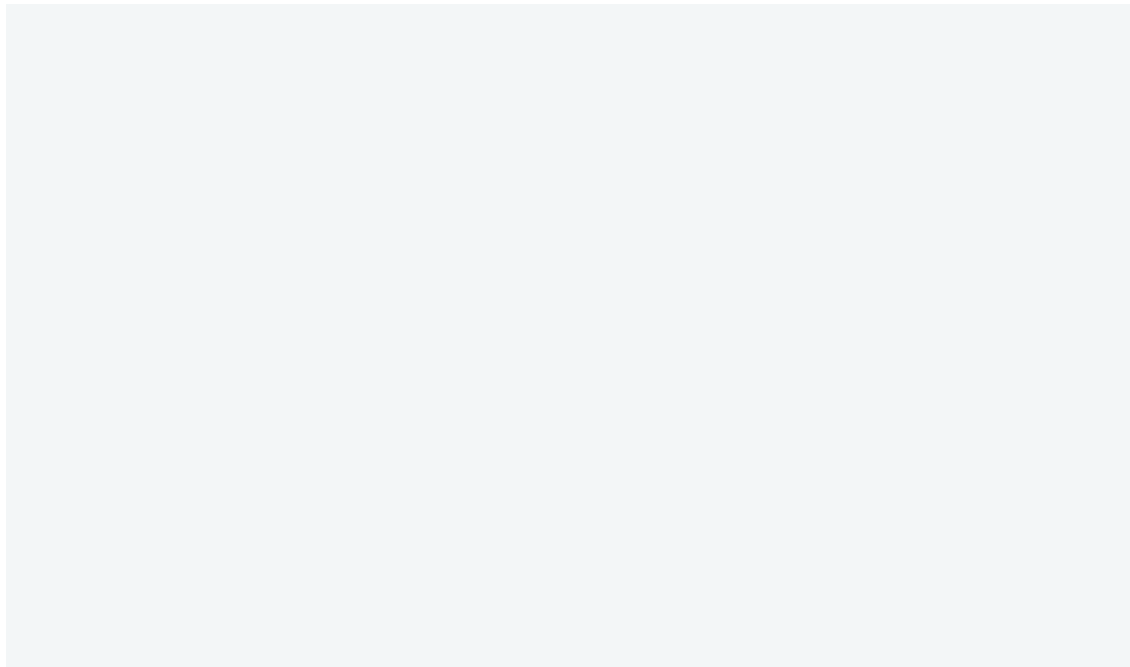# NOTHING YOU OWN IS SAFE FROM THE REVENGE HACKERS!!

DARK WEB Brit teen hacker posed as CIA boss to access secret military files – and sent lewd rape threats to Homeland Security chief

Kane Gamble, 18, hacked into John Brennan's emails, rang his home and took control of his wife's iPad, a court heard

By Tom Michael

A BRIT teen hacker posed as a CIA boss to access secret military files – and sent lewd rape threats to a Homeland Security chief, a court has heard.

Kane Gamble, 18, hacked into intelligence head John Brennan's email account, made hoax calls to his family home and even took control of his wife's iPad, judges were told.

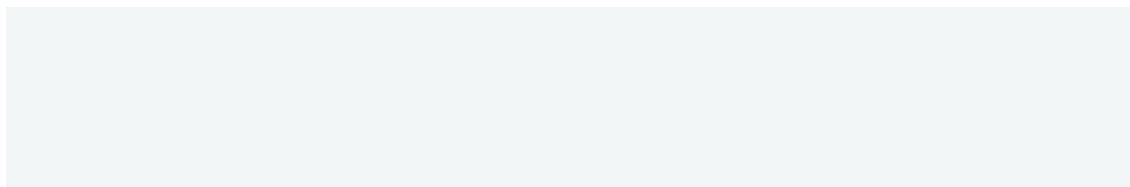Kane Gamble, 18, has pleaded guilty to a string of charges

3

Kane Gamble, 18, has pleaded guilty to a string of charges

The hacks were carried out as part of a campaign of harassment against top US officials motivated by his political views, a court heard.

Gamble was just 15 when he posed as a telecoms worker and Brennan himself to gain information including passwords, contacts lists and sensitive documents about operations in Afghanistan and Iraq.

He then taunted the CIA on Twitter about his successes as a leading member of a collective called "Crackas With Attitude", which supported the Free Palestine movement.

Prosecutor John Lloyd-Jones QC told the Old Bailey Gamble started the group.

Gamble arrives at the Old Bailey in London, where he will be sentenced

PA:PRESS ASSOCIATION

🗢 3

Gamble arrives at the Old Bailey in London, where he will be sentenced

Gamble told a journalist: "It all started by me getting more and more annoyed at how corrupt and cold-blooded the US Government is so I decided to do something about it."

The court heard Gamble "felt particularly strongly" about US-backed Israeli violence against Palestinians, the shooting of black people by US police, racist violence by the KKK and the bombing of civilians in Iraq and Syria.

After Brennan, Gamble went on to carry out a series of similar attacks on other top security figures from his bedroom in Leics.

His victims included the secretary of Homeland Security Jeh Johnson, to whom he sent a photo of his daughter and said he would "f*** her", the court heard.

Gamble was 17 when he was arrested at his council home near Leicester

BPM MEDIA

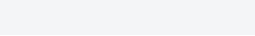Gamble was 17 when he was arrested at his council home near Leicester

He also targeted the ex-deputy director of the FBI Mark Giuliano and James Clapper, director of national intelligence under Obama, as well as their families.

He boasted about carrying out "the best breach ever" after accessing an FBI database to get the names of 1,000 staff and details of the officer responsible for the notorious shooting of Michael Brown in Ferguson, Missouri.

The information Gamble gathered was later used to carry out a "swatting" attack on John Holdren, a science and technology adviser to US President Barack Obama, resulting in armed officers being sent to Mr Holdren's family home.

A similar prank carried out by another hoaxer in the US resulted in the victim being shot dead by gun cops who raided his house.

Gamble was arrested in February 2016 at his council home in Coalville, near Leicester, at the request of the FBI after he hacked into the Department of Justice network.

The teen, who claims he did not realise the seriousness of what he was doing because of his autism, will be sentenced at a later date.

Gamble was allowed to sit next to his mother behind his barrister rather than the dock when he appeared at the Old Bailey.

The teen, of Coalville, Leicester, admitted eight counts of performing a function with intent to secure unauthorised access and two counts of unauthorised modification of computer material.
The hearing continues.

Can you hear me now?: NSA can find & track people with 'voice-matching technology'

Can you hear me now?: NSA can find & track people with 'voice-matching technology'

© Alex Milan Tracy / Global Look Press

Declassified documents reveal the National Security Agency has been using secret "speaker recognition" technology to identify people by their unique "voiceprint" for more than a decade.

The NSA has been recording and gathering private phone calls for years, but it used to be difficult for the agency to identify unknown speakers. In the past, signals intelligence (SIGINT) transcribers worked on the same targets for years before they became familiar enough with a speaker's unique voice to be able to verify their identity.

Read more

[A police vehicle blocks an entrance into the NSA facility in Fort Meade, Maryland, US, March 30, 2015. © Gary Cameron NSA sought to prevent Snowden-style leaks, ended up losing staff – whistleblower to RT](#)

Now, the NSA is using more advanced computational systems developed by the Massachusetts Institute of Technology (MIT) in order to catch spies and terrorists, according to a declassified NSA document obtained by media outlet the Intercept.

The document describes how the NSA used the technology during Operation Iraqi Freedom to match an audio recording to former leader Saddam Hussein's *"voiceprint."* The NSA also used

the technology to compare the voice of a captured suspect with previous audio recordings from terrorist Abu Hakim to confirm that the suspect was not a match.

In order to test their technology, analysts at the NSA compared old intercepts and audio files relating to Ron Pelton, a former NSA analyst who sold details about several secret US programs to the Soviet Union. At the time, the agency failed to identify Pelton through human voice identification. However, in 2006, the agency was able to automatically match Pelton's voice using the technology.

"Had such technologies been available twenty years ago, early detection and apprehension could have been possible, reducing the considerable damage Pelton did to national security," the document states.

> Remember that scene in The Dark Knight where Batman makes a hyberbolic crazy surveillance system that uses all phones to find the Joker based on his voice? That could actually happen 5/10 pic.twitter.com/JSQMmzEQO6
>
> — 🤔Jake Laperruque😒 (@JakeLaperruque) January 19, 2018

According to the classified document, the NSA was able to automatically identify a Chinese speaker when they were speaking in English. The document states that voice recognition technologies were *"rapidly becoming the standard in the Intelligence Community"* more than a decade ago.

Civil liberties advocates are concerned that the technology could make it easier for the NSA to violate the privacy rights of American citizens.

"This creates a new intelligence capability and a new capability for abuse," Timothy Edgar, a former White House adviser to the Director of National Intelligence, told the Intercept. *"Our voice is traveling across all sorts of communication channels where we're not there. In an age of mass surveillance, this kind of capability has profound implications for all of our privacy."*

> Here's the (new) report describing how NSA is laying the groundwork to track people down through the microphones around us every day (your phone calls, a friend's laptop, the phone next to you on the train, that Amazon Echo on the shelf…): https://t.co/EPuPhzG2UWhttps://t.co/KjMkZPa21u
>
> — Edward Snowden (@Snowden) January 19, 2018

Since a "voiceprint" is nearly impossible to change or disguise, privacy advocates also fear the NSA would be able to instantly locate and track anyone who can be heard by a microphone.

"There are microphones all around us all the time. We all carry around a microphone 24 hours a day, in the form of our cellphones," Trevor Timm, executive director of the Freedom of the Press Foundation, told the Intercept. *"And we know that there are ways for the government to hack into phones and computers to turn those devices on."*

Former NSA intelligence analyst, Edward Snowden added that the technology could even be used to track people down through other kinds of listening devices, including *"a friend's laptop, the phone next to you on the train, that Amazon Echo on the shelf..."*

> House voted 256-164 in favor of renewing #FISA for six years. It will now go before the US Senate https://t.co/OOImMsjSNDpic.twitter.com/CHo1Wn6Fgj
>
> — RT America (@RT_America) January 11, 2018

Although the NSA has kept their voice-matching technology a secret, the Associated Press reported that Turkcell, the largest mobile phone company in Turkey, used a popular speech recognition technology to collect voice data from approximately 10 million customers in 2014.

In October, Human Rights Watch reported that the Chinese government has been gathering tens of thousands of "*voice pattern*" samples to establish a national voice biometric database and a program that can automatically identify voices in phone conversations.

Interpol also recently announced the Speaker Identification Integrated Project (SIIP), a speaker identification technology funded by the European Union, had passed its final field test.

The program, which began in 2014, was finally able to identify unknown speakers talking in different languages in November of last year.

The Senate recently voted to reauthorize Section 702 of the Foreign Intelligence Surveillance Act (FISA), permitting electronic surveillance of non-Americans. However, it has been shown that the NSA has also collected data on Americans during their surveillance.