Apple’s iPhone and iPad run undisclosed services that allow security features to be bypassed, according to a prominent computer security researcher.

In a presentation at the HOPE/X hacking conference in New York on Friday, forensic researcher Jonathan Zdziarski described several undocumented iOS services that can function backdoors, allowing ostensibly encrypted data to be accessed and subverting user privacy.

Zdziarski in a blog post stresses that he is not accusing Apple of working with the NSA, but he voices suspicion that the NSA might have used some of these services to access data on iOS devices, as described in a recent Der Spiegel report.

I am not suggesting some grand conspiracy, Zdziarski explains.

“There are, however, some services running in iOS that shouldn’t be there, that were intentionally added by Apple as part of the firmware, and that bypass backup encryption while copying more of your personal data than ever should come off the phone for the average consumer.

Zdziaski says he hopes Apple will correct the issue because these services should not be present. He claims to have emailed both CEO Tim Cook and former CEO Steve Jobs about these “backdoors,” some of which have existed for years, and to have received no response.

In a paper describing his findings, the services com.apple.pcapd and com.apple.mobile.file\_relay are among the most questionable code routines that Zdziarski discusses.

The former launches a silent packet sniffer that allows the client to copy the network traffic and HTTP header data coming in and out of the device.

The latter accepts a list of requested data sources, and delivers an archive of the data requested, bypassing Apple’s built-in backup encryption system in the process.

These services and related ones, which have been augmented over the years by Apple, appear to represent an effort to provide law enforcement agencies with easier access to device data.

Yet it’s accepted wisdom among computer security experts that backdoors are a bad idea because they’re potentially exploitable by anyone –investigators, intelligence, or cyber criminals/

When parties communicate using services with [lawful intercept] features.

There is an increased likelihood that an unauthorized and/or malicious adversary with the right technical knowledge and access to the system could capture communications contents without detection, a Center for Democracy and Technology report noted last year.

Zdziarski questions why Apple allows a packet sniffer to run on some 600 million iOS devices, why there are undocumented services that bypass user backup encryption, and why most iOS user data is still not encrypted to protect it from Apple.

Apple did not respond to a request for comment.