By Chris Williams, TheRegister.co.uk

Everyone is having fun this week speculating on all aspects of the alleged Russian spy ring busted in the US on Monday. How were they initially detected? Are they just a decoy to hide the real spies? Why did the US go public now? Has anyone got any more pictures of Anna Chapman for the front pages?

From what little we do know though - ie the content of the FBI's criminal complaints - it's apparent the group's technology tradecraft was not as sharp as you might expect from deep cover spies.

//

Here we present their two most glaring infosec failings:

- ## Return of the MAC

Anna Chapman and her UN-based Russian government handler allegedly held ten meetings around Manhattan between January and June. They would not make overt contact but would exchange data over an ad hoc Wi-Fi network.

FACEPALM
Because expressing how dumb that was in words just doesn't work.

Chapman and the offical made things easy for their watchers, however, by using the same laptops with the same MAC addresses every time. It meant the FBI could tell whenever the pair were in contact simply by following them and using an off-the shelf Wi-Fi network analyser package to match the two MAC addresses.

The pair could have simply used multiple machines, or used any one of an array of utilities that would have allowed them to spoof their MAC addresses. Instead, the FBI's complaint that Chapman was an undeclared agent of a foreign government draws heavily on correlating the two numbers broadcast between her laptop and her handler's.

Chapman knew enough about countering surveillance to buy a "burner" mobile phone and international calling card under a fake name to contact Moscow, apparently after she suspected her new handler (in fact an undercover FBI agent) was not all he seemed last weekend. But that was after she had given him her laptop for repairs.

There are plenty of other options of course for more secure coffee shop wireless data exchanges; post your idea in comments.

- **Password pants down**

In 2005, the FBI obtained a warrant for a covert search of Richard and Cynthia Murphy's home in Montclair, New Jersey.

Agents made forensic copies of "a set of computer disks" and took photographs of documents. The disks are described in court documents as "password protected" - it's unclear whether the password was required to decrypt the disks, or simply to use the steganography

DOUBLE FACEPALM
FOR WHEN ONE FACEPALM DOESN'T CUT IT

[illegible]