A Dangerous Spy in Your Pocket

On 21 September 2018, RT's Israel correspondent Paula Slier reported that Israel's cell phone spy program is known to have been found in 45 countries so far. The program (virus) in question is called Pegasus and was developed by a Tel Aviv company named "NSO Group." This program exploits cell phone's camera, microphone, text and all other functions for spying purposes. This program turns a targeted telephone device into an instrument of absolute espionage.

Originally touted as a crime fighting feature, this program now attacks every smart phone indiscriminately. It all starts with a simple click on a received message and the program embeds itself secretly in the phone. From then on, all your data, passwords, contacts and the future use of the phone are spirited away to the Pegasus operators. Pegasus thus has a global reach and catching criminals is merely incidental to the process.

One of the reported targets of this system was Amnesty International, but the system is sold to foreign governments to target crime and political opponents, of course, while Pegasus oversees all these uses and processes. Mexico and United Arab Emirates are known to have signed contracts with the NSO Group. The Qatari royal family was also targeted and so were journalists and human rights activists. While all this falls into the category of despicable and dirty business, when it comes to targeting United States citizens, it becomes crime under American law. The NSO Group proclaims that the software is not designed to work in the U.S. but it does and it works on mobile devices traveling the world. The company's ad boasts:

> "You can remotely and covertly collect information
> about your target's relationships, location, phone calls,
> plans and activities – whenever and wherever they are."

The company did not take up the offer for an interview.

It is more than a paradox that the witch hunt for the alleged Russian interference in the American election has not uncovered anything ,but Pegasus carries on harvesting data and information in America without even an eyebrow being raised. One can only speculate whom they are targeting in the U.S. and who is benefiting from this information.