2013 MOBILE SURVEILLANCE TRENDS

TREND #1: Ever-expanding abuse of lawful intercept tools

1/18: Researchers disclose Dark Caracal, a global spyware campaign with links to the Lebanese intelligence agency GDGS

TREND #2: Rise of state-sponsored mobile surveillance campaigns

2/26: Cybersecurity firm DarkMatter launches its Katim smartphone, which includes a button for disconnecting power from the camera and microphone

TREND #3: Scrutiny grows on the acceptance of commercial mobile spyware

5/15: Researchers divulge two pieces of mobile malware – Stealth Mango and Tangelo – believed to be used by the Pakistani military

TREND #4: Introduction of new products featuring anti-surveillance capabilities

5/22: A Pentagon memo sets new restrictions for mobile devices within secure spaces where classified information is handled

TREND #5: Government agencies impose rigid mobile device policies

7/31: Amnesty International reveals that one of its researchers has been targeted with Pegasus, a popular iOS spyware tool

8/3: A Department of Defense memo establishes a policy banning personnel from using geolocation features on any device

8/31: The New York Times reports that a vendor of commercial spyware performed illegal surveillance as part of a technology demonstration

9/4: Parim announces the launch date for its Librem 5 smartphone, which features a hardware kill switch for shutting off the camera and microphone

9/7: Researchers unveil Domestic Kitten, a mobile spyware operation thought to be affiliated with the Iranian government

9/10: CNN reports that the White House has changed policy to prevent smartphones from being stored directly in the Situation Room

9/18: The Citizen Lab documents the results of its analysis showing that Pegasus may have operators in as many as 45 countries

10/3: Privoro releases the SafeCase, a first-of-its-kind iPhone case that blocks the phone’s cameras and continuously masks surrounding audio

10/20: An investigation by Haaretz shows how Israel’s cyber-spy industry has sold mobile espionage products to repeated policy violators

11/6: Edward Snowden claims that Pegasus was used to help track Jamal Khashoggi, a dissident Saudi journalist residing in the US

12/7: A column by David Ignatius in The Washington Post pieces together how Saudi Arabia has used commercial surveillance tools to fight a deadly cyberwar