http://wikileaks.org/The-Spyfiles

The Spy Files

12/1/2011

Mass interception of entire populations is not only a reality, it is a secret new industry spanning 25 countries

It sounds like something out of Hollywood, but as of today, mass interception systems, built by Western intelligence contractors, including for 'political opponents' are a reality. Today WikiLeaks began releasing a database of hundreds of documents from as many as 160 intelligence contractors in the mass surveillance industry. Working with Bugged Planet and Privacy International, as well as media organizations form six countries – ARD in Germany, The Bureau of Investigative Journalism in the UK, The Hindu in India, L'Espresso in Italy, OWNI in France and the Washington Post in the U.S. Wikileaks is shining a light on this secret industry that has boomed since September 11, 2001 and is worth billions of dollars per year. WikiLeaks has released 287 documents today, but the Spy Files project is ongoing and further information will be released this week and into next year.

International surveillance companies are based in the more technologically sophisticated countries, and they sell their technology on to every country of the world. This industry is, in practice, unregulated. Intelligence agencies, military forces and police authorities are able to silently, and on mass, and secretly intercept calls and take over computers without the help or knowledge of the telecommunication providers. Users' physical location can be tracked if they are carrying a mobile phone, even if it is only on stand by.

But the WikiLeaks Spy Files are more than just about 'good Western countries' exporting to 'bad developing world countries'. Western companies are also selling a vast range of mass surveillance equipment to Western intelligence agencies. In traditional spy stories, intelligence agencies like MI5 bug the phone of one or two people of interest. In the last ten years systems for indiscriminate, mass surveillance have become the norm. Intelligence companies such as VASTech secretly sell equipment to permanently record the phone calls of entire nations. Others record the location of every mobile phone in a city, down to 50 meters. Systems to infect every Facebook user, or smart-phone owner of an entire population group are on the intelligence market.

Selling Surveillance to Dictators

When citizens overthrew the dictatorships in Egypt and Libya this year, they uncovered listening rooms where devices from Gamma corporation of the UK, Amesys of France, VASTech of South Africa and ZTE Corp of China monitored their every move online and on the phone.

Surveillance companies like SS8 in the U.S., Hacking Team in Italy and Vupen in France manufacture viruses (Trojans) that hijack individual computers and phones (including iPhones, Blackberries and Androids), take over the device, record its every use, movement, and even the sights and sounds of the room it is in. Other companies like Phoenexia in the Czech Republic collaborate with the military to create speech analysis tools. They identify individuals by gender, age and stress levels and track them based on 'voiceprints'. Blue Coat in the U.S. and Ipoque in Germany sell tools to governments in countries like China and Iran to prevent dissidents from organizing online.

Trovicor, previously a subsidiary of Nokia Siemens Networks, supplied the Bahraini government with interception technologies that tracked human rights activist Abdul Ghani Al Khanjar. He was shown details of personal mobile phone conversations from before he was interrogated and beaten in the winter of 2010-2011.

How Mass Surveillance Contractors Share Your Data with the State

In January 2011, the National Security Agency broke ground on a $1.5 billion facility in the Utah desert that is designed to store terabytes of domestic and foreign intelligence data forever and process it for years to come.

Telecommunication companies are forthcoming when it comes to disclosing client information to the authorities - no matter the country. Headlines during August's unrest in the UK exposed how Research in Motion (RIM), makers of the Blackberry, offered to help the government identify their clients. RIM has been in similar negotiations to share BlackBerry Messenger data with the governments of India, Lebanon, Saudi Arabia, and the United Arab Emirates.

Weaponizing Data Kills Innocent People

There are commercial firms that now sell special software that analyze this data and turn it into powerful tools that can be used by military and intelligence agencies.

For example, in military bases across the U.S., Air Force pilots use a video link and joystick to fly Predator drones to conduct surveillance over the Middle East and Central Asia. This data is available to Central Intelligence Agency officials who use it to fire Hellfire missiles on targets.

The CIA officials have bought software that allows them to match phone signals and voice prints instantly and pinpoint the specific identity and location of individuals. Intelligence Integration Systems, Inc., based in Massachusetts - sells a “location-based analytics” software called Geospatial Toolkit for this purpose. Another Massachusetts company named Netezza, which bought a copy of the software, allegedly reverse engineered the code and sold a hacked version to the Central Intelligence Agency for use in remotely piloted drone aircraft.

IISI, which says that the software could be wrong by a distance of up to 40 feet, sued Netezza to prevent the use of this software. Company founder Rich Zimmerman stated in court that his “reaction was one of stun, amazement that they (CIA) want to kill people with my software that doesn’t work."

Orwell’s World

Across the world, mass surveillance contractors are helping intelligence agencies spy on individuals and ‘communities of interest’ on an industrial scale.

The Wikileaks Spy Files reveal the details of which companies are making billions selling sophisticated tracking tools to government buyers, flouting export rules, and turning a blind eye to dictatorial regimes that abuse human rights.