

# **Track 17: The New Attacker Model**



#### Dr. Ghassan Karame

NEC Laboratories Europe Heidelberg, Germany

ghassan@karame.org www.ghassankarame.com

### The Surge of a New Attacker Model



"We know you're upset, we hear you. Believe me, we're listening. We read you. You're coming in loud and clear."

**Image Source: TheLaw.tv** 



**Image Source: pcworld.com** 

### The Surge of a New Attacker Model

#### Global surveillance [edit]

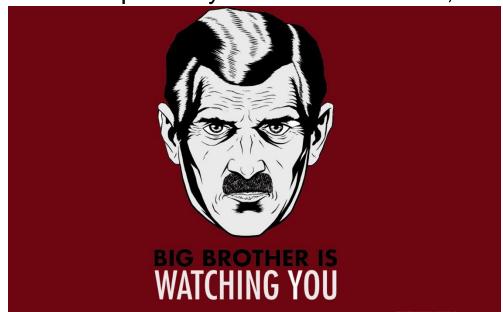
Main article: Global surveillance

Global surveillance programs		
Program	International contributors and/or partners	Commercial partners
PRISM	Australian Signals Directorate (ASD/DSD) of Australia <sup>[49]</sup> Government Communications Headquarters (GCHQ) of the UK <sup>[50]</sup> Algemene Inlichtingen en Veiligheidsdienst (AIVD) of the Netherlands <sup>[51]</sup>	Microsoft[33][52][53]
X <mark>Keys</mark> core	Bundesnachrichtendienst (BND) of Germany <sup>[6][54]</sup> Bundesamt für Verfassungsschutz (BfV) of Germany <sup>[6][54]</sup> National Defence Radio Establishment (FRA) of Sweden <sup>[55][56]</sup>	
Tempora	National Security Agency (NSA) <sup>[57][58]</sup>	British Telecommunications (codenamed "Remedy") <sup>[59]</sup> Interoute (codenamed "Streetcar") <sup>[59]</sup> Level 3 (codenamed "Little") <sup>[59]</sup> Global Crossing (codenamed "Pinnage") <sup>[59]</sup> Verizon Business (codenamed "Dacron") <sup>[59]</sup> Viatel (codenamed "Vitreous") <sup>[59]</sup> Vodafone Cable (codenamed "Gerontic") <sup>[59]</sup>
Muscular	• NSA <sup>[60]</sup>	
Project 6	Central Intelligence Agency (CIA) <sup>[61]</sup>	
Stateroom	□SD <sup>[62][63]</sup> □ Communications Security Establishment Canada (CSEC) <sup>[63][64]</sup> □ GCHQ <sup>[63][65]</sup> □ Special Collection Service (SCS) <sup>[63][65][66]</sup>	Source: wikipedia
Lustre	NSA <sup>[67][68]</sup> Direction Générale de la Sécurité Extérieure (DGSE) of France <sup>[67][68]</sup>	

Last updated: December 2013

### The New Attacker

- The new attacker controls the entire network
  - Mining data from social networks and Internet Service Providers (ISPs)
  - Performing illegal digital taps on private communication channels between individuals.
- The new attacker controls the secret keys
  - Secret keys were acquired by means of coercion, backdoors, etc.



### This panel

This panel will explore possible avenues to enhance user privacy in the presence of a powerful attacker model.









## Empowered by Innovation

