(Straw) Man in the Middle:

A Modest Post-Snowden Proposal
Brussels, Belgium

Jacob Appelbaum

[redacted]

10 December 2015

Post-Snowden?

What does that mean?

Understanding the plumbing

Mass surveillance works by first illegally and generally seizing data, and then indiscriminately searching all data, until a specific search term is found. This is selector based surveillance, a kind of surveillance that requires mass surveillance. It comes from vulnerabilities in core internet and other network protocols.

A shift?

We have experienced a huge shift.

Key changes

Specific understanding about a handful of protocols.

Key changes

A general and pervasive fear; a feeling of helplessness.

Key changes

People have lost faith in the authorities and adopted a fatalistic attitude.

A new assumption

A pervasive fear of mass surveillance, jokes about being on lists; a new default of total monitoring!

A new default to fight passive attackers

Changes are now detectable.

A new default to fight passive attackers

Changes are now detectable.
Encryption is here to stay. Passive interception moves to active.

A new default to fight passive attackers

Changes are now detectable.
Encryption is here to stay. Passive interception moves to active.
Signal/ZRTP clients and Let's Encrypt CA change the game.

A new default to fight passive attackers

Changes are now detectable.
Encryption is here to stay. Passive interception moves to active.
Signal/ZRTP clients and Let's Encrypt CA change the game.
This impacts Law Enforcement and Intelligence; focusing on LE.

Cultural differences

In the US, the UK and in other countries in Europe - searches and notification are different. Cryptography brings us to a new convergence for all cultures at once.

A recent European Court of Human Rights ruling

Oversight isn't enough: accountability is required

Checking validity

Example interactions with the police:

- Siren on an otherwise unmarked car pulling over a driver
  - Drive to a well lit area, dial 112/911, confirm identity of "officer"
- No know raid by armed people
  - Did they declare they are police? How do we verify it?
- Knock at the door with a search warrant
  - Is it a valid warrant?
- Other examples such as a famous Tupac shooting involving police in plain clothing

Reality check

In most of these situations - we acknowledge the serious issue of police impersonation.

How do we detect crimes?

Cyber cyber cyber

How do we detect crimes?

Cyber cyber cyber
(Hint: You will receive nearly no help from any authority!)

An example standard of evidence

In the German Chancellor Merkel case there was a supposed lack of evidence.

An example standard of evidence

In the German Chancellor Merkel case there was a supposed lack of evidence.

Thus we see - we need a new standard of evidence!

A short summary

- First, we acknowledge a change in thinking because of Snowden.
- Secondly, we see a move towards more and more transparency.
- Thirdly, we control those we can control and not those that we don't...

Wait, control?

I have no democratic control over the majority of services. I do have democratic control over a small set of services: local LE, national LE

Wait, transparency?

The new protocols force transparency, the proposed standard of evidence give us data for action; but how might we choose what to act on?

Ask the honest parties to prove their honesty

They sign their interception request in real time, point it to a given court (docket, judge, case, etc.) just as with the search of the home.

And anyone who doesn't sign...

Is subject to investigation with the collected evidence.

Wait, what?

There is no requirement that cryptophone or signal help with this proposal - only that a system of real time notification is implemented by states and their relevant agencies.

Wait, what about TARGETED surveillance

Like cryptography that horse has left the barn with the move from passive to active.

Wait, what about malware

The same standard of evidence and notification should apply.

Help the (honest) police

No ”Golden Key” required

Help the (honest) police

No ”Golden Key” required

A trade of the secrecy property that keeps security for the majority of users

Help the (honest) police

No ”Golden Key” required

A trade of the secrecy property that keeps security for the majority of users

Law enforcement is always asking for a way to do this; my proposal allows an avenue while also asking them to give up secrecy and commit to accountability and transparency.

An equal standard

From homes to phones - interference is not secret, lawful processes exist, crimes committed by thousands of unlawful attackers now subject to reporting.

Questions?