Protecting yourself From the

NSA / GCSB / GCHQ

Government

Contents

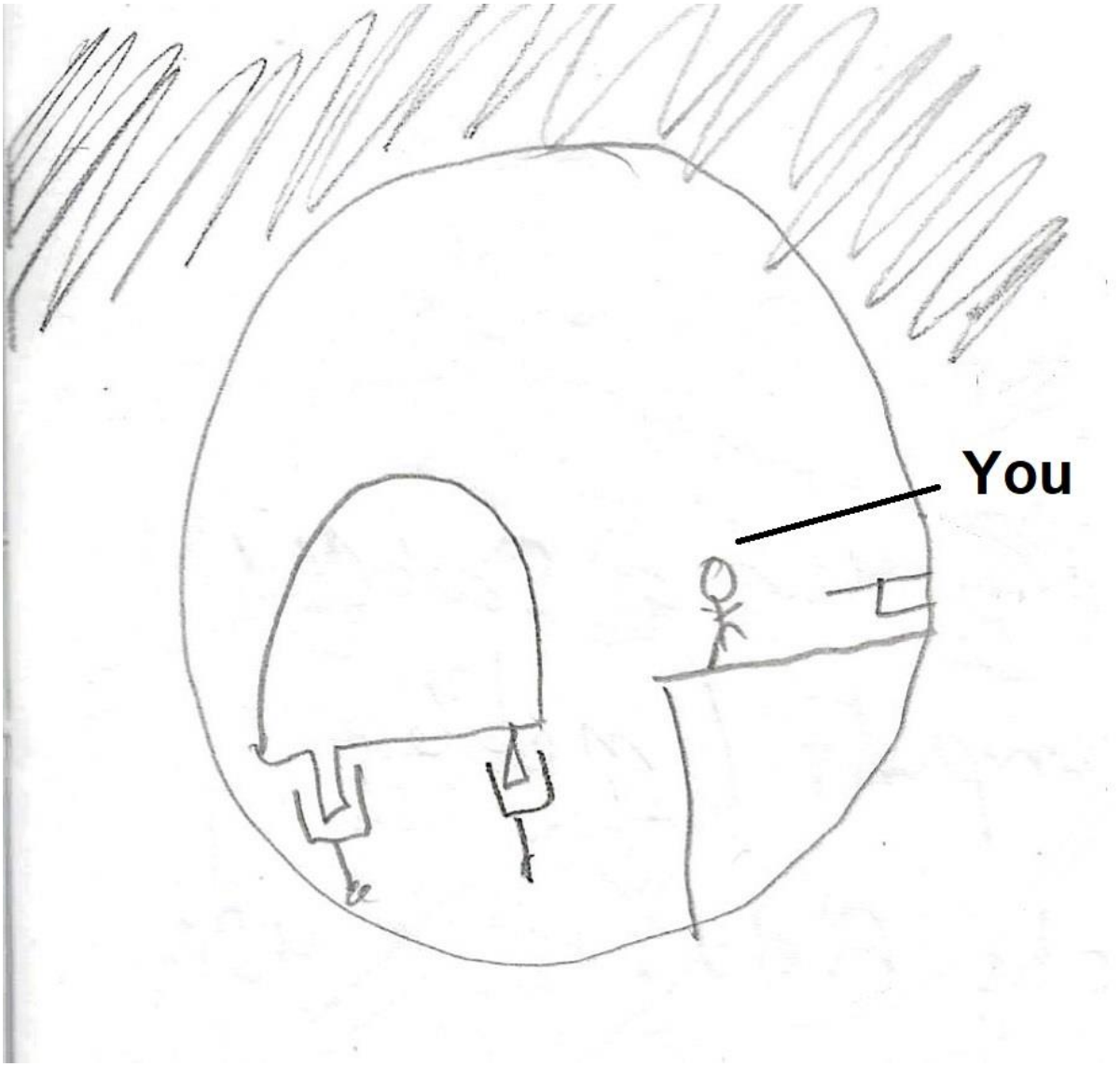
Phone call: as secure as can be

Typical work process

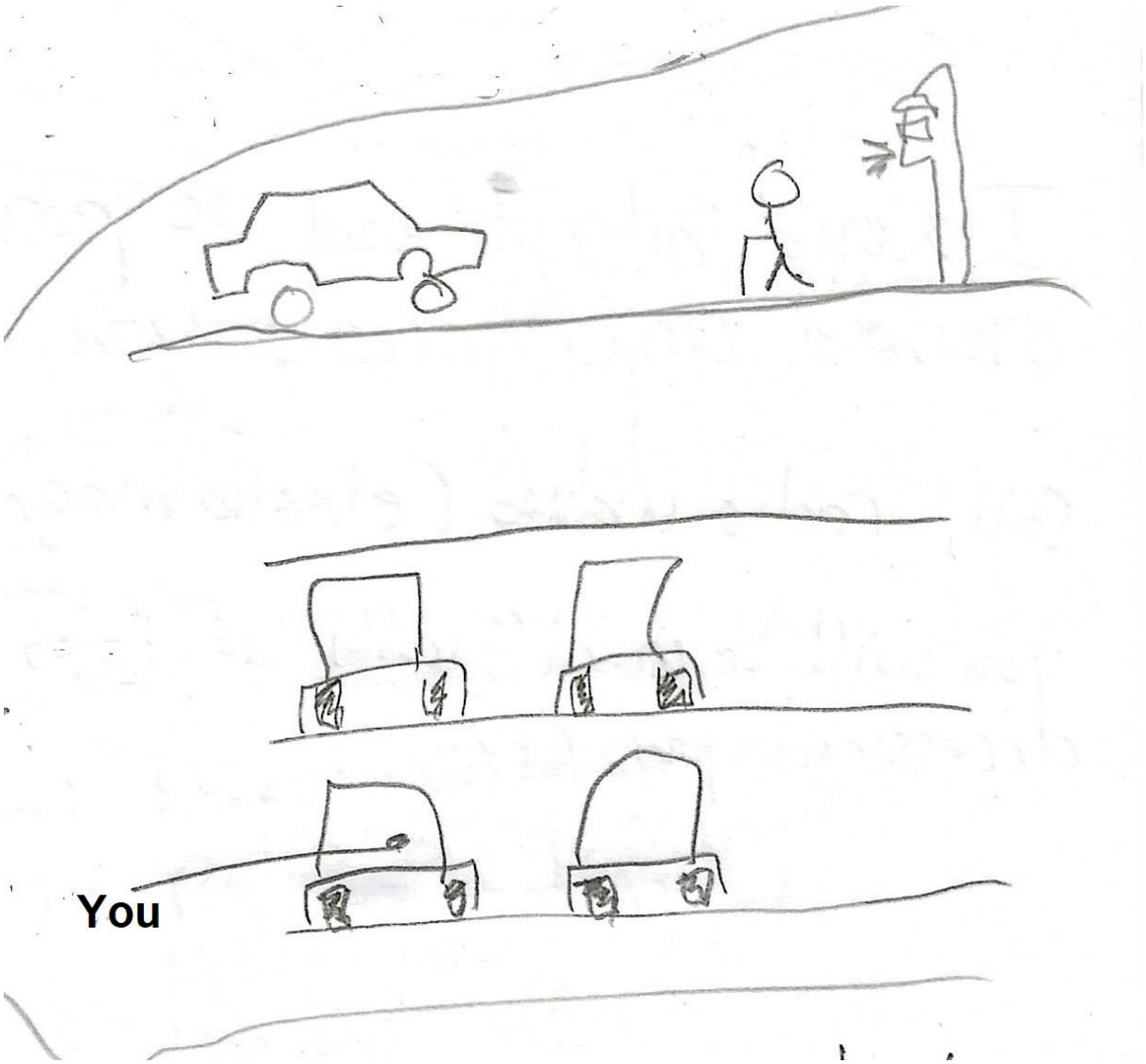
Data/location storage ideas

“Safe” places to do work

In a church in a rural area.



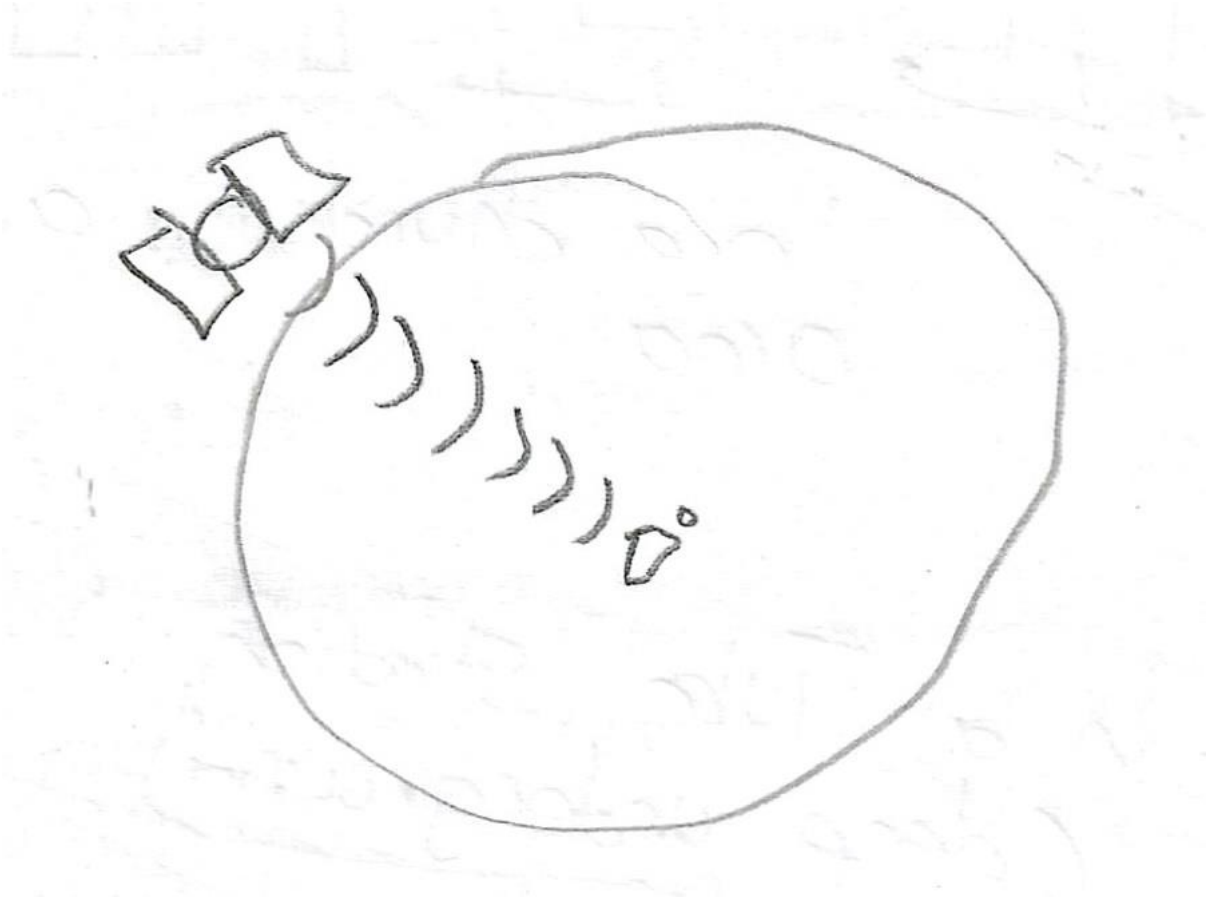
In a Tube Station (deep underground).



At the bottom of an underground car park

In ALL cases check that your mobile is (out) of coverage. No signal.

The key understanding is that the NSA/GCHQ rely on radio wave technology to access your computer.



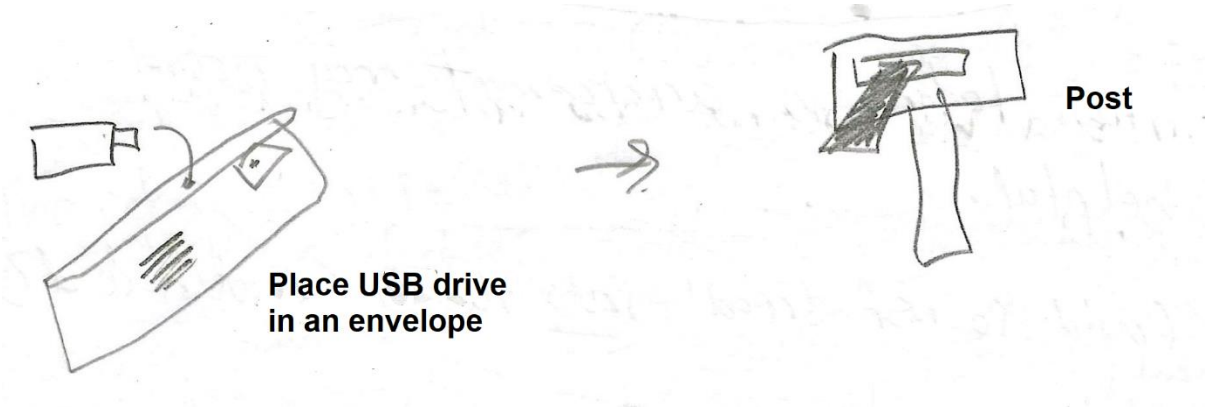
I would not rule out the possibility that a satellite overhead could access your computer/mobile.

Still, radio waves (electromagnetic field) are in use. You will be in difficulty if this is how the NSA is accessing your CPU.

Getting your data to its recipient

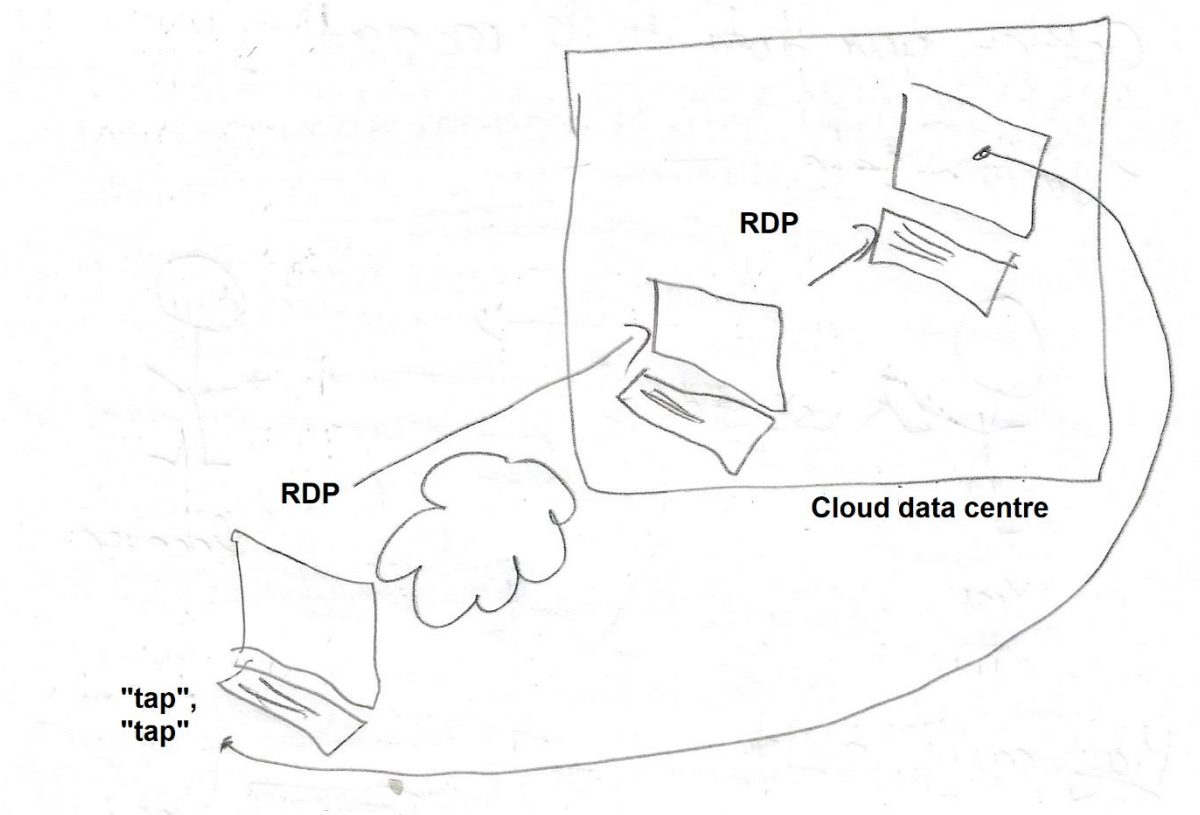
100% safe

May carry a risk



The risk is that there may be spies operating in the post office processing centre. The envelope might go through an X-Ray scan, with the operator discovering there is a USB drive in it. To the spies, data is intelligence.

Random ideas

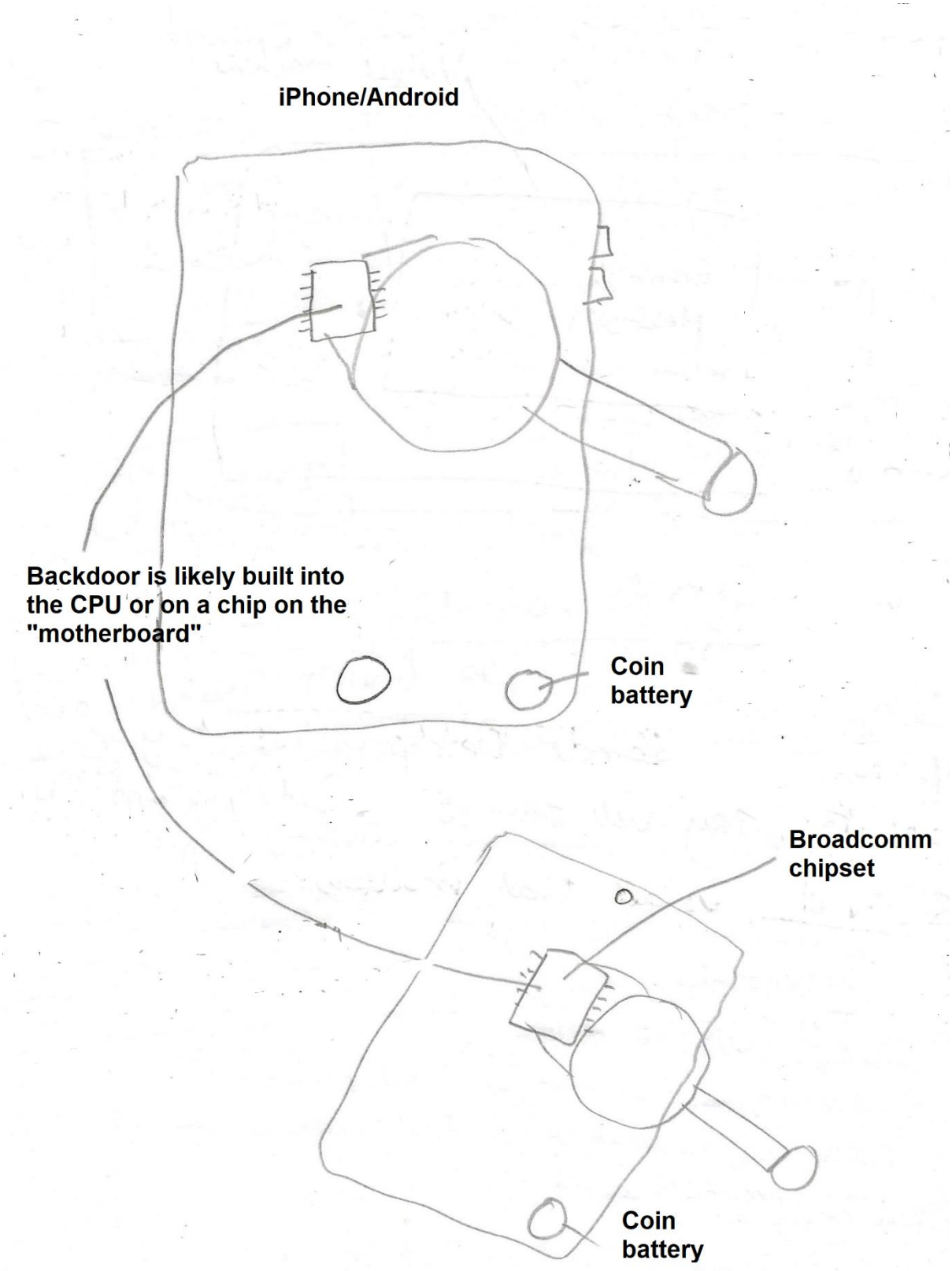


This technology arrangement may prove helpful.

Could the NSA ‘read’ into this? (And hack it?)

RDP stands for Remote Desktop Protocol. In practice you are using a Remote Desktop Connection into the computer in the Cloud.

Mobiles


iPhone/Android
Backdoor is likely built into the CPU or on a chip on the "motherboard"
Coin battery
Broadcomm chipset
Coin battery

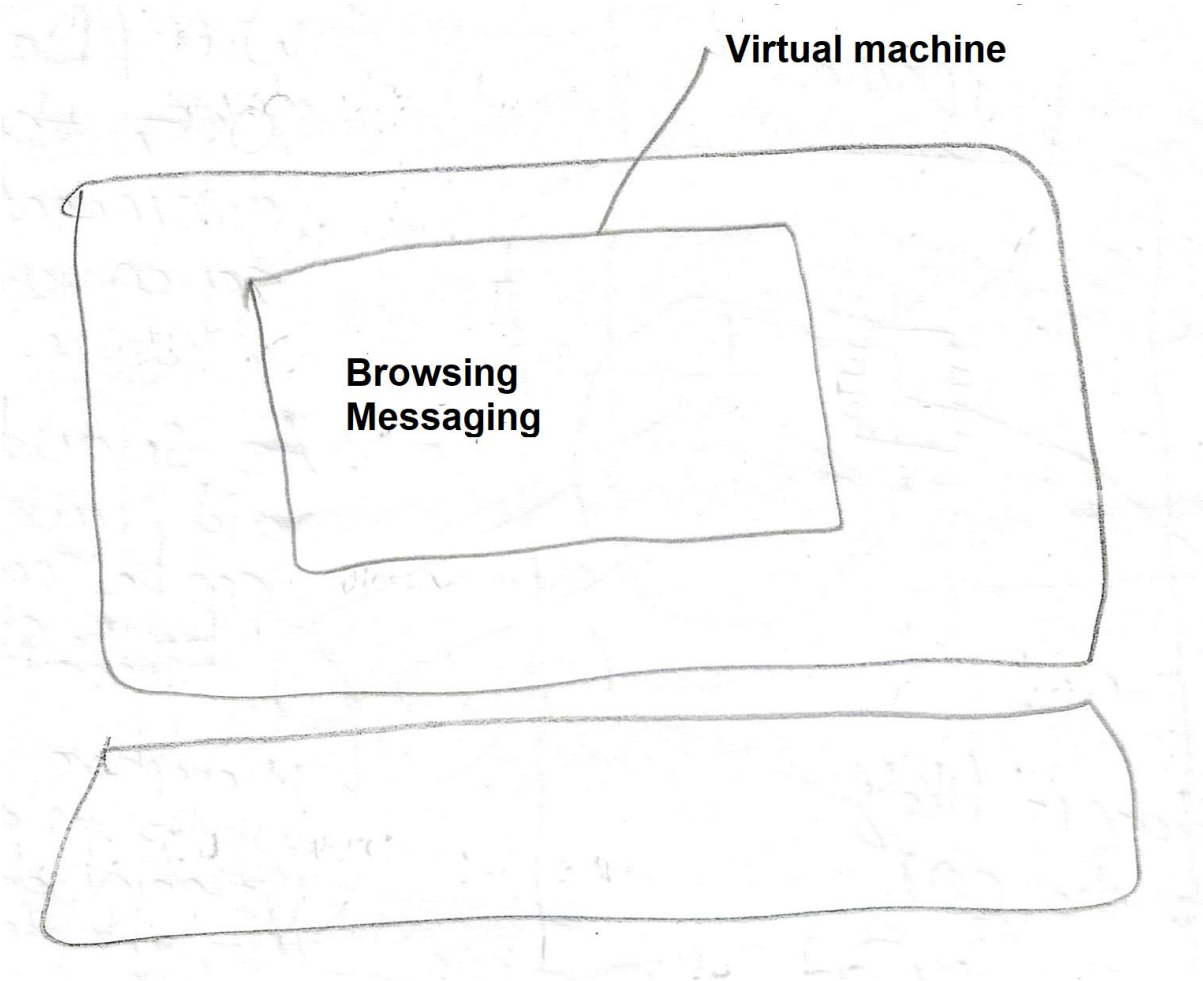
Even with the Wifi or Data connection turned OFF, the NSA can spy on your device.

As Snowden said, your mobile can be controlled by the State.

Microphone works as a listening device even when the device is turned off.

As for the CPU understanding: The idea is to force the manufacturers to install backdoor access. If it is a separate component, the manufacturer can remove it.

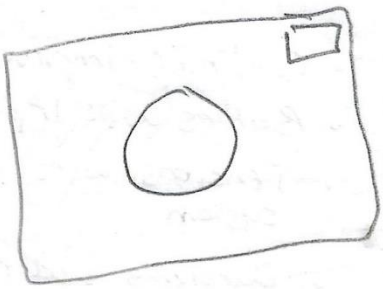
Random ideas – 2



If the NSA has Remote Desktop access to your computer, they will still see what you do.

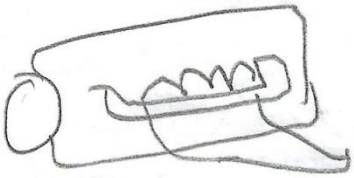
Seeing it, is all that matters.

Safe devices – as long as NOT network enabled



Digital Camera:
- to hold data (storage)
- to make a movie

(To capture events)



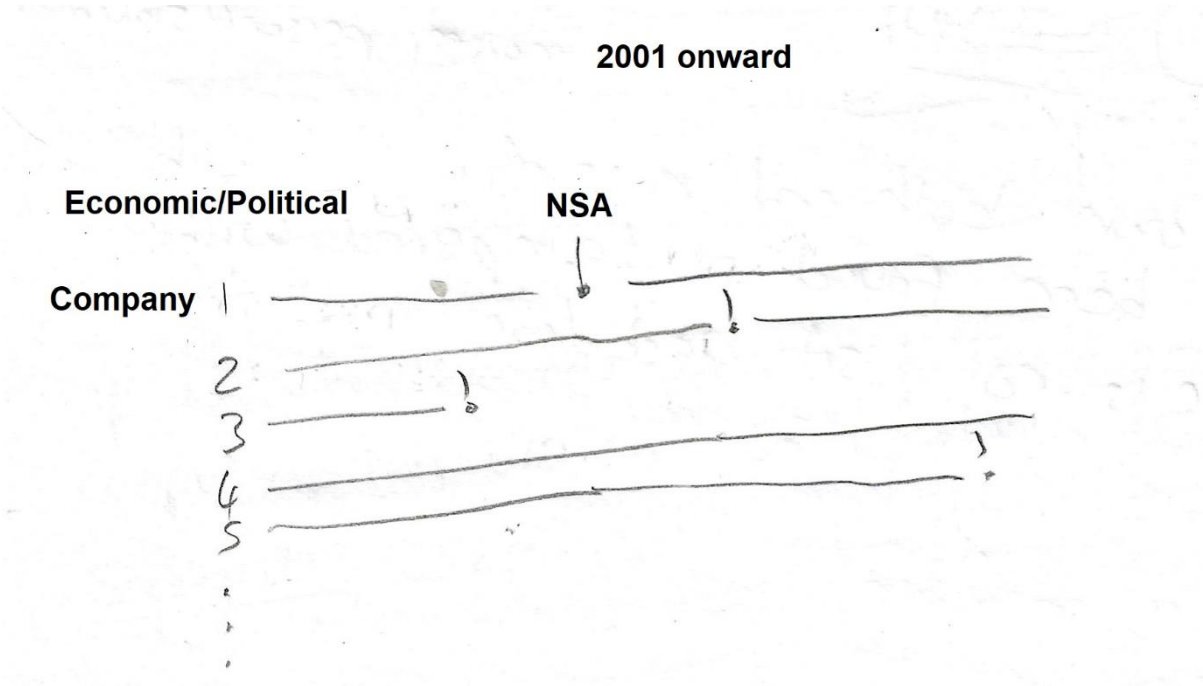
Camcorder:
- Safe for making movies, personal statements

I own both and none of my work has been found or tampered with. There is no NSA backdoor. The older the model the better, although picture quality will be less.

Technology relationship points

The culture is a hybrid of:

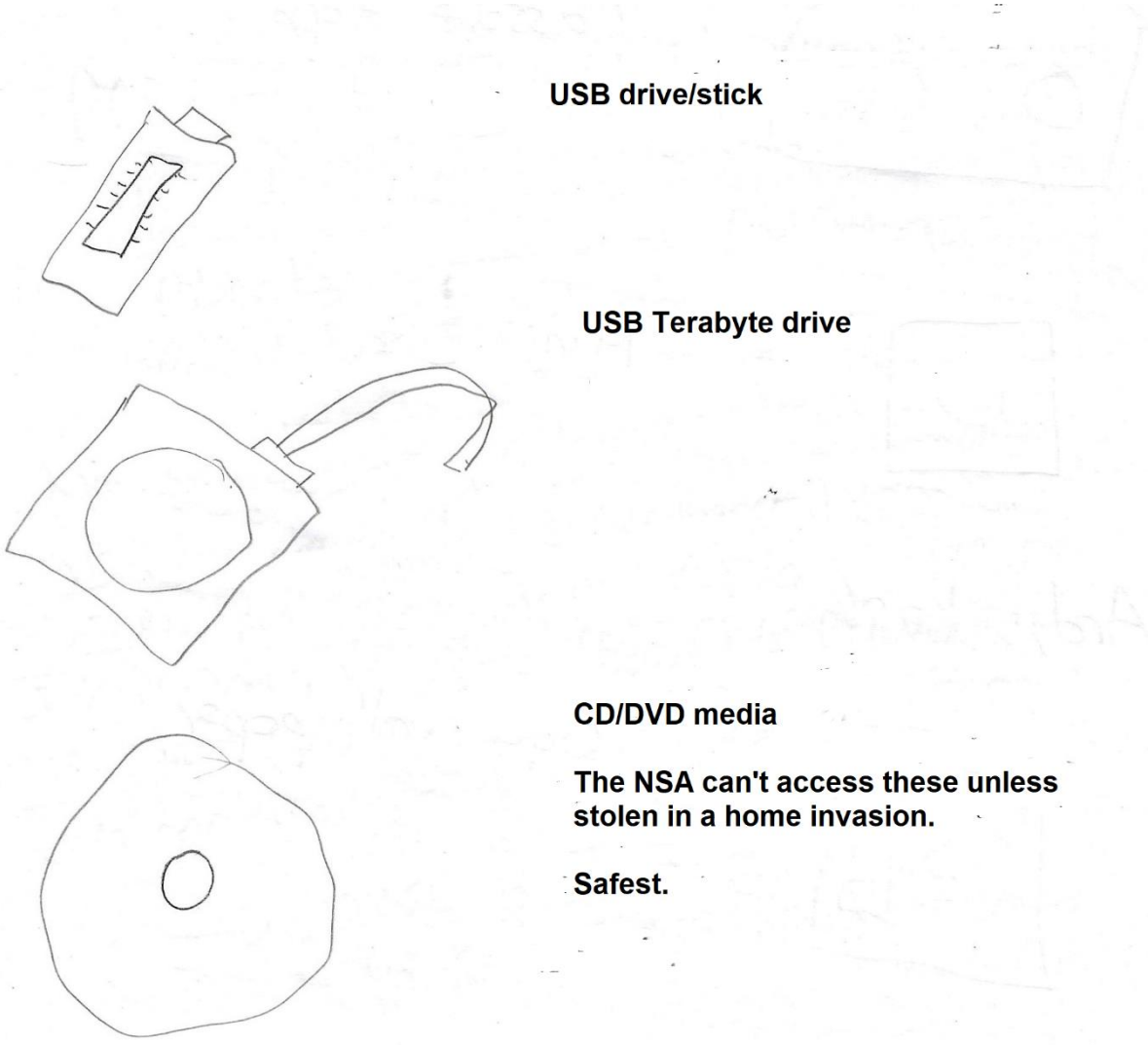
- Innovation
- Creativity
- Trial and error
- Academic involvement
- Peer based critiquing
- Obsolescence
- Continual improvement
- Battles with IP protection
- Tensions with the legal system
- Dynamics with the Web relationship



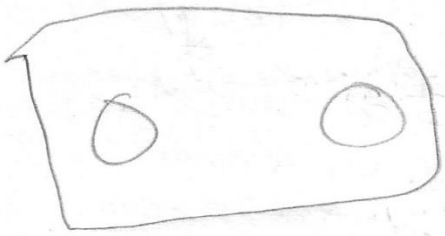
The above image is about the idea that the NSA will be monitoring companies all the time. Products/services will be examined for NSA worthiness (intervention).

Wondering why a competitor seems to have your secrets and you swear you kept your trade secrets under close guard? If they're on a computer…..

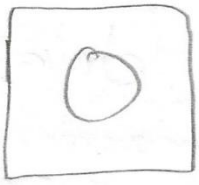
Safe storage devices



The NSA/GCHQ can remotely access the data on a USB drive (memory chip). The range of the remote access device is 50-100 metres.

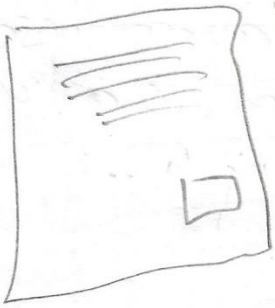


Cassette tape



Mini Disc

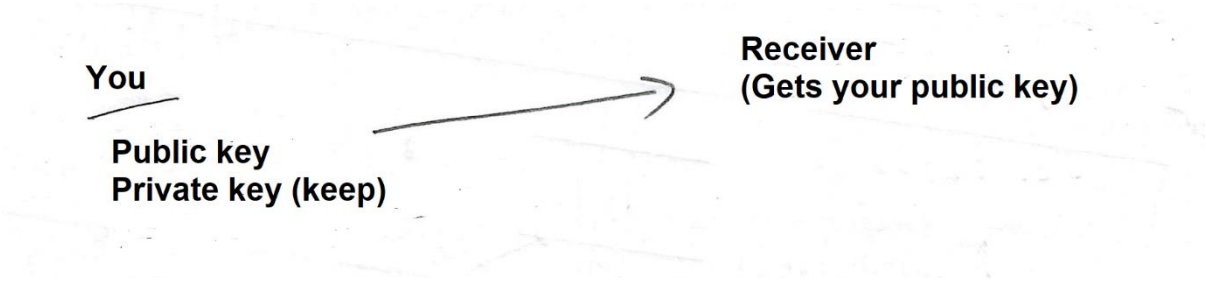
And, lastly:



Good, 'ol paper

If you HAVE to send data over the Net

(1) PGP- Pretty Good Privacy

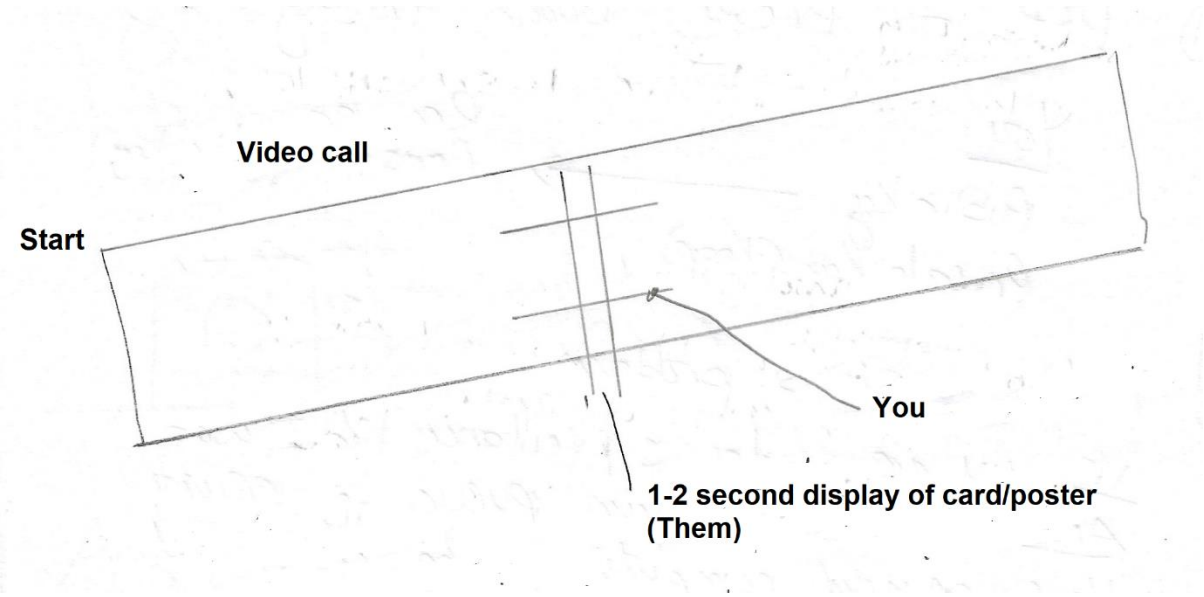


! Not so obvious problem:

IF you are under surveillance like I was AND you store your PUBLIC and PRIVATE PGP keys on your computer, the NSA will find them. Your security is compromised.

- Store the PRIVATE key on a USB drive (And hide the thing somewhere safe).

(2) Flash a card in a video call



1) Run a screen recorder app
2) A few seconds later, stop
3) During playback you will see a ‘still’ of the card for you.

NSA thoughts:

You might be lucky and go unnoticed.

If you are being spied on: it will take the NSA some time to get to the ‘flash card’ moment. It might take them hours or days (or minutes if you are serious case).

Advice? The flashed card should be ambiguous. Establish understanding in a prior, in person meeting.