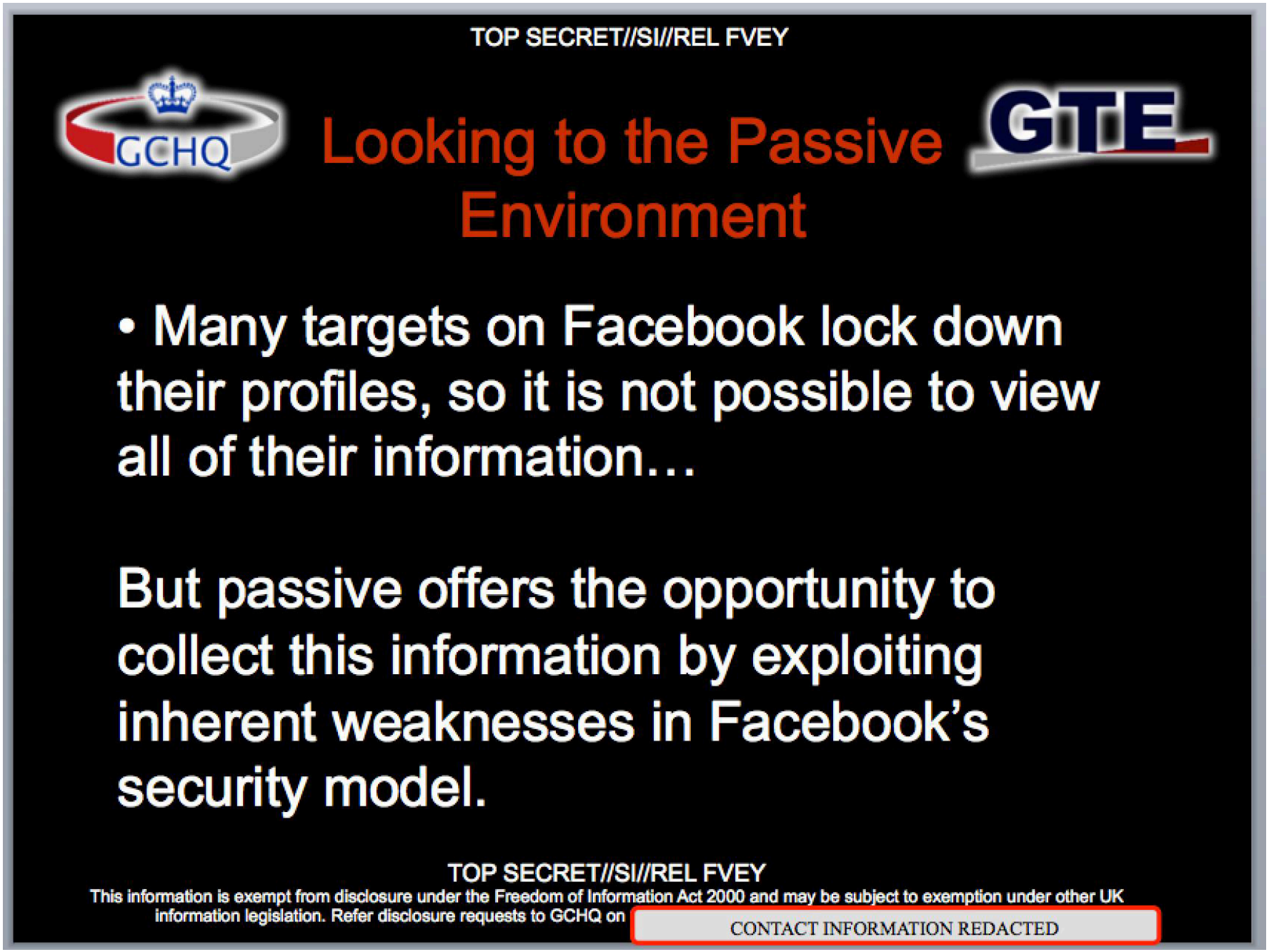

TOP SECRET//SI//REL FVEY
GCHQ
GTE
Exploiting Facebook traffic in the passive environment to obtain specific information
NAME REDACTED
Capability Developer
Global Telecommunications Exploitation (GTE)
GCHQ
TOP SECRET//SI//REL FVEY
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ
CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY

Why OSNs?

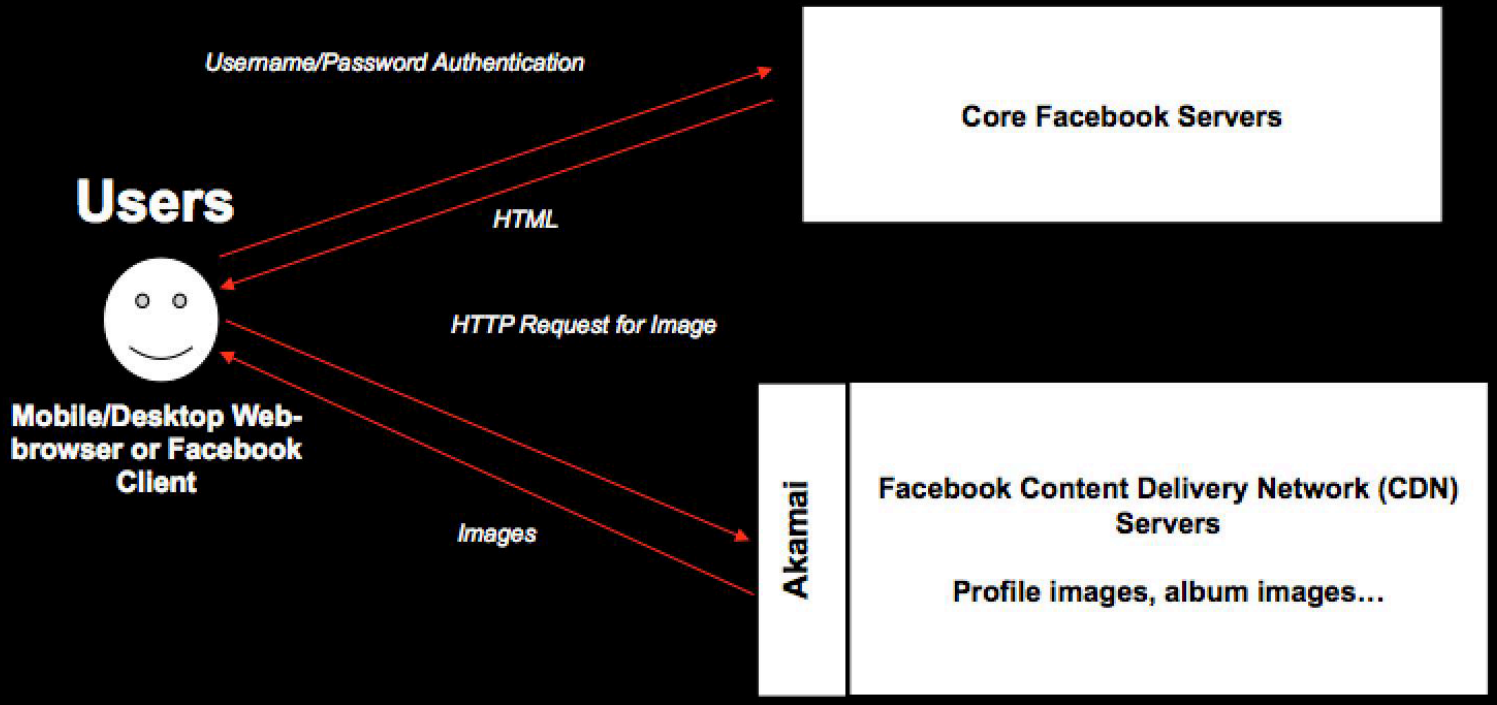
- Targets increasing usage of Facebook, BEBO, MySpace etc.
- A very rich source of information on targets:
  - Personal details
  - 'Pattern of Life'
  - Connections to associates
  - Media

TOP SECRET//SI//REL FVEY
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED


TOP SECRET//SI//REL FVEY
GCHQ
Looking to the Passive Environment
GTE
• Many targets on Facebook lock down their profiles, so it is not possible to view all of their information…
But passive offers the opportunity to collect this information by exploiting inherent weaknesses in Facebook's security model.
TOP SECRET//SI//REL FVEY
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY

Facebook's use of the Akamai CDN



TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY

Exploiting the FB CDN

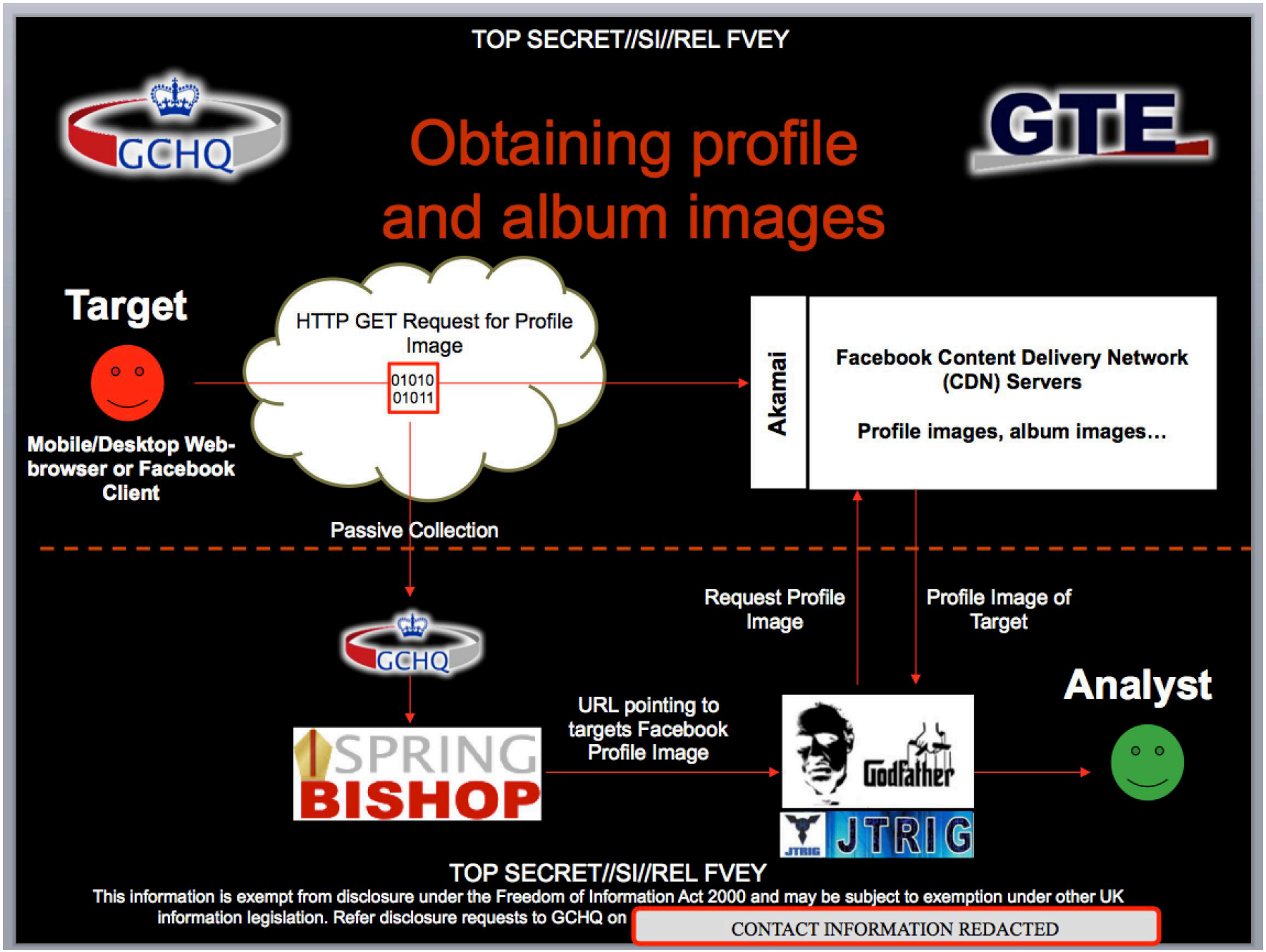
- Weaknesses
  - Assumed Authentication
  - Security through obscurity

It is possible to dissect the CDN URL's generated by Facebook in order to extract the Facebook User ID of the user whose picture the file pertains to. For example, below is a typical profile image URL:

http://**profile.ak.fbcdn.net**/hprofile-ak-sf2p/
hs621.snc3/27353_REDACTED_2215_q.jpg

The text highlighted in green specifically relates to the specific server within Facebooks CDN. And the text highlighted in yellow is the users Facebook User ID.

TOP SECRET//SI//REL FVEY
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED


TOP SECRET//SI//REL FVEY
GCHQ
Obtaining profile and album images
GTE
Target
HTTP GET Request for Profile Image
01010
01011
Akamai
Facebook Content Delivery Network (CDN) Servers
Profile images, album images…
Mobile/Desktop Web-browser or Facebook Client
Passive Collection
Request Profile Image
Profile Image of Target
GCHQ
Analyst
URL pointing to targets Facebook Profile Image
SPRING BISHOP
GodFather
JTRIG
TOP SECRET//SI//REL FVEY
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
CONTACT INFORMATION REDACTED