AFRICAN FORUM ON CYBERCRIME

Policies and Legislation, International Cooperation and Capacity Building

Capacity Building Workshop

Strengthening collaboration between LEAs and Service Providers

Addis Ababa, 16-18 October 2018

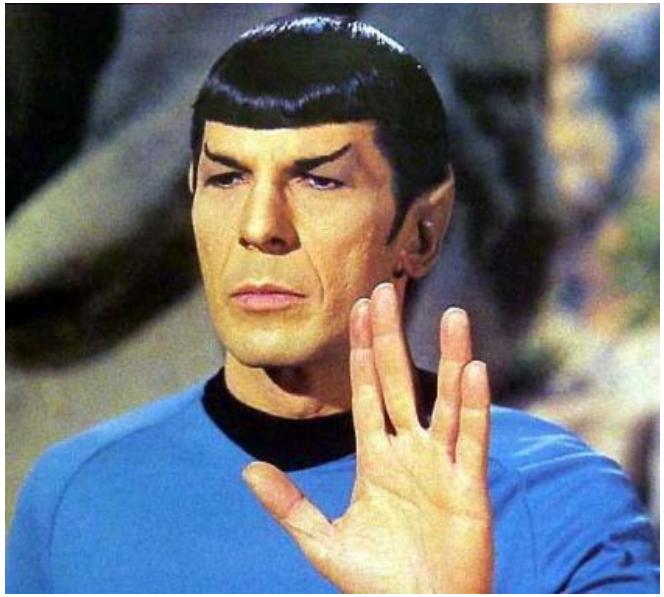
COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

The virtual crime scene

What do we need
and how do we need it?

Subscriber information
Log files
Content

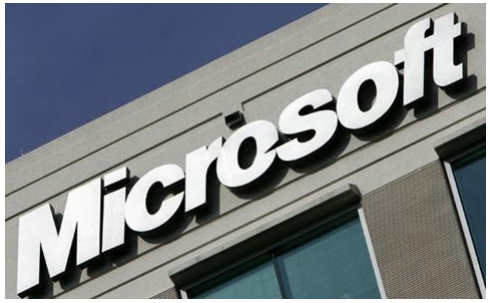


Quick freeze
International collaboration
Single point of contacts (SPOC)

	GOOGLE (USA) Department in Belgium	MICROSOFT (USA) Department in Belgium	FACEBOOK (USA) Department in Belgium	TWITTER (USA)	WHATSAPP (USA)	VIBER (Tokyo)	EBAY (Ireland)	SKYPE (Luxemburg)
Identification	YES User Information IP Registration (If user is located in Europe) Registered Mobile Number Recovery address Activated services	YES User Information IP Registration (if IP address is from in Europe)	YES User Information E-mail address Registered Mobile Number If there is a link with Belgium (except for terrorism / child abuse cases / life in danger)	YES User Information IP Registration (If user is located in Europe)	YES (CRI) Basis subscriber data Device Info App Version Registration date Last date and time of connection Push name(Pseudo)	YES (CRI) User Information IP Registration	YES User Information IP Registration Financial Info Include Item Details Include Seller Registration Information Include Buyer Registration Information	YES User Information IP Registration (if IP address is from in Europe)
Localisation	YES 180 Days IP Logs (If IP addresses are from Europe) Country out of Europe	YES 60 Days IP Logs (Mails IP) MSA Records (=Microsoft life) (if user is located in Belgium)	YES 90 Days IP Logs (if user has a link with Belgium) IP address of registration (if from Belgium and within last 90 days)	YES 90 Days IP Logs (If user is located in Europe)	YES (CRI) 30 Days IP address – date and time of the last connection	YES (CRI) IP Logs 60 Days	YES 4 years ID Logs Billing History List of sold/bought objects	YES IP Logs
nterception/Content	YES (CRI) Content Contact list	YES (CRI) Content Contact list	YES (CRI) Snapshot of the account: Profile contact Information Friends Listing Groups Listing Future and past events Posted Videos Liked Photo	YES (CRI) Non-public tweets Private messages	NO (encrypted)	NO	NO	NO
Preservation	YES Identification Localisation Content	YES Identification Localisation Content	YES Identification Localisation Content	YES Identification Localisation Content	YES Identification Localisation	YES Identification Localisation Content	NO	YES Identification
Urgent procedure	YES Answer between 4 and 6 H	YES +/-1H	YES – life in danger +/-1H	YES +/-1H	YES +/-2H	NO	NO	YES
Based on	Mail account	Mail account	Facebook ID Mail account Cell phone number	Pseudonyme(@...)	Cell phone number	Cell phone number	User ID Item number Mail account	Pseudo

	PAYPAL (Ireland)	2èmeMain/2DeHands (Nederland) Department in Belgium	APPLE (Ireland)	SONY (United Kingdom)	BLACKBERRY (Canada) Department in Belgium	INSTAGRAM (USA) Department in Belgium	UBER (Ireland) Department in Belgium	BADOO (United Kingdom
Identification	YES User Information IP Registration	YES User Information IP Registration Posting Information Payment Information	YES User Information IP Registration (if IP address is from Belgium) Logging logs of contacts that users have had with the customer service iTunes account information Mac address from Bluetooth,Ethernet,Wifi or Firewire connections on one device UDID Gift Cards IOS device activation	YES User Information IP Registration	YES User & devise Information IP Registration	YES	YES User Information IP Registration	YES
Localisation	YES 4 years IP Logs Transactional data Financial Instruments	YES 6 months List of postings IP Logs	YES 6 months IP Logs Itunes account: Download history IP Logs Purchases in Apple stores Online shopping Apple Store Icloud: IP logs connection op Icloud (30 days) Apple mail logs (30 days) IP Logs of Game Center	YES 1 year IP Logs	YES 1 year Transaction logs BBM Transaction logs PIN Current BBM Contact List	YES 1 year	YES IP Logs Requested rides Requested Meals	YES 6 months
Interception/Content	NO	NO	YES CRI Bought items / apps Content (photos,...) from an Icloud account	YES CRI Network messaging information (including text messaging, party chat, etc.),	YES Content BBM Content PIN messages Via CTIF (within Belgium) CRI (outside of Belgium)	YES (CRI) Photo and reactions	NO	NO
Preservation	NO	NO NEED	YES	YES Identification Localisation Content	YES	YES	YES	YES
Urgent procedure	NO	NO	YES	NO	YES	YES	YES	NO
sed on	Mail account Transaction number Account number	Mail account User ID ID object	IMEI Serial number Apple ID/Icloud account Credit Card Number Mail account	Pseudo Mail account Serial number Credit card number	IMEI PIN Number Cell phone number Linked Blackberry e-mail address	Pseudo +date of facts	Driver Info (License plate Name- Cell phone number- Mail account) Rider Info (Name- Cell phone number- Mail account- Credit card number- Trip Info (Date and Time - Start-end location –Trip ID–Triptype of vehicle)	Badoo ID

The ISP-cooperation



= What is happening?

- *Very short data retention 60 days*

Google™

= Good but can do better

- *Only IP addresses in Europe*

facebook®

= **Good** but can do a lot better:

- **only ip addresses from own country**
- 1st amendment – freedom of speech
- internal investigation

facebook Sign Up

Email or Phone | Password | Log In

Keep me logged in | Forgot your password?

Law Enforcement Online Requests

A confirmation email has been sent to request@fccu.be containing a link to the Law Enforcement Online Request System. The link will give you access to the system for one hour.

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the Law Enforcement Guidelines.

facebook Sign Up

Email or Phone | Password | Log In

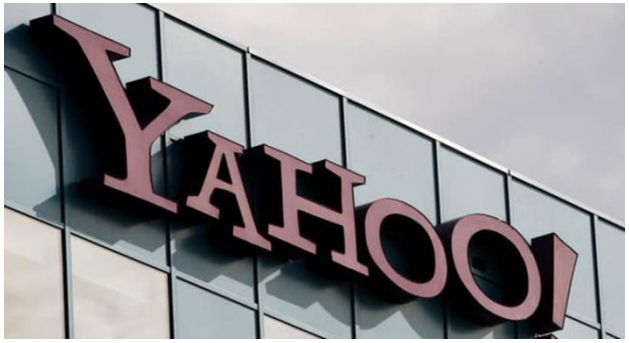
Keep me logged in | Forgot your password?

Home | Preservation Request | Records Request | FAQ | Log Out

Law Enforcement Online Requests

Showing Requests 1 - 25 of 430

Case	Reference	Status	Account	Request Type	Date Requested
312896		Resolved	Facebook · 100002750060132 Download Facebook · 100002259174198 Download	Records	Nov 20, 2013 11:28am
312852	Dossier TG.42.L5.005674/13	Rejected	Facebook · olga.pisters Facebook · naeem.qadir.12	Records	Nov 20, 2013 10:15am
312103	13-019861	Open	Facebook · 100003446697316	Records	Nov 19, 2013 2:52am
312101	13-019848	Open	Facebook · michael.vrijmoed.73	Records	Nov 19, 2013 2:48am
312099	13-019846	Open	Facebook · 100004304074659	Records	Nov 19, 2013 2:45am
312093	13-019825	Open	Facebook · spottedars Facebook · actu.arssoumagne	Records	Nov 19, 2013 2:35am
311668	13-019864	Resolved	Facebook · olga.pisters Download Facebook · naeem.qadir.12 Download	Records	Nov 18, 2013 8:11am
310819	Dossier TG.42.L5.005674/13	Resolved	Facebook · naeem.qadir.12 Download	Records	Nov 15, 2013 5:40am
310768	Dossier TG.42.L5.005674/13	Resolved	Facebook · olga.pisters Download	Records	Nov 15, 2013 2:52am



= BAD

- only through **MLA**
- takes 23-52 months if no imminent threat

= COULD BE A LOT BETTER

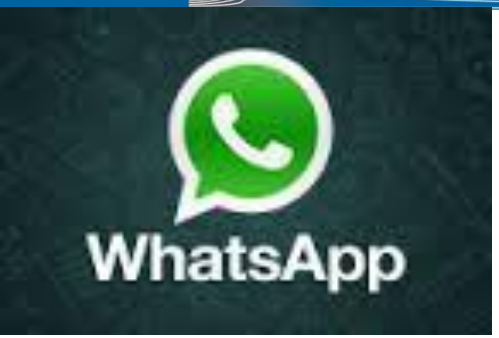
- OK if imminent threat, but very strict policy
- 1st amendment – freedom of speech
- **they warn the user**
- internal investigation

= POOR

- MLA to Luxemburg: Skype Communications SARL
- only IP of the date of creation and financial data if Skype-out
- very short data retention 60 days
- IP date of creation account
- No logs available
- Skype Out: financial data + IP's
- **Can it be wire tapped? BELGIAN SKYPE CASE!**

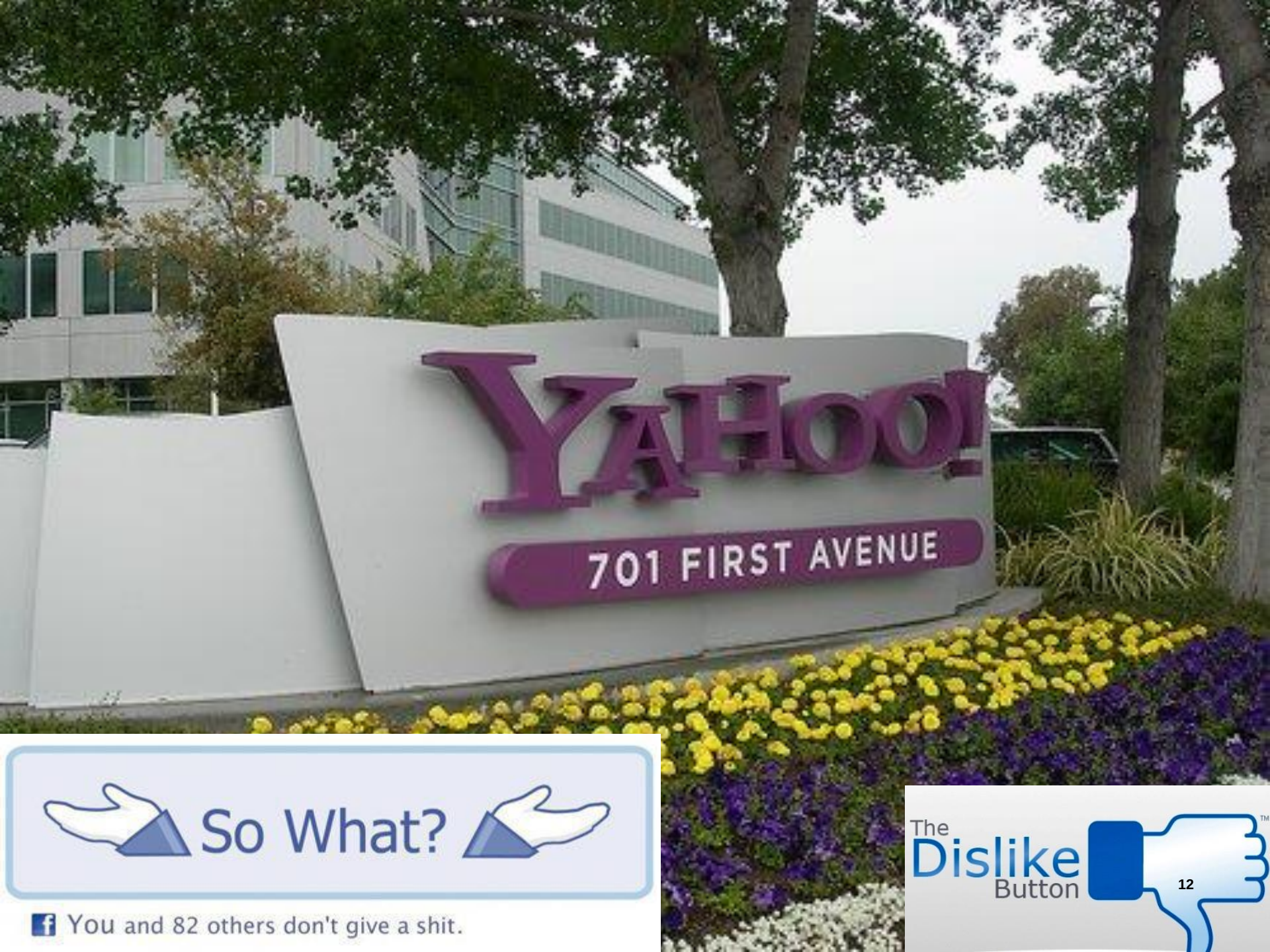
= POOR (non existing)

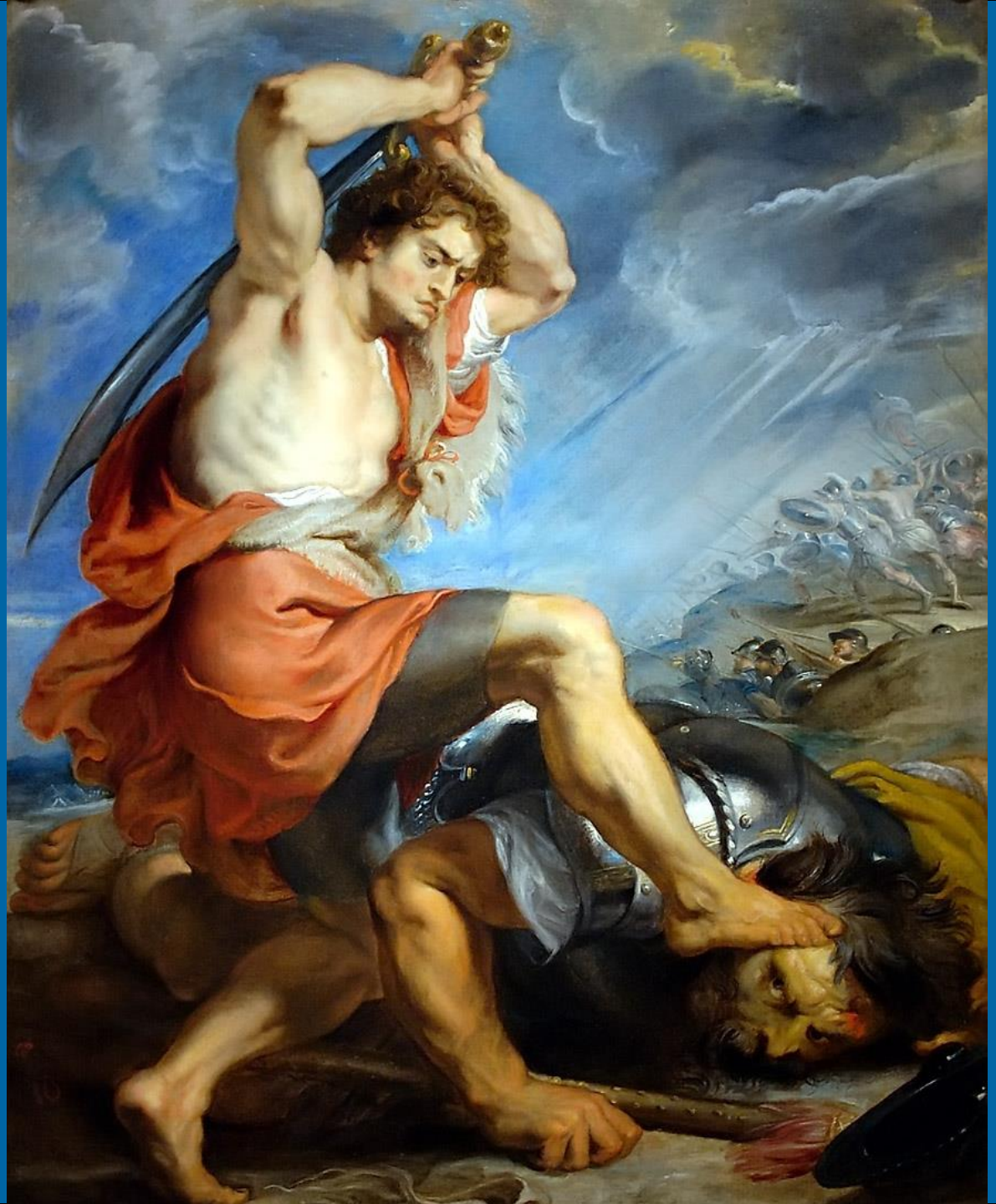
- Very often used by terrorists
- Where is telegram?
- How to reach them?



- Criminal communication tool n° 1
- Cooperation is starting up
- No server content if account is active
- IP from date creation, some traffic data, pictures…
- No mirror possible, no counter measures possible
- **confusion** with the linked phone number!!!

- **they warn the user**!


YAHOO!
701 FIRST AVENUE
So What?
You and 82 others don't give a shit.
The Dislike Button
12



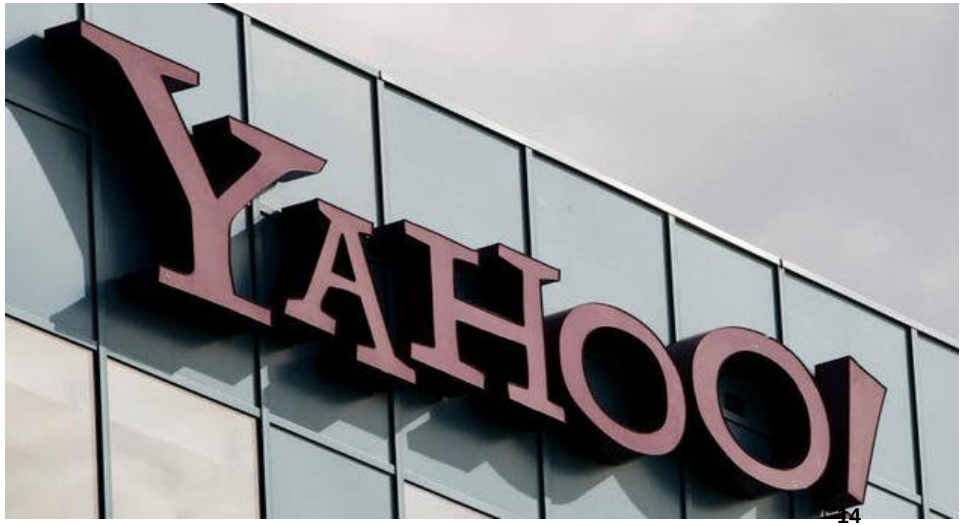
Peter Paul Rubens
(1577 – 1640)

David Slaying Goliath

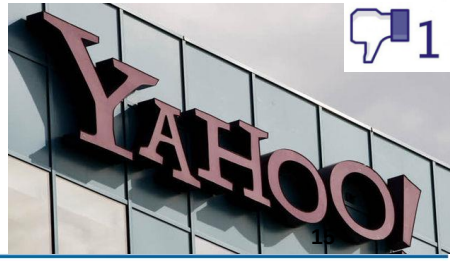
oil on canvas
(123 × 99 cm)
ca. 1616

The Yahoo! case

A Belgian attempt to find a way and to take a position in the war on cybercrime and to cope with the **cyberparadox** of virtual presence and physical absence…



- **The reasoning:**
  - Yahoo Inc.! is (virtually and economically) present in Belgium
  - MLAT = when you think **extra-territorial**
  - Direct request = when you think **territorial**
  - Available for consumers = available for justice
- **The result:**
  - A Belgian request
  - from a Belgian magistrate
  - handed over in Belgium
  - to an ISP that can be found in Belgium



- **Court of First Instance Dendermonde – March 2nd 2009**
  - Conviction: YAHOO! has to collaborate
- **Court of Appeal Gent – June 30th 2010**
  - Acquittal…
- **Supreme Court – January 18th 2011**
  - Cassation: broad interpretation: also foreign ISP's!
- **Court of Appeal Brussels – October 12th 2011**
  - Acquittal…
- **Supreme Court – September 4th 2012**
  - Cassation: valid request!
- **Court of Appeal Antwerp – November 20th 2013**
  - Conviction: YAHOO! has to collaborate
- **Supreme Court – December1th 2015**
  - Cassation: Yahoo must deliver BSI at first request of the Belgian prosecutor

- **Court of First Instance Dendermonde – March 2nd 2009:**
  - Commercially present: “even if it may be through the internet or ‘virtually’”
  - Presence for economic purposes = presence in terms of justice
  - Yahoo! is a provider of an electronic communications service according to article 46bis BCCP = clear intention of legislator
  - Yahoo! is free to exclude the IP range of the Belgian IAP
  - Duty of cooperation extends to any ISP that is displaying services in Belgium

- **Supreme Court – January 18th 2011:**
  - Not only the Belgian operator
  - “any person providing services of electronic communications, such as inter alia the transmission of communications data”
  - “any person offering a service that entirely or mainly consists in transferring signals through electronic communications networks”

- **Supreme Court – September 4th 2012:**

"The circumstance that the Public Prosecutor sends, from Belgium, his written request as meant in Art. 46bis of the (Belgian) Code of Criminal Procedure, requesting the cooperation of the operator of an electronic communication network or of the provider of an electronic communication service established outside of Belgian territory, to a foreign address, ***does not invalidate the request****."*

Court of Appeal Antwerp - November 20th 2013:

- Confirms point of view of the Court of First Instance of Dendermonde
- No formalities prescribed for the demand
- Territorial presence (office in Belgium is not needed)
- Yahoo! is a provider of an electronic communications service according to article 46bis BCCP
- Yahoo! Has to bring the information
- No rogatory commission needed
- If Yahoo! doesn't want to collaborate: exclude IP

Pecuniary penalty of 44.000 Euros (1/2 suspended penalty)

- **Supreme Court – December 1th 2015:**
  - Yahoo = territorially present in Belgium
  - Submitted voluntarily to Belgian law
  - Doesn't require any substantive act abroad
  - No extra-territorial jurisdiction = no MLA needed
  - Production order (art. 18 CCC) = domestic

<= Subscriber information: Yahoo!

Content data: Skype =>

Court of First Instance of Mechelen October 27th 2016: conviction

- Official order from the investigating judge on September 7th 2012
- Official refusal to collaborate on August 27th 2013
- Skype is a provider of a electronic communication service
- No extra-territoriality, Skype is economically present
- Standardized reactions of clear non-collaboration
- Technical impossibility was created by Skype itself, no excuse

"Court considers the crime serious taken in consideration the focus on economical gain without any responsibility towards the Belgian judicial authorities"

Court of Appeal of Antwerp
November 15th 2017: conviction

*The fact that the accused SKYPE is a **provider of an electronic communication service** is apparent from the necessary intervention of SKYPE in the electronic communication by its users in two senses: firstly, all users of SKYPE have to download the software of SKYPE on a computer, tablet, etc. and secondly, at the start of each communication, each user of SKYPE must make a connection with the server of SKYPE, whereupon SKYPE performs a verification and authentication of the relevant users' login data. The fact that the ultimate communication takes place over the Internet and not via a proprietary network of SKYPE does not detract from this position.*

Court of Appeal of Antwerp November 15th 2017: conviction

With regard to the obligations…, which entails the obligation to provide technical assistance for the wiretapping measure, the Court considers that the position of the Court of Cassation, as expressed in its judgment dated 01.12.2015, also applies here in full: the technical cooperation must be provided ***by the operator of the communication network or the provider of the telecommunications service in Belgium, whenever the Belgian examining magistrate requests this****. Any other interpretation would completely erode this legal obligation and make it unworkable in practice.*

Court of Appeal of Antwerp
November 15th 2017: conviction

SKYPE states in … its conclusion that it does not have access to the signals sent by its users via the Internet, and that it could not obtain this access "without making at least substantial changes to its software, working method and physical infrastructure". ***This implies that, if the necessary modifications were made to its technical installations and its working method, SKYPE could gain access to the signals sent by its users and it could therefore provide technical assistance to the examining magistrate if this were ordered****. For example, the accused SKYPE itself states … that it has recently begun storing the content of "instant messaging" Communications, being the text messages that can be sent to each other by SKYPE users online.*

Case now pending at the Supreme Court…

UNIVERSAL JURISDICTION?